Towards a deeper understanding of APN functions and related longstanding problems

Nikolay Stoyanov Kaleyski

Thesis for the degree of Philosophiae Doctor (PhD)
University of Bergen, Norway
2021

UNIVERSITY OF BERGEN

Towards a deeper understanding of APN functions and related longstanding problems

Nikolay Stoyanov Kaleyski

Thesis for the degree of Philosophiae Doctor (PhD)
at the University of Bergen

Date of defense: 24.08.2021

Year: 2021

Title: Towards a deeper understanding of APN functions and related longstanding problems

Name: Nikolay Stoyanov Kaleyski

Print: Skipnes Kommunikasjon / University of Bergen

Acknowledgements

First and foremost, I would like to express my deep gratitude to Lilya Budaghyan for introducing me to this endlessly fascinating field of study; for all the help, support, and encouragement that I received from her in the past four years; for her brilliant leadership of the Selmer centre throughout my studies in Bergen, and for her equally brilliant ideas that helped spark countless avenues of fruitful work; and, in brief, for being the best doctoral supervisor that one could possibly hope for.

Likewise, I am deeply grateful to my co-supervisors, Claude Carlet and Marco Calderini, for their unwavering support whenever it was needed, for the breadth and depth of the knowledge that they shared with me, and for the several interesting projects that we worked on together. Regretfully, I did not have the time to pursue and conclude all the investigations that I would have wanted to; but I look forward to doing so in the future.

In addition, I believe all of my supervisors deserve a separate "thank you" for their careful proofreading of this dissertation, and the plethora of helpful comments and suggestions that they provided.

Although not officially one of my supervisors, I would also like to express my gratitude to Tor Helleseth for his help and support, and for the six months or so of joint work on what I still consider to be the most exciting of the results that I have obtained so far, namely, the infinite family of APN quadrinomials.

As helpful and reliable as they were, my supervisors were not the only ones that I collaborated with during my studies; and so I would like to also thank all those that I had the pleasure of working with. Among those that have not been mentioned so far, I thank: Robert Coulter, Diana Davidova, Constanza Riera, Sondre Rønjom, Pantelimon Stănică, and Yuyin Yu.

I would also like to thank Anne Canteaut and Daniel Panario for agreeing to be on my defense committee; I am deeply honoured to have researchers of their rank take part in my defense and graduation. I am also grateful to George Petrides for coordinating and organizing the procedure, which can be a difficult task in its own right.

It is fair to say that no endeavour can be successful, no matter how ambitious or carefully planned, without the right environment; and so I extend my gratitude to the leadership, administration and technical staff at the Department of Informatics, who made all of this possible. First and foremost, I want to thank Pinar Heggernes for the support and encouragement that I received from her, and for giving me the opportunity to participate in the Christie conference, in addition to many other exciting events, as well as for her phenomenal tenure as head of our department; I have no doubt that she will be equally wonderful in her new role as prorector. I am also grateful to everyone who kept things running smoothly throughout the years and have constantly assisted

me with my teaching, grant applications, necessary bureaucracy, and technical issues. At the risk of forgetting someone, and in no particular order, I therefore thank Linda Vagtskjold, Stefanie Meyer, Tor Bastiansen, Ingrid Kyllingmark, Mo Yan Yuen, Pål Magnus Gunnestad, Ida Rosenlund, Eirik Rekve Thorsheim, Stanislav Oltu, and Olaf Sarnow.

Needless to say, a good working environment is impossible without a friendly social atmosphere, and I have been fortunate to have some of the nicest friends and colleagues that one could wish for. I extend my profound gratitude to Isaac, Sachin, and Srimathi, who helped me to walk through some of those stretches where, alone, I would have struggled to stand. I also want to say a special thank you to Diana, who was my office-mate for the better part of my PhD career; as well as to all my friends from the Selmer centre who helped make the past four years one of the most memorable experiences of my life: Alessandro, Amund, Andrea, Chunlei, Dan, Ermes, Irene, Matthew, Navid, Stein, and Wrya.

I would like to thank Tor Helleseth (once again), and Igor Semaev for their very interesting lectures that I attended in the first years of my PhD; and, on the opposite end, I want to thank my master students, Alise, Ivana, Kjetil, Maren, and Marie, for working together with me and sharing my enthusiasm in the study of cryptographic Boolean functions.

I thank my mother and my grandfather for their unfaltering care and support; without them, none of this would have been possible.

Finally, if your name is not among one of those mentioned above, I would like to thank you, the reader of this dissertation, for taking interest in my work. Whatever the reason that you picked up this text, I hope you will find it entertaining or, at the very least, informative.

NSK

Heard melodies are sweet, but
those unheard are sweeter.

JOHN KEATS

Abstract

This dissertation is dedicated to the properties, construction and analysis of APN and AB functions. Being cryptographically optimal, these functions lack any general structure or patterns, which makes their study very challenging. Despite intense work since at least the early 90's, many important questions and conjectures in the area remain open. We present several new results, many of which are directly related to important longstanding open problems; we resolve some of these problems, and make significant progress towards the resolution of others.

More concretely, our research concerns the following open problems: i) the maximum algebraic degree of an APN function, and the Hamming distance between APN functions (open since 1998); ii) the classification of APN and AB functions up to CCZ-equivalence (an ongoing problem since the introduction of APN functions, and one of the main directions of research in the area); iii) the extension of the APN binomial $x^3 + \beta x^{36}$ over $\mathbb{F}_{2^{10}}$ into an infinite family (open since 2006); iv) the Walsh spectrum of the Dobbertin function (open since 2001); v) the existence of monomial APN functions CCZ-inequivalent to ones from the known families (open since 2001); vi) the problem of efficiently and reliably testing EA- and CCZ-equivalence (ongoing, and open since the introduction of APN functions).

In the course of investigating these problems, we obtain i.a. the following results: 1) a new infinite family of APN quadrinomials (which includes the binomial $x^3 + \beta x^{36}$ over $\mathbb{F}_{2^{10}}$); 2) two new invariants, one under EA-equivalence, and one under CCZ-equivalence; 3) an efficient and easily parallelizable algorithm for computationally testing EA-equivalence; 4) an efficiently computable lower bound on the Hamming distance between a given APN function and any other APN function; 5) a classification of all quadratic APN polynomials with binary coefficients over $\mathbb{F}_{2^n}$ for $n \leq 9$; 6) a construction allowing the CCZ-equivalence class of one monomial APN function to be obtained from that of another; 7) a conjecture giving the exact form of the Walsh spectrum of the Dobbertin power functions; 8) a generalization of an infinite family of APN functions to a family of functions with a two-valued differential spectrum, and an example showing that this Gold-like behavior does not occur for infinite families of quadratic APN functions in general; 9) a new class of functions (the so-called partially APN functions) defined by relaxing the definition of the APN property, and several constructions and non-existence results related to them.

List of papers

1. N.S. Kaleyski. *Changing APN functions at two points*. Cryptography and Communications 11, 1165–1184 (2019)
   Presented at the 10th Int. Conference on Sequences and Their Applications (SETA 2018)

2. L. Budaghyan, C. Carlet, T. Helleseth, N. S. Kaleyski. *On the Distance Between APN Functions*. IEEE Transactions on Information Theory, vol. 66, no. 9, pp. 5742-5753, Sept. 2020
   Presented at the 3rd Int. Workshop on Boolean Functions and their Applications (BFA 2018), under the title "Changing points in APN functions"

3. Y. Yu, N. S. Kaleyski, L. Budaghyan, Y. Li. *Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9*. Finite Fields and Their Applications, Volume 68, 2020, 101733
   Presented at the 4th Int. Workshop on Boolean Functions and their Applications (BFA 2019), under the title "Classification of Quadratic APN Functions with Coefficients in $\mathbb{F}_2$"

4. L. Budaghyan, T. Helleseth, N. Kaleyski. *A New Family of APN Quadrinomials*. IEEE Transactions on Information Theory, vol. 66, no. 11, pp. 7081-7087, Nov. 2020
   Presented at the 4th Int. Workshop on Boolean Functions and their Applications (BFA 2019)

5. N. S. Kaleyski. *Deciding EA-equivalence via invariants*. To appear in Cryptography and Communications
   Presented at the 11th Int. Conference on Sequences and Their Applications (SETA 2020)

6. D. Davidova, N. S. Kaleyski. *Generalization of a class of APN binomials to Gold-like functions*. In: Bajard J.C., Topuzoğlu A. (eds) Arithmetic of Finite Fields. WAIFI 2020. Lecture Notes in Computer Science, vol. 12542
   Presented at the International Workshop on the Arithmetic of Finite Fields (WAIFI 2020)

7. L. Budaghyan, N. S. Kaleyski, S. Kwon, C. S. Riera, P. Stanica. *Partially APN Boolean functions and classes of functions that are not APN infinitely often*. Cryptography and Communications 12, 527–545 (2020)
   Presented at the 10th Int. Conference on Sequences and Their Applications (SETA 2018)

8. L. Budaghyan, N. S. Kaleyski, C. S. Riera, P. Stanica. *Partially APN functions with APN-like polynomial representations*. Designs, Codes and Cryptography 88, 1159–1177 (2020)
   Presented at the 4th Int. Workshop on Boolean Functions and their Applications (BFA 2019)

9. L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, N. S. Kaleyski. *On two fundamental problems on APN power functions*. Cryptology ePrint Archive: Report 2020/1359. Submitted to IEEE Transactions on Information Theory
   Presented as two talks at the 11th Int. Conference on Sequences and Their Applications (SETA 2020), under the titles "On a Relationship between Gold and Kasami Functions and other Power APN Functions" and "A note on the Walsh spectrum of Dobbertin APN functions"

Contents

Chapter 1

Introduction

The work presented in this thesis is dedicated to the properties and construction of APN and AB functions. The study of these two classes of functions is important for a number of reasons. The immediate practical utility comes from the design of secure block ciphers in symmetric cryptography; from this point of view, APN and AB functions provide the best possible security against differential and linear cryptanalysis, respectively. On the other hand, APN and AB functions correspond to optimal objects in many other areas of study across mathematics and computer science, including sequence design, combinatorics, coding theory, and projective geometry. In this sense, these two classes of functions have a far-reaching, universal significance which transcends the practical needs of cryptography. Advances in the study of APN and AB functions can thus lead to progress in many other areas, and, conversely, results and techniques from different branches of mathematics and computer science can provide a better understanding of the properties and structure of these functions.

Despite such noteworthy correspondences, APN and AB functions are remarkably difficult to study. Since they are cryptographically optimal, they lack by design any general structure or clear patterns that could be exploited by a potential adversary; and the lack of such structure and patterns makes their construction and analysis very difficult as well. Indeed, despite an intense interest in these functions and a huge amount of work and investigations conducted since at least the early 90's, there are many difficult problems in the area that have remained open for a very long time. In this dissertation, we try to address some of these problems; we successfully solve some of them, and make significant contributions towards the resolution of others.

More precisely, we consider the following open problems:

1) the maximum algebraic degree of an APN function, and the Hamming distance between APN functions (open since 1998);

2) the classification of APN and AB functions up to CCZ-equivalence (an ongoing problem, open since the introduction of APN functions in the early 90's);

3) the generalization of the APN binomial $x^3 + \beta x^{36}$ over $\mathbb{F}_{2^{10}}$ to an infinite family of APN functions (open since 2006);

4) the Walsh spectrum of the Dobbertin APN power function (open since its introduction in 2001; note that the Walsh spectra of all the remaining infinite APN power families have already been computed);

5) Dobbertin's conjecture that the known infinite APN power families exhaust all possible cases, i.e. that any APN power function is CCZ-equivalent to a representative from one of the known families;

6) efficiently testing the equivalence between two given functions (an ongoing problem open since at least the introduction of APN functions, and a prerequisite for classifying APN and AB functions); note that the currently known methods are unreliable or do not work at all for dimensions n greater than 10.

In brief, the main highlights of our progress on the individual problems is as follows:

1) we contribute a number of theoretical and computational results to problem 1) that suggest that the algebraic degree of an APN function over $\mathbb{F}_{2^n}$ can not be equal to n, and we develop theoretical criteria and algorithms for estimating the minimum Hamming distance between a given APN function F and any other APN function;

2) we classify all quadratic APN functions with binary coefficients over $\mathbb{F}_{2^n}$ up to $n = 9$;

3) we generalize the binomial $x^3 + \beta x^{36}$ into a new infinite family of APN functions, and thereby completely resolve problem 3);

4) we experimentally compute the Walsh spectrum of the Dobbertin function over $\mathbb{F}_{2^n}$ up to $n = 35$, and conjecture its exact form;

5) motivated by problem 5), we formulate two alternative representations of power APN functions; we expect that these representations might help to investigate properties of power APN functions that are difficult to handle otherwise;

6) we introduce two new invariants (one under CCZ-equivalence, and one under EA-equivalence), as well as an efficient algorithm for computationally testing EA-equivalence over any finite field of even extension degree that only relies on elementary operations.

In addition, we introduce the class of partially APN functions, which is a new class of functions obtained by relaxing the definition of APN-ness, and we investigate its behavior and properties theoretically and experimentally. A more detailed summary of our results follows.

We first present results on the Hamming distance between APN functions; this study is motivated by problem 1), which has been investigated via a construction in which an output value of a given function F is modified in order to obtain a new function G [21]. Previous attempts to construct new APN functions by changing a small number of outputs have been unsuccessful (including ones described in [21], and our own experiments); we derive characterizations that explain why this is so. In the case of changing $K = 2$ outputs, we obtain non-existence results for some important classes of functions. In the general case when $K \in \mathbb{N}$ outputs are changed, we formulate a filtering algorithm for determining how the outputs need to be modified to obtain an APN function; we derive a lower bound on the distance between a given APN function F and any other APN function; and we obtain the first useful CCZ-invariant for APN functions in the past 10 years or so.

Our next result is on problem 2), i.e. the classification of APN functions. This is itself a very hard problem: to date, APN functions have been classified up to CCZ-equivalence only up to dimension 5 (in 2008) [14], up to dimension 7 for quadratic functions (in 2012 for $n = 6$ [56], and 2020 for $n = 7$ [53]), and up to dimension 6 for cubic functions (in 2012) [56]. We specialize a matrix representation of quadratic (n,n)-functions developed by Yu et al. [71] to the case of quadratic functions with binary coefficients, and derive restrictions on the representation of such functions. This results in a reduction in the search space that is sufficient to find and classify up to CCZ-equivalence all quadratic APN functions with binary coefficients up to $n = 9$. Remarkably, we find two new instances of APN functions over $\mathbb{F}_{2^9}$.

We construct an infinite family of APN quadrinomials that generalizes the binomial $x^3 + \beta x^{36}$ over $\mathbb{F}_{2^{10}}$, thereby resolving problem 3). The latter has been known since 2006, and is one of the earliest known examples of an APN function CCZ-inequivalent to a monomial. Despite attracting a lot of interest for this reason, it had remained unclassified into an infinite family up to now. At least one paper based on the approach used in our work has already appeared [72].

One of the most difficult practical problems in the study of APN functions is to decide whether two given functions are equivalent under some notion of equivalence (typically, CCZ-equivalence or EA-equivalence). The existing equivalence tests solve this problem through coding theory, which has a number of shortcomings, including long running times and prohibitively large memory consumption. Recently, the notion of an orthoderivative was introduced and shown to be very useful in practice for deciding the CCZ-equivalence of quadratic APN functions [62] (see also Section 1.4.2); the orthoderivatives associated with two EA-equivalent functions are themselves EA-equivalent, and the invariants (such as the differential spectrum or the extended Walsh spectrum) of the orthoderivatives are almost always distinct for functions belonging to distinct EA-equivalence classes (with some very rare exceptions, such as for some power APN functions). Despite their practical utility, orthoderivatives (and their properties) do not constitute a test for EA-equivalence since they can only be used to disprove the EA-equivalence of two given quadratic APN functions (more precisely, if two functions have orthoderivatives with distinct values of an invariant, then the functions are necessarily EA-inequivalent; however, even if the values of all known invariants are the same for their orthoderivatives, this does not imply that two functions are EA-equivalent). In our work, we develop a test for EA-equivalence that is easy to implement, uses only basic arithmetic and logic operations, and is naturally parallelizable. In the course of doing so, we introduce yet another useful invariant, this time for the case of EA-equivalence. We note that our test is significantly faster in the case of quadratic functions, but can be applied to functions of any algebraic degree.

The Gold power functions are defined as x^{2^i+1} over $\mathbb{F}_{2^n}$ with $\gcd(i,n) = 1$. Relaxing this condition to $\gcd(i,n) = t$ is known to give power functions all of whose derivatives are 2^t-to-1. Furthermore, the functions from one of the known infinite families (given under F1-F2 in Table 1.3 for n divisible by 3) can be generalized to functions with good nonlinearity, all of whose derivatives are 2^t-to-1 functions, in a similar way [13]. We show that this is possible for yet another infinite polynomial family (namely, for the family indexed as F1-F2 in Table 1.3 for n divisible by 4), and compute a lower bound on the resulting nonlinearity. We demonstrate by a counterexample that there

are infinite families of APN functions that behave like the Gold functions in many other respects, but for which such a generalization is not possible; and so, the families that do allow such a generalization are particular in this sense.

Further, we introduce and study a new class of functions called partially APN (or pAPN) functions by relaxing the definition of APN functions. Thus, any APN function is pAPN, but not vice-versa. Constructions, properties, and non-existence results for pAPN functions could potentially be applied to APN functions in order to resolve hard open problems, including the existence of APN permutations for even n, and the maximum algebraic degree of an APN function. For instance, obtaining non-existence results on APN permutations could potentially be done by going through pAPN-permutations first: since any APN permutation must, in particular, be a pAPN permutation, showing that a pAPN permutation (or function, in general) cannot have a certain form implies that the same is true for an APN permutation; conversely, finding constructions and characterizations of pAPN permutations would be a natural way to try and find APN ones. We provide several characterizations of the new class of functions, investigate their properties theoretically and computationally, and provide several constructions for functions of this type.

Finally, we study simpler representations of functions from the known monomial families as a method for approaching problems 4) and 5). We derive such representations of the form $x^i \circ x^j$ for the Niho and Dobbertin power functions, and show that they are optimal (in some sense). Separately, we consider compositions of the form $x^i \circ L \circ x^j$ where L is a linear polynomial. We observe that it is possible to express APN functions CCZ-inequivalent to x^i and x^j in this way. In the case when L has binary coefficients, we mathematically investigate some specific cases of such constructions, and conduct computer searches showing that the cases that we treat exhaust all possibilities over $\mathbb{F}_{2^n}$ with $n \leq 9$ (when L has binary coefficients). This will be useful for investigating the existence of APN power functions CCZ-inequivalent to representatives from the known infinite families. We experimentally compute the Walsh spectrum of the Dobbertin power function over $\mathbb{F}_{2^n}$ for $n \leq 35$, and conjecture its exact form. The Dobbertin family is the only infinite monomial APN family for which the Walsh spectrum has not been computed, and problem 4) has been open since the introduction of the family in 2001. It was later shown that all Walsh coefficients of the Dobbertin function over $\mathbb{F}_{2^{5m}}$ are divisible by 2^{2m} [30], and there has been practically no further progress until now.

This dissertation is organized as follows. In Section 1.1, we introduce the basic notion of a vectorial Boolean function and related concepts, and discuss how such functions can be represented as truth tables, and as multivariate and univariate polynomials over finite fields. In Section 1.2, we define some cryptographic properties of vectorial Boolean functions, including differential uniformity and nonlinearity, and we introduce the classes of APN and AB functions. In Section 1.3, we consider the most important equivalence relations used in the classification and study of APN and AB functions, namely CCZ-equivalence, EA-equivalence, and cyclotomic equivalence. In Section 1.4, we present a summary of the known invariants under CCZ- and EA-equivalence and how they can be used to facilitate testing CCZ- and EA-equivalence. In Section 1.5, we survey the known infinite families of APN functions, while in Section 1.6, we consider the known sporadic instances of APN functions, i.e. those APN functions that have not yet been classified into infinite families. In Section 1.7, we give

an overview of the papers that make up the rest of the dissertation, and briefly discuss the main scientific contributions of each paper, and how they tie in with the current state of knowledge presented in the preceding sections. Finally, Section 1.8 provides a brief conclusion to the work, and points out some potential directions for future study.

The remainder of the dissertation consists of nine papers that document our work. The first eight of these papers have already been published, or accepted for publication, in various journals, while the last one is under review at IEEE Transactions on Information Theory at the time of writing. The content of the papers is exactly the same as the final version that was submitted to the respective journals immediately prior to publication (in particular, some of the references given in the papers may be outdated; the list of references at the end of this chapter is up-to-date). The only major difference between the papers as they are presented here, and their published versions, is an aesthetic one: we have tried to make the style and formatting of the papers as uniform as possible; while the actual published versions follow different guidelines and templates according to the particular journal.

1.1 Vectorial Boolean functions and their representation

Let $\mathbb{F}_2$ be the finite field with two elements, and let $\mathbb{F}_2^n$ denote the vector space of dimension n over $\mathbb{F}_2$, for any natural number n. A **vectorial Boolean function**, or (n,m)**-function**, is any mapping F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We can immediately appreciate the enormous range of the applications of such functions as soon as we note that any operation that takes n bits as input and produces m bits as output can be modeled as an (n,m)-function. Since any data can be encoded in binary, this means that any arithmetic operation, any logical operation, and, indeed, any computer program, can be represented as an (n,m)-function. It is thus no surprise that vectorial Boolean functions naturally occur in many different branches of pure and applied mathematics and computer science.

In the particular case when $m = 1$, we call $(n,1)$-functions simply **Boolean functions** (as opposed to vectorial Boolean functions). A Boolean function can be seen as encoding an assignment of true and false values to every element from its domain. Despite having the appearance of being very restrictive due to their co-domain consisting only of the elements 0 and 1, Boolean functions are one of the most important and well-studied subclasses of vectorial Boolean functions. Indeed, many of the most natural applications of (n,m)-functions are of this type: for instance, if $S \subset T$ are arbitrary sets, then the indicator function of S in T can be represented as a Boolean function on $\lceil \log_2 \#T \rceil$ variables; the incidence or adjacency matrix of an undirected graph can be viewed as a Boolean function, where each input sequence of bits encodes some combination of an edge and a vertex (in the case of the incidence matrix) or two vertices (in the case of the adjacency matrix), respectively.

We remark that any (n,m)-function can be represented as an m-dimensional vector of Boolean $(n,1)$-functions; this provides another justification for the name "vectorial Boolean function". More precisely, if $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is an (n,m)-function, we can write

$$F(x_1, x_2, \ldots, x_n) = (f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

where $f_1, f_2, \ldots, f_m$ are $(n,1)$-functions. If $y = (y_1, y_2, \ldots, y_m) = F(x)$ for some $x \in \mathbb{F}_2^n$

and $y \in \mathbb{F}_2^m$, then $f_i(x) = y_i$ for $i = 1, 2, \ldots, m$, i.e. f_i expresses the i-th coordinate of the output. For this reason, the Boolean functions f_i are called the **coordinate functions** of F. In this way, any (n,m)-function can be decomposed into m coordinate functions; and any m Boolean functions on n variables can be combined into an (n,m)-function. Some properties of vectorial Boolean functions are defined in terms of their coordinate functions; and, what is even more usual, some properties are defined in terms of the non-zero linear combinations of the coordinate functions. The $2^m - 1$ non-zero linear combinations of the coordinates functions of an (n,m)-function F are called the **component functions** of F. Thus, every coordinate function is a component function, but not vice-versa. Since any linear combination of the coordinate functions corresponds to taking the sum of a subset of $\{f_1, f_2, \ldots, f_m\}$, we can identify any component function with a non-zero vector in $\mathbb{F}_2^m$. For instance, if $F = (f_1, f_2, f_3, f_4)$, then the vector $b = (0,1,0,1)$ would correspond to the linear combination $f_2 + f_4$. Based on these considerations, we can denote the component function $x \mapsto f_2(x) + f_4(x)$ by F_b.

Another way of expressing vectorial Boolean functions using Boolean functions is by means of their graph indicators. The **graph** of an (n,m)-function F is the set $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$; this essentially amounts to a "look-up table" of its values. Note that $\Gamma_F \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m$, and the pairs in $\mathbb{F}_2^n \times \mathbb{F}_2^m$ can be identified with the elements of $\mathbb{F}_2^{n+m}$. The **graph indicator** of F is then the indicator function of Γ_F; that is, the Boolean $(n+m,1)$-function 1_{Γ_F} such that $1_{\Gamma_F}(x,y) = 1$ if $y = F(x)$, and $1_{\Gamma_F}(x,y) = 0$ if $y \neq F(x)$. Knowledge of the graph indicator of a vectorial Boolean function is clearly equivalent to knowledge of the vectorial Boolean function itself; and so this constitutes another way in which vectorial Boolean functions can be represented by Boolean ones.

In fact, the principle behind the representation of an (n,m)-function F by its graph indicator is essentially the same as that of one of the conceptually simplest representations of vectorial Boolean functions. The representation in question consists of explicitly listing the values $F(x) \in \mathbb{F}_2^m$ for every possible input $x \in \mathbb{F}_2^n$, and is known as the **truth table (TT)** representation (strictly speaking, the term "truth table" is used for Boolean functions, whose outputs, 0 and 1, can be interpreted as "true" and "false", respectively; while the same representation for (n,m)-functions with $m > 1$ is typically referred to as a lookup table; since both cases rely on the same principle, we will allow ourselves a slight abuse of terminology, and talk about "truth tables" in the case of vectorial Boolean functions as well). The TT representation is frequently used in the implementation of (n,m)-functions on a computer, since evaluating a function F at a given input x then amounts to simply looking up a value in the table (which is typically represented as an array). An example of the truth-table of a $(3,3)$-function is given in Table 1.1. We thus have e.g. $F(0,1,1) = (1,1,1)$, $F(0,0,1) = (1,0,1)$.

Unfortunately, the TT representation has many shortcomings that make other representations preferable. For one, the TT of an (n,m)-function contains 2^n entries, and each entry consists of m bits. The size of the table is thus at least $2^n \cdot m$ bits. For small values of n and m, this is not a problem; but the size of the TT increases exponentially with n, and for say $n = m = 30$, we will need almost 4 GB of memory to store the table. When working with large values of n and m, other, potentially more compact representations, are typically preferred. Another issue is that the TT reveals very little about the structure of the function. As we shall soon see, properties such as the algebraic degree can be extracted almost immediately from the ANF and the univariate representation; while in the case of the TT, one would have to perform some non-trivial computations

x	$F(x)$
000	000
001	101
010	110
011	111
100	100
101	011
110	001
111	010

Table 1.1: Truth table of a $(3,3)$-function

in order to find the algebraic degree. In practice, these non-trivial computations quite frequently amount to converting the function to a different representation from which the algebraic degree (or other property of interest) can be easily read. One final problem is that the TT representation does not appear to be suitable for expressing general formulas and infinite constructions, or for deriving theoretical properties of functions. All infinite families of APN functions, for instance, are given in terms of the univariate or bivariate representation; to date, there is not a single example of an infinite construction based on the TT.

We now consider how vectorial Boolean functions can be expressed as polynomials; these representations are some of the most convenient and frequently used in the literature. Any (n,m)-function can be uniquely represented as a polynomial in n variables $x_1, x_2, \ldots, x_n$ taking values in $\mathbb{F}_2$, with coefficients $a_I \in \mathbb{F}_2^m$, of the form

$$F(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{i \in I} x_i. \tag{1.1}$$

This is known as the **algebraic normal form (ANF)** of F. For example, the function given by the TT in Table 1.1 has the ANF

$$\begin{aligned} F(x_1, x_2, x_3) = (0,1,1)x_1x_2 + (0,1,0)x_1x_3 + (1,0,0)x_2x_3 + \\ (1,0,0)x_1 + (1,1,0)x_2 + (1,0,1)x_3. \end{aligned} \tag{1.2}$$

Note that, as usual, we do not write terms having a zero coefficient. For the function from the example, the ANF in (1.2) is not significantly shorter than the representation in Table 1.1. Nonetheless, if an (n,m)-function F has very few terms with a non-zero coefficient in its ANF, the latter will be a very compact representation of F; and this will be particularly prominent when the values of n and m are large. As a simple example, we can define an infinite family of $(n,1)$-functions $F(x_1, x_2, \ldots, x_n) = x_1x_2$ for any natural number n; the ANF will always consist of the single term x_1x_2, while the size of the TT will grow exponentially with n.

Let F be an (n,m)-function for some natural numbers n, m. The degree of its ANF (as a multivariate polynomial) is called the **algebraic degree** of F, and is denoted by $\deg(F)$. In other words, the algebraic degree is the size of the largest term with a non-zero coefficient in the ANF. The function from (1.2) has three terms of size two, viz. x_1x_2, x_1x_3, and x_2x_3; and three terms of size one, viz. x_1, x_2, and x_3. Its algebraic degree is thus 2. The algebraic degree of a function is an important property, and it has

cryptographic significance: it should be high in order to resist cube and higher-order differential attacks [40, 55]. As we can see, the algebraic degree of a function can be extracted from its ANF by direct observation; while in the case of the TT representation, there is no straightforward way to do so.

A related concept is that of the minimum degree, introduced in [25]. The **minimum degree** of an (n,m)-function F, denoted by $\min d^\circ(F)$, is the smallest among the algebraic degrees of all component functions of F.

If an (n,m)-function F is of algebraic degree at most 1, resp. 2, resp. 3, then it is called **affine**, resp. **quadratic**, resp. **cubic**. It is not difficult to see that any affine (n,m)-function F satisfies

$$F(x)+F(y)+F(z)=F(x+y+z) \tag{1.3}$$

for any $x,y,z \in \mathbb{F}_2^n$; thus, the definition of affinity in terms of the algebraic degree expresses the same familiar notion of affinity that one would expect. If F is affine and satisfies $F(0)=0$, then it is called **linear**; clearly, a linear (n,m)-function F satisfies

$$F(x)+F(y)=F(x+y)$$

for any $x,y \in \mathbb{F}_2^n$. Once again, this is a linear function in the same sense that one would expect, and so all notions and approaches from linear algebra can easily be adapted to the case of linear (n,m)-functions.

A **purely quadratic** function (or homogeneous quadratic function) is a quadratic function that has no linear or constant terms. As we shall see in Section 1.3, adding linear and constant terms to a function F always results in a function EA-equivalent to F, and so we can usually restrict any computational search or theoretical argument involving quadratic functions to the subclass of purely quadratic functions.

In our study of (n,m)-functions, we typically concentrate on the case when $n=m$. This is arguably the most important and well-studied special case of (n,m)-functions besides the Boolean $(n,1)$-functions. In the case of cryptography, at least, it is easy to see why this is so: in the process of encrypting a block of data, one usually wants to replace this block with a block of the same length; and so, it makes the most sense for the vectorial Boolean functions in the design of a block cipher to have the same number of input and output bits. Of course, (n,m)-functions with $n \neq m$ are used in block ciphers as well; indeed, one need look no further than the well-known Data Encryption Standard (DES) in order to find examples of $(6,4)$-functions (see e.g. [61]). However, unless a specific cipher design is considered or there is some particular reason dictating the choice of $n \neq m$, (n,n)-functions are a natural choice. In fact, two of the most important constructions of block ciphers at present are Feistel networks and Substitution Permutation Networks (SPN) (see e.g. [34] or [61] for some basic background on the general design of block ciphers). In a Feistel network, the underlying vectorial Boolean functions do not have to be permutations (or even injective), and so, in particular, the dimensions of their domain and co-domain can take many different combinations of values (although certain other properties may have to be imposed on them in order to make sure that the resulting cipher is secure; one such possibility could be to use balanced functions, although there can be other options as well [63]). The aforementioned DES is an example of a cipher based on a Feistel network. The (n,m)-functions used in an SPN, on the other hand, must necessarily be permutations; in particular, we must

have $n = m$. This is one of the main practical considerations that make the "big APN problem" of finding APN (n,n)-permutations for even values of n so important (see Section 1.2.3 below for a bit more on the "big APN problem"). The Rijndael cipher, for instance, was selected as the Advanced Encryption Standard (AES) by the U.S. National Institute of Standards and Technology (NIST) [38, 39], and is currently one of the most secure and widely used block ciphers. It is an example of a construction based on the SPN model, and is built around an $(8,8)$-permutation with good cryptographic properties.

When $n = m$, we typically use the so-called univariate representation, in which the vector space $\mathbb{F}_2^n$ is identified with the finite field $\mathbb{F}_{2^n}$. Recall that any finite field of extension degree n can be seen (up to isomorphism) as a vector space of dimension n over its prime field; and so, we can use $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ interchangeably. Now, any (n,n)-function can be seen as a function from $\mathbb{F}_{2^n}$ to itself, and can be uniquely represented as a univariate polynomial of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, \tag{1.4}$$

where $a_i \in \mathbb{F}_{2^n}$ for $0 \leq i \leq 2^n - 1$. This is called the **univariate representation** of F. The univariate representation is by far the most widely used in the study of cryptographically optimal (n,n)-functions, since many important instances of e.g. APN functions (including infinite constructions thereof) have a very simple expression in univariate polynomial form. Easily the most eloquent example is the Gold function $F(x) = x^3$, which is known to be APN over $\mathbb{F}_{2^n}$ for any natural number n. Its univariate representation thus consists of a single term; while the sizes of its ANF and TT increase with the dimension n. In fact, the function represented by Table 1.1 and by the ANF in (1.2) is precisely $F(x) = x^3$ for $n = 3$.

Like in the case of the ANF, the univariate representation allows us to compute the algebraic degree of the represented function with only very little effort. In this case, the algebraic degree is equal to the largest binary weight of an exponent i with a non-zero coefficient a_i in the univariate representation. The **binary weight**, or 2-weight, of an integer i, denoted by $w_2(i)$, is the number of non-zero digits in its binary notation; equivalently, $w_2(i)$ is the number of distinct powers of 2 that add up to i. For instance, 19 can be written as $2^4 + 2^1 + 2^0$, or as 10011 in binary; and so $w_2(19) = 3$. Since the univariate representation of the Gold function, $F(x) = x^3$, has a single term with a non-zero coefficient, and since the exponent satisfies $w_2(3) = 2$, we can immediately see that the Gold function is quadratic.

The concept of a component function can also be adapted to the case of the univariate representation with the help of the absolute trace function. Recall that the **trace** from the finite field $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^m}$, where $n = mk$ for some natural number k, is defined as

$$\mathrm{Tr}_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(k-1)m}}$$

for $x \in \mathbb{F}_{2^n}$. The **absolute trace** is simply the trace from $\mathbb{F}_{2^n}$ to the prime field $\mathbb{F}_2$, i.e. Tr_1^n; we will typically write Tr_n as shorthand for Tr_1^n, which we will further simplify to Tr when the dimension n is clear from the context. All component functions of an (n,n)-function F can then be expressed as $F_b : x \mapsto \mathrm{Tr}_n(bF(x))$ for all non-zero $b \in \mathbb{F}_{2^n}$.

Here, the product $bF(x)$ is computed in $\mathbb{F}_{2^n}$, and is then mapped to $\mathbb{F}_2$ via the absolute trace function.

We remark that a univariate polynomial can also be used to express an (n,m)-function for $n \neq m$, as long as $m \mid n$, so that the co-domain of the function is a subfield of the domain. In this case, some additional restrictions need to be applied to the definition of the univariate form in order to ensure its uniqueness. However, we will not go into details, as the dissertation focuses only on the case of (n,n)-functions.

When the dimension $n = 2m$ is even, one can identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, and represent an (n,n)-function as a pair of (n,m)-functions; this is similar to the ANF of an (n,n)-function, except that the input and output are "split" into two coordinates instead of n. More formally, we can write

$$F(x,y) = (f_1(x,y), f_2(x,y)),$$

where $x,y \in \mathbb{F}_{2^m}$ and f_1, f_2 are (n,m)-functions. Furthermore, if β is any element from $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, then $\{1,\beta\}$ forms a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$, and so we can write

$$F(z) = f_1(z) + \beta f_2(z),$$

where $z = (x,y) \in \mathbb{F}_{2^n}$. Then F can be uniquely represented as

$$F(x,y) = \sum_{i,j=0}^{2^m-1} a_{i,j} x^i y^j,$$

with $a_{i,j} \in \mathbb{F}_{2^n}$. This is called the **bivariate representation** of F. Although it may seem a bit less natural to work with than the univariate representation, some important functions having a complicated univariate expression have a fairly simple bivariate one. In fact, some infinite families of APN functions are given in the bivariate representation (for instance, family F12 from Table 1.3 was originally given in bivariate form).

To date, all the known infinite families of APN functions are given in univariate and bivariate form; at the time of writing, infinite constructions via the ANF, TT, or any other representation, have yet to be found.

Vectorial Boolean functions can also be represented by the so-called Walsh transform. We first define the Walsh transform for Boolean functions; the generalization to (n,m)-functions with $m > 1$ is then natural via the component functions. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function for some natural number n. The **Walsh transform** of f is the integer-valued function $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x},$$

where $a \cdot x$ denotes a scalar product on $\mathbb{F}_2^n$ (that is, a symmetric bivariate function on $\mathbb{F}_2^n$ such that $x \mapsto a \cdot x$ is a non-zero linear form for any $0 \neq a \in \mathbb{F}_2^n$). This is typically defined as

$$(a_1, a_2, \ldots, a_n) \cdot (x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i,$$

for $(a_1, a_2, \ldots, a_n), (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, with addition and multiplication in $\mathbb{F}_2$; or as

$$a \cdot x = \mathrm{Tr}_n(ax),$$

for $a, x \in \mathbb{F}_{2^n}$, with the product ax computed in the finite field $\mathbb{F}_{2^n}$. The concrete choice of the scalar product is immaterial, and the properties that we consider do not depend on it. The former definition is usually preferable in computer implementations and when working with vector spaces; while the latter is more convenient if the functions are treated as mappings over finite fields. Note that the component function F_b of an (n,n)-function F for $b \in \mathbb{F}_{2^n}$ can be expressed using the scalar product as $F_b(x) = b \cdot F(x)$; for each of the two concrete choices of the scalar product described above, we get one of the two concrete representations of the component functions that we discussed previously.

Now, let F be an (n,m)-function for some natural numbers n, m. The **Walsh transform** of F is the integer-valued function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ given by

$$W_F(a,b) = W_{F_b}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x},$$

where $F_b : \mathbb{F}_2^n \to \mathbb{F}_2$ is the component function of F given by $b \in \mathbb{F}_2^m$ (note that, although denoted by the same symbol, there are two scalar products in the exponent, one over $\mathbb{F}_2^m$ and one over $\mathbb{F}_2^n$). Thus, the value of $W_F(a,b)$ is simply the Walsh transform of F_b evaluated at a. When working with the finite field representation, the above can be written as

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(bF(x)) + \mathrm{Tr}_n(ax)}.$$

In the particular case when $n = m$, and using the additivity of the trace function, this becomes

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(bF(x) + ax)}.$$

The multiset of all values of W_F is known as the **Walsh spectrum** of F. The multiset of their absolute values, denoted $\mathcal{W}_F$, is called the **extended Walsh spectrum** of F.

As we shall see below, a number of important properties of (n,n)-functions can be expressed using their Walsh transform. In some cases, computing certain properties of a function from its Walsh transform can be significantly faster than doing so from the definition. Furthermore, the extended Walsh spectrum is invariant under CCZ-equivalence [35], and can thus be used to distinguish between distinct CCZ-equivalence classes of functions. Perhaps the most remarkable aspect of the Walsh transform is that it is invertible; that is, if for some (n,m)-function F, one knows the values $W_F(a,b)$ for all $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}$, then one can uniquely reconstruct F. In this way, the Walsh transform constitutes yet another representation of (n,m)-functions (we refer the reader to Sections 2.3.2 and 2.3.6 of [34] for more details).

A matrix representation of purely quadratic (n,n)-functions was introduced in 2014 [71]. A purely quadratic (n,n)-function, by definition, must have a univariate representation of the form

$$F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}.$$

The coefficients $a_{i,j} \in \mathbb{F}_{2^n}$ of the function can be written in a symmetric matrix C_F so that the entry on the i-th row and j-th column of C_F is equal to $a_{i,j}$ (or $a_{j,i}$); all elements on the main diagonal are zero. In this way, a one-to-one correspondence can be established between purely quadratic (n,n)-functions and $n \times n$ symmetric matrices

over $\mathbb{F}_{2^n}$ with zero main diagonal. We note that the same representation was used in the study of quadratic bent functions; see e.g. Section 6. 1. 13 of [34].

Let now $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{2^n}$, and consider an $n \times n$ matrix M with the value $\alpha_j^{2^{i-1}}$ in the i-th row and j-th column. The product $H_F = M^T C_F M$ (where M^T is the transpose of M) then essentially produces a matrix expressing the evaluation of F on all elements of $\mathbb{F}_{2^n}$. In this way (given a fixed basis), there is a one-to-one correspondence between the matrices H_F and the purely quadratic function over $\mathbb{F}_{2^n}$. In [71], a sufficient and necessary condition for F to be APN is given in terms of the matrix H_F. This is then exploited computationally in order to find new instances of APN functions. Up to 2020, when more than 12 000 new APN functions were discovered over $\mathbb{F}_{2^n}$ with $n \leq 10$ [3], this was the largest set of computationally found APN functions, containing more than 8 000 CCZ-inequivalent classes for $n \leq 8$.

One of the results in this dissertation shows how the method from [71] can be adapted to the case of purely quadratic functions with binary coefficients. This allows a classification up to CCZ-equivalence of all APN functions of this type to be performed up to $n = 9$, and is documented in Paper III. For comparison, a full classification of APN functions up to CCZ-equivalence is only available up to $n = 5$ [14]; a classification of cubic APN functions only up to $n = 6$ [56]; and of quadratic APN functions only up to $n = 7$ [53, 56].

The above is by no means a complete list of all possible representations of (n,m)-functions, or even just (n,n)-functions. A promising direction of research for finding new instances of cryptographically optimal functions is to formulate new representations and conduct computational searches over functions that have a simple expression under them. Without going into details, we will only mention as interesting examples the representation of an (n,n)-function by means of the values of its derivatives, developed in some detail in [65]; and the representation of quadratic APN functions by means of an associated algebraic structure [68].

1.2 Cryptographic properties of vectorial Boolean functions

A big advantage of modeling e.g. components of block ciphers via vectorial Boolean functions is that the resistance of the functions against various types of attacks can be objectively measured, and can be used to quantify the strength of the cipher against these attacks. Once a new type of attack is discovered, researchers identify the weaknesses of the functions that make such an attack possible, and define properties that a function must satisfy in order to resist it. In this section, we will look at some of the most important properties of this type, and the classes of functions that attain the optimal values of these properties.

1.2.1 Differential uniformity

Differential cryptanalysis [7] is a powerful attack that exploits statistical dependencies between the inputs and outputs of a function F. We note that the attack is somewhat more complicated than the following description in practice, and takes into account the round structure of the cipher under consideration; since our purpose here is merely to

give the basic idea behind the attack, we restrict ourselves to a more abstract and simplified view. The attacker considers two inputs x_1 and x_2, and the difference $d_x = x_2 - x_1$ between them. He then computes the corresponding outputs $y_1 = F(x_1)$ and $y_2 = F(x_2)$, and the difference $d_y = y_2 - y_1$ (we note that the design of any modern cryptographic cipher, including the exact definition of all underlying functions, is openly known; and a cipher should be secure against attacks regardless). If for some input difference d_x a certain output difference d_y is significantly more likely than others, this can be used by the attacker to gain information about the encryption and, potentially, to break the cipher. In order for a function to be secure against this type of cryptanalysis, the output difference d_y should be as uniformly distributed as possible for any choice of d_x (except for $d_x = 0$, since then $x_1 = x_2$, and the output difference is always equal to 0).

The differential uniformity describes how uniform the output difference is in the worst case, and thereby quantifies the resistance to differential cryptanalysis. Let F be an (n,n)-function for some natural number n. We first define the **(first-order) derivative** D_aF of F in **direction** $a \in \mathbb{F}_{2^n}$ as the (n,n)-function

$$D_aF(x) = F(a+x) - F(x).$$

Since addition and subtraction coincide over a field of characteristic 2, this is usually written as

$$D_aF(x) = F(a+x) + F(x).$$

Now, let $\delta_F(a,b)$ denote the number of solutions $x \in \mathbb{F}_{2^n}$ to the equation

$$D_aF(x) = b,$$

that is,

$$F(x) + F(a+x) = b$$

for $a,b \in \mathbb{F}_{2^n}$. Observe that if we substitute x_1 for x, d_x for a and d_y for b, this is exactly the relation between the inputs and outputs that we described when giving the basic idea of the differential attack. Thus, according to our previous observations, if we fix any $0 \neq a \in \mathbb{F}_{2^n}$, we would like $\delta_F(a,b)$ to be as low as possible for all possible values of $b \in \mathbb{F}_{2^n}$; if $\delta_F(a,b)$ is large for some choice of a and b, this means that the output difference $d_y = b$ is more likely than uniform given $d_x = a$; and so, the cipher would be vulnerable to differential attacks.

The **differential uniformity** Δ_F of an (n,n)-function F is the largest value of $\delta_F(a,b)$ for any $a,b \in \mathbb{F}_{2^n}$ with $a \neq 0$; that is,

$$\Delta_F = \max\{\delta_F(a,b) : a,b \in \mathbb{F}_{2^n}, a \neq 0\}.$$

The multiset of the values $\delta_F(a,b)$ for all $a,b \in \mathbb{F}_{2^n}$ with $a \neq 0$ is called the **differential spectrum** of F; thus, the differential uniformity Δ_F of F is the largest value in its differential spectrum. We also say that an (n,n)-function F is **differentially δ-uniform** for some natural number δ, if $\Delta_F \leq \delta$. From the above, the differential uniformity should be as low as possible in order to have a strong encryption.

Since $D_aF(x) = D_aF(a+x)$ over any field of characteristic 2, $a+x$ is a solution to $D_aF(x) = b$ whenever x is; and so, the numbers $\delta_F(a,b)$ (and hence also the differential uniformity) are always even. The differential uniformity of any (n,n)-function can

therefore never be less than 2. The functions that achieve this lower bound with equality are called **almost perfect nonlinear (APN)**, and, therefore, provide the best possible resistance to differential cryptanalysis. APN functions are the central topic of this dissertation.

As we have seen above, an (n,n)-function F is APN by definition if and only if there are at most two solutions $x \in \mathbb{F}_{2^n}$ to any equation of the form $D_aF(x) = b$ for any $0 \neq a \in \mathbb{F}_{2^n}$ and any $b \in \mathbb{F}_{2^n}$. Equivalently, we can say that F is APN if and only if equality in

$$D_aF(x) = D_aF(y)$$

implies $x = y$ or $x + y = a$ for any $0 \neq a \in \mathbb{F}_{2^n}$ and any $x, y \in \mathbb{F}_{2^n}$. This formulation is sometimes more convenient to work with, and it can lead to simpler characterizations of APN-ness in some cases, such as for quadratic functions. If F is quadratic, then its derivative D_aF is affine (for any $0 \neq a \in \mathbb{F}_{2^n}$) and so $D_aF(x) = D_aF(y)$ is equivalent to $D_aF(x+y) = D_aF(0)$. A quadratic (n,n)-function is then APN if and only if the equation

$$D_aF(x) = D_aF(0)$$

has precisely $x = 0$ and $x = a$ as solutions for any $0 \neq a \in \mathbb{F}_{2^n}$.

It is worth noting that the name "almost perfect nonlinear" may be a bit misleading, as it seems to imply that APN functions are not optimal. In fact, the name alludes to the class of perfect nonlinear (PN) functions, whose differential uniformity is equal to 1; but PN (n,n)-functions only exist over finite fields of odd characteristic, and so the almost perfect nonlinear functions are indeed optimal in the binary case.

1.2.2 Nonlinearity

Another efficient cryptanalytic attack is linear cryptanalysis [57], the idea of which is to approximate a function F used in a block cipher by a linear (or affine) function. Since linear functions are well-structured and behave in a predictable way, it is quite easy for the attacker to analyze a modified version of the cipher in which the linear function is used in place of F; and if this linear function is a good approximation of F, then the results obtained in this way can provide information about the original cipher.

Let us first assume that we have a Boolean function f, i.e. $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ for some natural number n. An affine Boolean function $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a good approximation of f if its outputs match those of f for most input values; that is, if $f(x) = a(x)$ for most $x \in \mathbb{F}_{2^n}$; or, equivalently, if the Hamming distance between f and a is small. Recall that the **Hamming distance** $d_H(F,G)$ between two (n,m)-functions F and G is the number of inputs $x \in \mathbb{F}_2^n$ on which their outputs are different; that is,

$$d_H(F,G) = \#\{x \in \mathbb{F}_2^n : F(x) \neq G(x)\}.$$

In order for the Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ to be resistant to linear cryptanalysis, it should be as far away as possible (in terms of Hamming distance) from all affine $(n,1)$-functions. The **nonlinearity** $\mathcal{NL}(f)$ of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is thus defined as

$$\mathcal{NL}(f) = \min\{d_H(f,a) : a \in \mathcal{A}_n\},$$

where $\mathcal{A}_n$ is the set of all affine $(n,1)$-functions.

The nonlinearity $\mathcal{NL}(f)$ of an $(n,1)$-function f can be expressed using the Walsh transform $W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$. Recall that all affine $(n,1)$-functions are of the form $x \mapsto a\cdot x + c$ for some $a \in \mathbb{F}_2^n$ and some $c \in \mathbb{F}_2$. The expression $f(x)+a\cdot x$ in the exponent of $W_f(a)$ is thus equal to 0 if the values of $x \mapsto a\cdot x$ and $f(x)$ match; and is equal to 1 if these values are different. Consequently, the term $(-1)^{f(x)+a\cdot x}$ is equal to $+1$ if $f(x) = a\cdot x$, and is equal to -1 otherwise. Summing these values for all $x \in \mathbb{F}_2^n$, we can see that $W_f(a) = E - N$, where E is the number of inputs $x \in \mathbb{F}_2^n$ for which $f(x) = a\cdot x$, and N is the number of inputs for which $f(x) \neq a\cdot x$. Since $E+N = 2^n$, we can see that $W_f(a) = 2^n - 2N$, and so $N = 2^{n-1} - \frac{1}{2}W_f(a)$. Taking into account that N is precisely the Hamming distance between f and $x \mapsto a\cdot x$, this means that the minimum distance between f and any linear $(n,1)$-function can be expressed as the smallest value of $2^{n-1} - \frac{1}{2}W_f(a)$ over all $a \in \mathbb{F}_2^n$. On the other hand, it is easy to see that in order to express the distance to the affine function $x \mapsto a\cdot x + 1$, one simply has to flip the sign of the Walsh coefficient in the formula above. We thus get the following important expression of the nonlinearity via the Walsh transform:

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_f(a)|. \tag{1.5}$$

In the case of an (n,m)-function F with $m > 1$, linear cryptanalysis can be successful if one of the component functions F_b is close to an affine $(n,1)$-function, even if F itself has a large Hamming distance to all affine (n,m)-functions. Thus, much like in the case of the Walsh transform, the notion of nonlinearity is extended from Boolean functions to vectorial Boolean functions through their component functions. More precisely, the **nonlinearity** of an (n,m)-function F is the minimum nonlinearity of any component function of F; symbolically:

$$\mathcal{NL}(F) = \min_{0\neq b\in\mathbb{F}_2^m}\mathcal{NL}(F_b).$$

It is then straightforward to extend (1.5) to the case of vectorial Boolean functions as

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n, 0\neq b\in\mathbb{F}_2^m}|W_F(a,b)|. \tag{1.6}$$

From the preceding discussion, the nonlinearity should be as high as possible in order to resist linear cryptanalysis. It can be shown [36, 66] that the nonlinearity of any (n,n)-function F satisfies

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{(n-1)/2}.$$

The class of functions that attain this upper bound with equality are called **almost bent (AB)** functions. From the definition, it is clear that such functions exist only for odd values of n. In the case of even n, functions with nonlinearity $2^{n-1} - 2^{n/2}$ are known, and it is believed that this value is optimal; nonetheless, the question of the exact upper bound in the case of even dimensions remains open.

It can be shown that any AB function is necessarily APN [36] (thus, AB functions provide the best possible resistance to both differential and linear cryptanalysis). The

converse implication is not true, although any quadratic APN (n,n)-function is AB when n is odd [35].

Much as in the case of APN functions, AB functions are the optimal (n,n)-functions with respect to nonlinearity; the name "almost bent" refers to the class of bent functions, which do not exist in the case of our study. To be more precise, it is known that bent (n,m)-functions exist only when $n \geq 2m$ [58]; and so, just like APN functions, AB functions are optimal objects despite the name.

1.2.3 Algebraic degree, and other desirable properties

The algebraic degree of an (n,m)-function F which, as we saw, can be easily computed from both the univariate representation and the ANF, is an important cryptographic property in its own right. More precisely, the algebraic degree should be high in order to resist so-called higher-order differential attacks [40, 55] (to make this more precise, we note that at the time of writing, such attacks have only been successful against quadratic functions; unless an improved attack of this type is introduced, taking functions with algebraic degree 3 or 4 should be sufficient for practical purposes).

In this respect, it is worth noting that most of the known APN and AB functions given in the literature are quadratic (which is the worst possible case from the point of view of the algebraic degree, as an affine function cannot be APN). Nonetheless, APN and AB functions of higher algebraic degree can be obtained from them by means of CCZ-equivalence; as we will see in Section 1.3.1, CCZ-equivalence preserves the differential uniformity and nonlinearity, but not the algebraic degree; and thus, traversing the CCZ-equivalence class of a quadratic APN (or AB) function can lead to APN (or AB) functions of higher algebraic degree.

In addition to the differential uniformity, nonlinearity, and algebraic degree, there are many other properties that are desirable for a function to have from a cryptographic or implementational point of view. Since the results presented in this dissertation concern APN and AB functions (and, thus, differential uniformity and nonlinearity) above all, we will not cover all possible properties; instead, we refer the reader to [34] for an excellent encyclopedic treatment of the subject.

We will only mention the property of a function being bijective, that is, a permutation. As we discussed in Section 1.1, the vectorial Boolean functions used in a Substitution Permutation Network, or SPN, must necessarily be permutations, which is one of the major factors that make bijectivity a desirable property for cryptographic functions. Even outside the context of SPN's, it is intuitively easy to appreciate that permutations correspond to the most natural (in some sense) transformations on bits. Unfortunately, it seems that requiring functions to be bijective (in addition to APN, or AB) makes them much more difficult to find. In the case of even dimensions, there is a single known example (up to CCZ-equivalence) of an APN permutation for $n = 6$, discovered only in 2010 [16]; finding APN permutations for a higher even dimension, or showing that such do not exist, is known as the "big APN problem", and is arguably the most important open problem in the study of APN functions at the moment. In the case of odd dimensions, APN permutations are known (in fact, all of the infinite families of power APN functions given in Table 1.2 are bijective for odd dimensions; and so we actually know infinitely many instances of APN permutations for odd dimensions). De-

spite this, the known instances for any given n are very few, and finding more examples of APN permutations is a difficult problem for odd dimensions as well.

In fact, with the exception of the power APN functions, there is only one known infinite family of APN permutations for odd dimensions, namely family F1-F2 from Table 1.3 whose instances over $\mathbb{F}_{2^n}$ are AB permutations for odd values of n [22]. A conjecture from [35] stated that any AB function is EA-equivalent to a permutation; this was disproved in [25], while the functions from F1-F2 are the earliest known counterexample to the more general conjecture that any quadratic AB function must be CCZ-equivalent to a permutation. Despite them being false, the fact that these two conjectures were formulated in the first place may seem to suggest that the majority of AB functions (and, in particular, quadratic APN functions over fields of odd dimension) are permutations or, at least, equivalent (under EA- or CCZ-equivalence) to permutations. In reality, this is far from true: for instance, we know that among the 491 known CCZ-inequivalent APN functions over $\mathbb{F}_{2^7}$ (which exhaust all possible quadratic APN functions in this dimension as shown in [53]), the only ones CCZ-equivalent to permutations are the power APN functions x^3, x^5, x^9, x^{13}, x^{57}, and x^{126} (Yuyin Yu, personal communication). Furthermore, with the exception of power APN functions, there are only 2 known instances of AB permutations over $\mathbb{F}_{2^9}$ [3]; and, in Paper III, we show that no quadratic APN polynomial (as opposed to monomial) with binary coefficients over $\mathbb{F}_{2^n}$ is CCZ-equivalent to a permutation for $n \leq 9$.

1.3 Equivalence relations on vectorial Boolean functions

One of the major factors that make the study and classification of vectorial Boolean functions so difficult is their extremely large number. More precisely, the number of (n,n)-functions is $(2^n)^{2^n}$, which becomes prohibitively large even for relatively small values of n; for instance, for functions on 4 bits, we already have

$$16^{16} = 18446744073709551616$$

distinct $(4,4)$-functions; furthermore, most cases of practical interest involve values of n significantly larger than 4. For one thing, this makes it clear that searching for e.g. APN functions by means of an exhaustive search is completely out of the question; indeed, computational searches are only done for subclasses of functions and in special cases where a theoretical characterization can speed up the search to a sufficient degree. For another thing, the vast number of (n,n)-functions suggests that the number of e.g. APN, or AB functions (despite them being rather specialized subclasses) is going to be very large as well.

A typical approach in studying and classifying a large number of mathematical objects is to partition them into equivalence classes with respect to a most general suitable equivalence relation, and then consider the objects only "up to equivalence". In our case, a "suitable" equivalence relation would be one that preserves the differential uniformity and nonlinearity (so that any function in the equivalence class of an APN or AB function is itself APN or AB, respectively). Two functions are then considered to be different only if they lie in distinct equivalence classes. Usually, the larger the number of functions in an equivalence class, the easier it is to perform classification,

since then we are left with fewer functions to deal with. In the absence of other considerations, one would thus typically prefer a more general equivalence relation (having larger classes) to a less general one.

The most general currently known equivalence relation that preserves the differential uniformity and the nonlinearity is CCZ-equivalence, and almost all results on the classification of APN and AB functions in the literature are given up to CCZ-equivalence. Another frequently used equivalence relation is EA-equivalence, which is a special (and strictly less general) case of CCZ-equivalence. Nonetheless, the two equivalence relations coincide for some important classes of functions; most notably, two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [69]. This can be potentially advantageous since EA-equivalence can be easier to work with in some cases. There are several further specializations of EA-equivalence (including affine equivalence, linear equivalence, and the so-called "restricted EA-equivalence" [27, 60]) that are of limited significance for the study of APN and AB functions. One special case of EA-equivalence, however, is worth noting, and that is cyclotomic equivalence. This equivalence relation is only applicable to the case of power functions, i.e. it only makes sense to talk about the cyclotomic equivalence of two functions when both of these functions are monomials. While it may seem that such an equivalence relation is too restrictive to be useful in practice, we note that some of the oldest and most important open problems in the area concern power functions. For example, a well-known conjecture by Dobbertin states that representatives from the infinite monomial families in Table 1.2 exhaust all APN monomials up to CCZ-equivalence [43]; and since two monomials are CCZ-equivalent if and only if they are cyclotomic equivalent [70], the notion of cyclotomic equivalence is likely to play a fundamental role in the resolution of this problem. We note that some of our results presented in Paper IX concerning the composition of power functions with linear polynomials might lead to new perspectives and approaches to Dobbertin's conjecture.

1.3.1 CCZ-equivalence

The Carlet-Charpin-Zinoviev equivalence (introduced in [35]), or CCZ-equivalence for short, of two functions is defined in terms of their graphs. Recall that the graph of an (n,n)-function F is the set $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$. The elements of Γ_F are pairs of elements in $\mathbb{F}_{2^n}$, and each such pair can be identified with an element of $\mathbb{F}_{2^{2n}}$; we can thus consider the graph of an (n,n)-function as a set of 2^n elements from $\mathbb{F}_{2^{2n}}$. Now, two (n,n)-functions F and G are said to be **CCZ-equivalent** if there exists an affine permutation A of $\mathbb{F}_{2^{2n}}$ mapping the graph of F to that of G, i.e.

$$\{A(x) : x \in \Gamma_F\} = \Gamma_G. \tag{1.7}$$

At present, CCZ-equivalence is the most general known equivalence relation on (n,n)-functions that preserves the differential uniformity and the nonlinearity; for this reason, APN and AB functions are typically classified up to CCZ-equivalence. The algebraic degree, however, is not invariant under CCZ-equivalence, and this allows one to search for APN and AB functions of high algebraic degree by traversing the CCZ-equivalence classes represented by known functions of a lower algebraic degree. In particular, this can overcome the limitation of most of the known APN and AB functions being quadratic: the CCZ-equivalence class of a quadratic function will typically

contain quite a few representatives of high algebraic degree; for instance, the CCZ-equivalence classes of all known APN functions over $\mathbb{F}_{2^6}$ contain functions of algebraic degree 4 [28]. In this way, CCZ-equivalence can be used constructively to improve the value of one desirable parameter (the algebraic degree) while leaving other desirable properties (being APN, or being AB) unchanged.

In fact, one of the most important results in the study of APN functions was achieved by a similar constructive application of CCZ-equivalence. The question of the existence of APN permutations of $\mathbb{F}_{2^n}$ for even values of n is easily one of the most important open problems in the area. This is one of the oldest problems in the study of APN functions; and it is remarkable that since their formal introduction in the early 90's, not a single instance of an APN permutation for even n was found until 2010, when John Dillon and his colleagues found an APN permutation of $\mathbb{F}_{2^6}$ [16] (see Section 1.6 for some more details, including the univariate form of the APN permutation). Dillon's method involves traversing the CCZ-equivalence class of a known, non-bijective APN function; much like in the case of the algebraic degree, CCZ-equivalence does not preserve the property of being a permutation, and can thus be used to search for permutations equivalent to APN functions that are not themselves bijective. Unfortunately, no further instances of APN (n,n)-permutations for even n have been found since 2010, and so the "big APN problem" remains open for $n > 6$.

Studying APN and AB functions up to CCZ-equivalence significantly reduces the number of functions that have to be considered, and makes their analysis and classification feasible (although still very difficult). However, it does raise the question of how to test whether two given (n,n)-functions F and G are CCZ-equivalent. This becomes necessary, as any tentatively new APN or AB function (originating from a theoretical construction or a computational search) must be shown to be CCZ-inequivalent to all currently known APN or AB functions. While the definition of CCZ-equivalence is quite straightforward, trying to decide the CCZ-equivalence of two given functions F and G is an extremely difficult problem, both computationally and mathematically. On the one hand, theoretical proofs of inequivalence are only possible in some very specific cases, and even then, they can be very technical and involved; one can see examples of such proofs in e.g. [22]. On the other hand, the number of affine permutations of $\mathbb{F}_{2^{2n}}$ is huge, and checking whether (1.7) holds for every such permutation is not practically feasible. Furthermore, the definition of CCZ-equivalence does not suggest any obvious way for testing it besides exhausting all possibilities for the affine permutation A.

In practice, CCZ-equivalence is tested computationally via the isomorphism of linear codes. Given any (n,n)-function F, we can associate with it a matrix over $\mathbb{F}_2$ with $2n+1$ rows and 2^n columns (by identifying the elements of $\mathbb{F}_{2^n}$ with vectors from $\mathbb{F}_2^n$) of the form

$$P_F = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \cdots & \alpha^{2^n-2} \\ F(0) & F(1) & F(\alpha) & \cdots & F(\alpha^{2^n-2}) \end{pmatrix},$$

where α is a primitive element of $\mathbb{F}_{2^n}$; and we can associate with F the linear code C_F having P_F as a parity-check matrix. Then F and G are CCZ-equivalent if and only if their associated codes C_F and C_G are isomorphic [15, 44], i.e. if there exists a permutation π of $\{1,2,\ldots,2^n\}$ such that $(x_1,x_2,\ldots,x_n) \in C_F$ if and only if $(x_{\pi(1)},x_{\pi(2)},\ldots,x_{\pi(n)}) \in C_G$.

Deciding whether the linear codes C_F and C_G are isomorphic is a difficult problem in its own right; the advantage of the above reduction is that coding theory is an old and well studied area, and algorithms and even working implementations of linear code isomorphism tests can be readily found. For example, the *Magma* algebra system [9] that we use for most of our computational experiments includes a built-in implementation of such an isomorphism test; and most other computer algebra systems are not an exception. Thus, the complexity of implementing a CCZ-equivalence test in practice reduces to that of constructing the matrix P_F, constructing the linear code C_F from P_F, and then delegating the rest of the work to an existing function or procedure.

The code isomorphism approach has several drawbacks. First and foremost, it uses a significant amount of memory that grows very quickly with the dimension n. This makes it impossible to test (n,n)-functions for CCZ-equivalence for $n \geq 12$ on our server, which has around 500 GB of memory. Even for lower values of n, the memory consumption (which depends on the concrete pair of functions being tested) can be prohibitive. What is worse, is that some implementations of the test (including the one that we currently have access to) can give false negatives: the isomorphism test returns either "true" or "false"; and if it returns "false", this might be either because the algorithm has exhausted all possibilities and found no possible equivalence between the two functions, or it may be because the implementation has run out of memory. A relatively minor issue is that the running times can be quite long, especially for higher dimensions, e.g. $n = 9$ or $n = 10$, with some tests running for multiple hours before they finish. Despite this, the linear code test is currently the only known way of testing CCZ-equivalence (except, of course, for exhaustive search). Testing CCZ-equivalence can frequently be facilitated by means of invariants (see Section 1.4), although this can only be used to show that two functions are CCZ-inequivalent. In the case of the less general EA-equivalence, a few different algorithms are known that can be used in some cases. As we shall see below, two quadratic APN functions are EA-equivalent if and only if they are CCZ-equivalent; and as we shall see in Section 1.5, the vast majority of known APN and AB functions are quadratic, which means that tests for EA-equivalence can be quite useful in practice as well. More details on testing EA-equivalence are given in the next section.

1.3.2 EA-equivalence

EA-equivalence is short for extended affine equivalence, and is easily the most frequently used notion of equivalence in the study of APN and AB functions after CCZ-equivalence. Two (n,n)-functions F and G are said to be **EA-equivalent** if there exist affine (n,n)-functions A_1, A_2, A, with A_1 and A_2 bijective, such that

$$A_1 \circ F \circ A_2 + A = G. \tag{1.8}$$

By imposing additional restrictions on the three affine functions, some particular cases of EA-equivalence can be obtained. If $A = 0$ in (1.8), we say that F and G are **affine equivalent**. If, in addition, $A_1(0) = A_2(0) = 0$ so that A_1 and A_2 are linear permutations (instead of merely affine), we say that F and G are **linear equivalent**. Additional restrictions lead to a number of further specialized cases of EA-equivalence, grouped under the umbrella term "restricted EA-equivalence" [27, 60]. We will not need any

of these special cases of EA-equivalence in the sequel, and we mention them merely for the sake of completeness, and because, to the best of our knowledge, these were previously the only cases for which algorithms operating from first principles (that is, not relying on e.g. auxiliary coding theory algorithms) were known.

EA-equivalence is a special case of CCZ-equivalence, and it is known that CCZ-equivalence is strictly more general than EA-equivalence combined with taking inverses of permutations [25]. Nonetheless, perhaps the most important fact about EA-equivalence from the point of view of the study of APN and AB functions is that it coincides with CCZ-equivalence in the case of quadratic APN functions [69]; that is, if F and G are both APN (n,n)-functions of algebraic degree 2, then F and G are CCZ-equivalent if and only if they are EA-equivalent (EA-equivalence also coincides with CCZ-equivalence in the case of power functions, but then both notions of equivalence reduce to that of cyclotomic equivalence [70], which is handled in Section 1.3.3). Since the vast majority of known APN and AB functions are quadratic (see Section 1.5), this means that being able to test two functions for EA-equivalence is almost as useful in practice as being able to test them for CCZ-equivalence.

Unfortunately, no simple algorithm is known for deciding the EA-equivalence of two given functions in the general case either. In [44], it is shown how the same approach via linear codes that is used in the CCZ-equivalence test can be adapted to the case of EA-equivalence; the only difference is that the form of the parity-check matrix P_F associated with an (n,n)-function F is different and, therefore, defines a different linear code. Regretfully, this approach does not make the test easier; on the contrary, the linear codes involved in the EA-equivalence test have a larger length and more complicated structure than those used for testing CCZ-equivalence. The known algorithms that operate from first principles are only applicable to the so-called "restricted EA-equivalence" [27, 60] and are, unfortunately, of limited practical use in the classification of APN and AB functions.

Very recently, a new algorithm for testing the EA-equivalence of two given quadratic functions has been proposed based on the so-called Jacobian matrices of the functions [31]. The algorithm appears to provide running times comparable to our approach from Paper V for even dimensions n, but the two algorithms are based on fundamentally different principles; they were developed independently, and were published as preprints and conference proceedings at roughly the same time. Furthermore, the algorithm from [31] is only applicable to quadratic functions, but can be used for any dimension n; while the one from Paper V works for vectorial Boolean functions of any algebraic degree, but can only be used in practice for even dimensions (although its running time increases by a factor of 2^n if the functions being tested are not quadratic).

In Paper V, we present an algorithm for testing the EA-equivalence of two given functions over $\mathbb{F}_{2^n}$ for even values of n. The algorithm operates from first principles, i.e. without making use of code isomorphism or other non-trivial properties, and can be implemented very easily on any general-purpose programming language. It has several other advantages, among which are the fact that it can be parallelized very easily and naturally, and that it gives rise to a useful invariant under EA-equivalence (described in Section 1.4.2 below) which is computed as a part of the algorithm. To the best of our knowledge, this is the first algorithm (along with the one from [31]) for testing EA-equivalence (even if only in even dimensions) that does not rely on linear code isomorphism and does not make any assumptions about the functions A_1, A_2, A

from (1.8). In fact, the algorithm works correctly for odd values of n as well, but then it defaults to an exhaustive search over all possible choices of A_1 and A_2 from (1.8) which is not feasible to do for large dimensions.

An important difference between CCZ- and EA-equivalence is that the latter preserves the algebraic degree, while the former does not; this largely limits the degree to which EA-equivalence can be used constructively. On the other hand, like CCZ-equivalence, EA-equivalence does not preserve the property of being a permutation; however, it has been shown that a quadratic APN function over a finite field of even dimension cannot be bijective [51], which restricts the possibility of obtaining APN permutations in this manner to the case of odd dimensions.

1.3.3 Cyclotomic equivalence

The final equivalence relation that we consider is rather specialized, as it can only be applied to the case of power functions. Let $F(x) = x^d$ and $G(x) = x^e$ be two (n,n)-power functions for some natural numbers d, e, n. We say that F and G are **cyclotomic equivalent** if there exists a natural number k such that

$$2^k \cdot d \equiv e \pmod{2^n - 1}, \tag{1.9}$$

or

$$2^k \cdot d^{-1} \equiv e \pmod{2^n - 1}, \tag{1.10}$$

where d^{-1} is the multiplicative inverse of d modulo $2^n - 1$ (if it exists). What makes this seemingly highly specialized notion of equivalence significant is that it coincides with CCZ-equivalence (and also with EA-equivalence) in the case of power APN functions [70]; that is, two power APN functions x^d and x^e are CCZ-equivalent if and only if they are cyclotomic equivalent.

Furthermore, in contrast to both CCZ- and EA-equivalence, deciding whether a given pair of power functions x^d and x^e is cyclotomic equivalent is quite easy, and amounts to checking whether (1.9) and (1.10) have solutions.

1.4 Invariants

An invariant for some given equivalence relation is a property that is preserved by the equivalence relation. For example, the differential uniformity and nonlinearity are invariants for CCZ-equivalence, which means that if F and G are two CCZ-equivalent (n,n)-functions, then $\Delta_F = \Delta_G$ and $\mathcal{NL}(F) = \mathcal{NL}(G)$. Indeed, this is the reason that functions with low differential uniformity (and APN functions, in particular) can be meaningfully classified up to CCZ-equivalence. However, there are many different invariants under CCZ-equivalence (and also under EA-equivalence) that can take a multitude of distinct values even among functions that have the same differential uniformity or nonlinearity. These are important tools for facilitating the classification of e.g. APN functions up to CCZ-equivalence and EA-equivalence.

First, if two (n,n)-functions F and G have different values of some given CCZ-invariant, then we can immediately conclude that they are not CCZ-equivalent. Second, if a tentative new instance of an e.g. APN function is found, it only has to be tested

for CCZ-equivalence against those known functions that have the same exact values of the known invariants as the newly discovered function. In this way, the study and computation of invariants allows one, in some cases, to show that two functions are inequivalent without having to perform any equivalence tests at all; and, even if a test is necessary, invariants can help reduce the number of functions that need to be tested. Furthermore, most invariants are concrete numerical values, and many of them have a natural interpretation related to the structure and properties of the function; this makes it easy to preclude the possibility of false positives or negatives such as in the case of testing CCZ- or EA-equivalence via linear codes.

In the following, we list some of the most frequently used CCZ- and EA- invariants, and comment on their advantages and disadvantages for the purpose of classifying APN (and AB) functions. Some important properties that an invariant should have in order to be useful in practice are that it should be easy to define and implement, efficient to compute, and it should take many different values for distinct equivalence classes of functions, so that it has good distinguishing capability.

One of the important scientific results presented in this dissertation is, in fact, a new invariant for APN functions. This is the multiset Π_F from Paper II, which can be used to derive a lower bound on the distance from a given APN function to a closest (in terms of Hamming distance) APN function. A more detailed introduction to the paper and its results is given in Section 1.7.2, and a brief description of the multiset Π_F is presented in Section 1.4.1 below.

Another invariant introduced as part of our scientific results is the multiset of multiplicities of Σ_F^k which is computed as part of the algorithm for testing EA-equivalence introduced in Paper V. The aforementioned multiset of multiplicities is invariant under EA-equivalence, and is described in more detail in Section 1.4.2, while a more systematic description of the entire algorithm is given in Section 1.7.5.

1.4.1 Invariants under CCZ-equivalence

As mentioned above, the differential uniformity (in fact, the whole differential spectrum) and the nonlinearity are invariant under CCZ-equivalence, which justifies the use of the latter as a tool for classifying APN and AB functions. With respect to distinguishing between CCZ-inequivalent APN and AB functions, however, these invariants are not useful, as any APN and AB function has a fixed value of the differential uniformity and nonlinearity by definition (more precisely, any APN function has differential uniformity equal to 2, and any AB function has nonlinearity equal to $2^{n-1} - 2^{(n-1)/2}$). In principle, the nonlinearity could be used to distinguish between CCZ-inequivalent classes of APN functions; however, on account of (1.6), the nonlinearity $\mathcal{NL}(F)$ of an (n,n)-function F can be derived from its extended Walsh spectrum $\mathcal{W}_F$, and so any distinguishing capability of the nonlinearity is subsumed by that of the extended Walsh spectrum.

The extended Walsh spectrum

The extended Walsh spectrum itself is one of the earliest known CCZ-invariants [35], and can be implemented and computed easily and efficiently. Unfortunately, it can take only a limited amount of distinct values over the known APN functions, and is thus not

very useful for distinguishing between CCZ-equivalence classes. To be more precise: we now know more than 20 000 CCZ-inequivalent APN functions over $\mathbb{F}_{2^8}$ (see Section 1.6 for more details), but they can take only 6 distinct values of the extended Walsh spectrum. Furthermore, all APN instances belonging to the known infinite polynomial (as opposed to monomial) families have a Gold-like extended Walsh spectrum, i.e. they have the same extended Walsh spectrum as the Gold power functions. Finally, in all dimensions n in the range $6 \leq n \leq 10$ other than $n = 8$, the extended Walsh spectrum of all known APN functions can take only two values, with virtually all functions having a Gold-like Walsh spectrum, and one or two functions taking the other value.

Despite this, the extended Walsh spectrum is far from useless when it comes to computing invariants. Many important properties of a function (including the values of many of the invariants listed below) can be expressed in terms of the Walsh transform, and it is often the case that computing them from the Walsh transform is significantly faster than from, say, the univariate representation. This makes the computation of the Walsh spectrum (and extended Walsh spectrum) a natural first step in analyzing and classifying a function. Furthermore, the extended Walsh spectrum (as well as the differential spectrum) can be very useful for distinguishing between EA-inequivalent functions by means of their orthoderivatives (see Section 1.4.2 below).

Design invariants

An **incidence structure** is a triple $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P} = \{p_1, p_2, \ldots, p_m\}$ is a set of points (for some natural number m), $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ is a set of blocks (for some natural number n), and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is an incidence relation. We typically assume that the blocks are subsets of $\mathcal{P}$, and that the incidence relation $\mathcal{I}$ is set membership. The notion of an incidence structure is quite natural and general; they occur in a lot of contexts under several different names, and the field of combinatorial design theory (from where the invariants described in this section originate) studies particular incidence structures called block designs. We can associate to any incidence structure a so-called **incidence matrix**, which is a binary $m \times n$ matrix M representing the incidence relation $\mathcal{I}$. More precisely, for any i, j in the range $1 \leq i \leq m$ and $1 \leq j \leq n$, the element $M_{i,j}$ on the i-th row and j-th column of M is equal to 1 if $(p_i, b_j) \in \mathcal{I}$; and is equal to 0 otherwise. We refer to [5, 37] for more background on incidence structures and combinatorial designs.

Given any (n,n)-function F for a natural number n, we can associate two designs with it [46]. The set of points in both cases is simply $\mathbb{F}_{2^n}^2$, that is, the set of all pairs of elements from the corresponding finite field. The first design is denoted by $dev(G_F)$, and its blocks are of the form

$$\{(x + a, F(x) + b) : x \in \mathbb{F}_{2^n}\}$$

for $a, b \in \mathbb{F}_{2^n}$. The second design is denoted by $dev(D_F)$, and its blocks are the sets

$$\{(x + y + a, F(x) + F(y) + b) : x, y \in \mathbb{F}_{2^n}\}$$

for $a, b \in \mathbb{F}_{2^n}$. The rank of the incidence matrix of $dev(G_F)$ is called the **Γ-rank** of F, and the rank of the incidence matrix of $dev(D_F)$ is called the **Δ-rank** of F. The Γ- and Δ-rank are shown to be invariant under CCZ-equivalence, and are two of the currently most widely used invariants in practice.

The orders of the automorphism groups of $dev(G_F)$ and $dev(D_F)$ are also CCZ-invariant, but their computation is only feasible for small dimensions, and so they are not quite as useful as the Γ- and Δ-rank. Nonetheless, these automorphism groups give rise to a CCZ-invariant that can be quite useful in practice: the order of the so-called multiplier group. The **multiplier group** is the subgroup of the automorphism group of $dev(G_F)$ consisting of automorphisms of a special form (the actual definition is slightly technical, and does not contribute anything to the discussion as far as our scientific results are concerned, so we do not give it here; instead, we refer the reader to the original paper [46] for the exact definition). The order of the multiplier group, denoted by $\mathcal{M}(G_F)$, is invariant under CCZ-equivalence, and can be computed much more efficiently than the order of the full automorphism group. We shall refer to all invariants arising from the designs $dev(G_F)$ and $dev(D_F)$ as the "design invariants".

A disadvantage of these invariants is that their implementation is somewhat complicated. In particular, the computation of the Γ- and Δ-rank involves computing the rank of a $2^{2n} \times 2^{2n}$ matrix, which is a laborious computation even for relatively small values of n. A natural implementation via e.g. Gaussian elimination is not efficient enough to be used in practice, and so more sophisticated algorithms have to be used whose implementation is far from straightforward. In practice, this means that computing these invariants requires software tools implementing such algorithms, and restricts the choice of programming languages that can be used. Fortunately, computer algebra systems such as *Magma* typically include very good implementations of such procedures. On the other hand, the calculation of these invariants is a very difficult computational problem per se, and using better and more efficient implementations can only facilitate it so much; thus, even with the advantage of a high-quality implementation, these computations are only feasible in practice in the case of small dimensions. Indeed, the time and memory complexity of the computations grow rapidly with the dimension n. Between the two, the memory consumption is by far the most problematic: computing Γ- and Δ-ranks in *Magma* on our department server (which has around 500 GB of memory) is possible only for (n,n)-functions with $n \leq 10$; for higher dimensions, this amount of memory is no longer sufficient. The running times can also be quite long, with computations lasting up to 10 days in the case of some functions over $\mathbb{F}_{2^{10}}$.

Despite these shortcomings, the design invariants are some of the most frequently used in practice due to their good distinguishing power. For instance, among the known 491 CCZ-inequivalent APN functions over $\mathbb{F}_{2^7}$, the Γ-rank can take 14 distinct values; the Δ-rank can take 6 distinct values; the order of the multiplier group can take 5 distinct values; and, together, these three invariants can take 20 distinct triples of values. In contrast to the extended Walsh spectrum, this is a very useful invariant for distinguishing between CCZ-inequivalent functions, and has been frequently used in practice to justify that newly found constructions and instances of APN functions are CCZ-inequivalent to the known ones. In fact, in Paper IV we construct a new infinite family of APN quadrinomials, and use the Γ-rank to show that its instances for $n = 10$ lie outsides the CCZ-equivalence classes of all known functions in that dimension.

The distance invariant

One of the results presented in Paper II is a lower bound on the distance between a given APN function F and a closest to it (in terms of Hamming distance) APN function. In

order to calculate this lower bound, one first computes a multiset Π_F associated with the function F. If we denote the smallest non-zero value in Π_F by m_F, then the lower bound on the Hamming distance is $\lceil m_F/3 \rceil + 1$. More details are given in Section 1.7.2 below.

Surprisingly enough, the multiset Π_F is an invariant under CCZ-equivalence for APN functions. In other words, if F and G are CCZ-equivalent APN functions over $\mathbb{F}_{2^n}$ for some natural number n, then $\Pi_F = \Pi_G$; note, however, that if F' and G' are CCZ-equivalent with $\Delta_F > 2$, then Π_F and Π_G can, in general, be distinct.

To define the multiset Π_F, we first introduce some auxiliary notation. Let F be an (n,n)-function, and let $b,c \in \mathbb{F}_{2^n}$. We denote by $\pi_F(b,c)$ the number of elements $a \in \mathbb{F}_{2^n}$ for which the equation $F(x)+F(a+x)+F(a+c)=b$ has solutions $x \in \mathbb{F}_{2^n}$, i.e.

$$\pi_F(b,c) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n}) F(x)+F(a+x)+F(a+c)=b\}.$$

The multiset Π_F is then defined as

$$\Pi_F = \{\pi_F(b,c) : b,c \in \mathbb{F}_{2^n}\}.$$

Furthermore, it is shown in the paper that if F is quadratic, we have

$$\{\pi_F(b,c) : b \in \mathbb{F}_{2^n}\} = \{\pi_F(b,c') : b \in \mathbb{F}_{2^n}\}$$

for any $c,c' \in \mathbb{F}_{2^n}$, and so in the quadratic case it is enough to compute the multiset

$$\Pi_F^0 = \{\pi_F(b,0) : b \in \mathbb{F}_{2^n}\},$$

whose computation is much simpler since we only have to go through all values of $b \in \mathbb{F}_{2^n}$ (instead of going through all values of both $b \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^n}$ as in the general case). Once Π_F (or Π_F^0 in the quadratic case) is computed, it remains to find its minimum value m_F and to compute the value of the lower bound as $\lceil m_F/3 \rceil + 1$.

The implementation of this invariant requires nothing more than elementary arithmetic operations (amounting to addition in a finite field, and counting the number of solutions to an equation), and is thus quite simple. The computation is rather efficient, too, especially in the quadratic case, where the computation of Π_F^0 for $n = 11$ still takes less than a second. Finally, Π_F has very good distinguishing properties: for the 21 103 CCZ-inequivalent quadratic APN functions over $\mathbb{F}_{2^8}$ given in [3] and [71], it takes 19 367 distinct values. It is worth noting, however, that Π_F takes the same value on all APN functions belonging to the currently known polynomial (as opposed to monomial) infinite families. Finding an infinite polynomial APN construction with instances having a different value of Π_F is thus an interesting open problem.

1.4.2 Invariants under EA-equivalence

Since EA-equivalence is a special case of CCZ-equivalence, any invariant under CCZ-equivalence is also an invariant under EA-equivalence. When classifying APN and AB functions, however, EA-equivalence is mostly used as an intermediate step towards a classification under CCZ-equivalence, and so this is not helpful.

The algebraic degree $\deg(F)$ and minimum degree $\min d^\circ(F)$ (as long as it is greater than 1) are invariant under EA-equivalence. Since most of the known constructions

and methods (both mathematical and computational) produce quadratic functions, the algebraic degree and minimum degree are of rather limited use when it comes to classifying new instances of APN functions. They can, however, be useful in theoretical arguments and proofs of inequivalence. For instance, the first infinite families of APN and AB functions that are EA-inequivalent to monomials are constructed in [22], and the minimum degree plays a crucial role in the theoretical proof of this inequivalence.

Subspaces in the non-bent components

Recall that a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called **bent** if its non-linearity equals $2^{n-1} - 2^{n/2-1}$; equivalently, f is bent if and only if its Walsh transform satisfies $W_f(a) = \pm 2^{n/2}$ for any $a \in \mathbb{F}_{2^n}$. Given an (n,n)-function F, we define the set $\mathcal{S}_F$ of its non-bent components, i.e.

$$\mathcal{S}_F = \{b \in \mathbb{F}_{2^n} : F_b \text{ is not bent}\}.$$

Using the Walsh transform, this can be expressed as

$$\mathcal{S}_F = \{b \in \mathbb{F}_{2^n} : (\exists a \in \mathbb{F}_{2^n}) W_F(a,b) \neq \pm 2^{n/2}\}$$

or, equivalently, as

$$\mathcal{S}_F = \{b \in \mathbb{F}_{2^n} : (\exists a \in \mathbb{F}_{2^n}) W_F(a,b) = 0\}$$

in the case that F is quadratic.

Denoting by $n_F(i)$ the number of i-dimensional linear subspaces in $\mathcal{S}_F$, the value $n_F(i)$ is invariant under EA-equivalence for any natural number i (as observed independently in [17] and in [49]). This follows from the fact that if $G = A_1 \circ F \circ A_2 + A$ (where F and G are (n,n)-functions, and A_1, A_2, and A are as in (1.8)), then $b \in \mathcal{S}_F$ if and only if $A_1'(b) \in \mathcal{S}_G$, where $A_1'(x)$ is the adjoint operator of $A_1(x) + A_1(0)$. We recall that if L is a linear (n,n)-function, then its adjoint with respect to the scalar product "$\cdot$" is the (n,n)-function L^* satisfying $x \cdot L(y) = L^*(x) \cdot y$ for any $x, y \in \mathbb{F}_{2^n}$.

Instead of a single invariant, we thus have an entire "family" of invariants: one for every natural number i. Furthermore, it is clear that if $n_F(i) = 0$ for some i, then $n_F(j) = 0$ for all $j > i$ as well; thus, given an (n,n)-function F, it is possible to compute the entire vector $N_F = (n_F(1), n_F(2), \ldots, n_F(i))$, where i is the smallest natural number for which $n_F(i) = 0$, and to use this vector for distinguishing between EA-inequivalent functions.

A drawback of this invariant is that it is only useful when n is even. In the case of odd dimensions, any quadratic APN function is AB, and so

$$\{W_F(a,b) : a \in \mathbb{F}_{2^n}\} = \{0, \pm 2^{(n+1)/2}\}$$

for any $0 \neq b \in \mathbb{F}_{2^n}$. Consequently, none of the components of F are bent, i.e. $\mathcal{S}_F = \mathbb{F}_{2^n}$, and N_F has no distinguishing power.

In the case of even dimensions, however, N_F can be a rather useful invariant. To begin with, its implementation is fairly straightforward, and does not involve anything more complicated than computing the Walsh transform, checking whether a tentative subspace is closed under finite field addition, and counting the number of such subspaces; all of these can be readily implemented via standard arithmetic operations in

any general-purpose programming language. The running time is quite reasonable as well: for $n \leq 8$, it is practically negligible, for $n = 10$, it is about 10 seconds, and for $n = 12$, around 20 minutes.

The distinguishing power of N_F is quite good; for instance, for the 21 103 known quadratic APN functions over $\mathbb{F}_{2^8}$, it takes 2 150 distinct values.

The thickness spectrum

The set of Walsh zeros of an (n,n)-function F is defined as

$$\mathcal{Z}_F = \{(a,b) : a,b \in \mathbb{F}_{2^n}, W_F(a,b) = 0\} \cup \{(0,0)\}.$$

The **thickness** of a linear subspace $V \subset \mathcal{Z}_F$ is defined as the dimension of the projection of V onto $\{(0,x) : x \in \mathbb{F}_{2^n}\}$. If we denote by $t_F(i)$ the number of n-dimensional subspaces of $\mathcal{Z}_F$ of thickness i, then $t_F(i)$ is invariant under EA-equivalence for any natural number i [32]. As in the case of the non-bent subspaces, if $t_F(i) = 0$ for some i, then also $t_F(j) = 0$ for all $j > i$, and so a vector $T_F = (t_F(1), t_F(2), \ldots, t_F(i))$ can be computed that completely describes the thickness of all n-dimensional subspaces of $\mathcal{Z}_F$, where i is the smallest natural number for which $t_F(i) = 0$. This vector T_F is called the **thickness spectrum** of F.

Computing the thickness spectrum is fairly straightforward. The set $\mathcal{Z}_F$ can be computed immediately from the Walsh transform of F, and computing the thickness of a subspace is a trivial operation that amounts to counting the number of elements contained in its projection. The most computationally heavy part is finding all n-dimensional subspaces of $\mathcal{Z}_F$; as in the case of N_F, there is no obviously better way of doing this than by exhaustive search. This does not, however, mean that the invariant cannot be efficiently computed with a good implementation. Computation times for $n = 10$ are only around 9-10 seconds, and for $n = 9$ they are around 200 seconds. It is worth noting that, as the previous example illustrates, the computation of this invariant is slower for odd dimensions. The distinguishing power of T_F is also quite reasonable; for the 21 103 quadratic APN functions from [3] and [71], it takes 256 distinct values, and thus can distinguish between distinct EA-equivalence classes of functions rather well.

The zero-sum invariants

The multiset Σ_F^k associated with an (n,n)-function F is defined in Paper V as part of an algorithm for computationally testing EA-equivalence. The multiplicities of the elements of Σ_F^k are invariant under EA-equivalence for any even natural number k, and they are used in the algorithm (with $k = 4$) to extract information about the form of A_1 from (1.8). The multiset is defined as

$$\Sigma_F^k = \left\{ \sum_{i=1}^{k} F(x_i) : x_1, x_2, \ldots, x_k \in \mathbb{F}_{2^n}, \sum_{i=1}^{k} x_i = 0 \right\}.$$

If we denote by $m_F^k(s)$ the multiplicity of $s \in \mathbb{F}_{2^n}$ in Σ_F^k, we can express it using the Walsh transform as

$$m_F^k(s) = \frac{1}{2^{2n}} \sum_{a,b \in \mathbb{F}_{2^n}} (-1)^{b \cdot s} W_F^k(a,b).$$

This approach has the advantage that the complexity of computing the multiplicities does not depend on k. In this way, the invariant is efficiently computable for any value of k.

The distinguishing capability of this invariant for all known quadratic APN functions for $k = 4$ coincides with that of Π_F in Section 1.4.1. Indeed, it is not difficult to see that if F and G are quadratic APN (n,n)-functions, then Σ_F^4 and Π_F^0 express the same quantities. However, the invariants Σ_F^k and Π_F are quite different: for one, Π_F is invariant under CCZ-equivalence, and only for APN functions; while Σ_F^k is invariant under EA-equivalence for any pair of (n,n)-functions. Furthermore, Σ_F^k encodes information about the EA-equivalence class of F, while Π_F does not (instead, it allows one to estimate the Hamming distance from F to a closest APN function to it).

Orthoderivatives

Orthoderivatives were introduced very recently [62, 31], and appear to induce EA-invariants with extremely good distinguishing capability, to the point of having almost the same strength as an actual EA-equivalence test in practice. Given an (n,n)-function F, an **orthoderivative** of F is any non-zero (n,n)-function ω_F (we note that the orthoderivative of F is denoted by π_F in [62], but here we denote it by ω_F to avoid confusion with the sets $\pi_F(b,c)$ from the definition of the multiset Π_F described in Section 1.4) such that, for any $a \in \mathbb{F}_{2^n}$, we have

$$\omega_F(a) \cdot (F(x) + F(a+x) + F(a) + F(0)) = 0$$

for all $x \in \mathbb{F}_{2^n}$. While orthoderivatives can be defined for any (n,n)-function, it can be shown that a quadratic function F is APN if and only ω_F is uniquely defined; and, in this case, the orthoderivatives ω_F and ω_G of two EA-equivalent (n,n)-functions F and G are EA-equivalent themselves. While a number of EA-invariants (such as the differential spectrum) are meaningless in the case of APN and AB functions, the orthoderivative of an APN function is not necessarily APN itself (in fact, we do not currently know of any case when the orthoderivative of an APN function is APN), and so e.g. the differential spectrum becomes useful for distinguishing between EA-inequivalent APN functions. The orthoderivatives tend to take a large number of distinct values of i.a. the differential spectrum and the extended Walsh spectrum, which can be computed very efficiently. Furthermore, the orthoderivative of a given quadratic APN function can be found very quickly, even by just implementing an exhaustive search for its values: computing ω_F for a $(12,12)$-function along with its Walsh spectrum and differential spectrum can still be performed in less than a second using a straightforward implementation.

What is most remarkable is that the Walsh spectra and differential spectra of the orthoderivatives take distinct values on almost all known EA-inequivalent classes of quadratic APN functions (the only known exception are the Gold functions x^{2^i+1}, for which the differential spectrum of the orthoderivative can be the same for distinct choices of i). This means that the orthoderivatives can be used as an EA-equivalence test in practice. Of course, as with any invariant, the orthoderivatives can only be used to show that two (n,n)-functions are EA-inequivalent; even if the values of all invariants for some two orthoderivatives ω_F and ω_G coincide, this cannot constitute a formal

Family	Exponent	Conditions	Algebraic degree	Source
Gold	2^i+1	$\gcd(i,n)=1$	2	[48, 59]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[52, 54]
Welch	2^t+3	$n=2t+1$	3	[42]
Niho	$2^t+2^{t/2}-1$, t even $2^t+2^{(3t+1)/2}-1$, t odd	$n=2t+1$	$(t+2)/2$ $t+1$	[41]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[4, 59]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[43]

Table 1.2: Known infinite families of APN power functions over $\mathbb{F}_{2^n}$

proof of the EA-equivalence of F and G. In practice, this is not such a big problem, as one typically wants to demonstrate the inequivalence rather than the equivalence of some given pair of functions (for instance, in order to show that a newly discovered APN instance is EA- or CCZ-inequivalent to all currently known ones).

1.5 Known infinite families of APN and AB functions

Although the notion of an APN function was introduced already in the early 90's, and constructing infinite families of APN and AB functions is one of the main goals of research in the area, there are very few such constructions known to date. As we shall later see in Section 1.6, we know a huge amount of CCZ-inequivalent APN (n,n)-functions for dimensions $n \leq 10$, and only a handful of these are covered by the known infinite constructions. On the one hand, this illustrates the difficulty of constructing new infinite families of APN and AB functions. On the other hand, it suggests that our current state of knowledge is merely the "tip of the iceberg", and there is much more to be discovered.

Some of the simplest (and most remarkable in a number of ways) APN and AB functions are power functions, or monomial functions; that is, functions of the form $F(x)=x^e$, where e is some natural number. These represent the earliest known instances of APN and AB functions, and the earliest known infinite constructions. To date, six infinite families of APN power functions are known; these are listed in Table 1.2. The second column gives the form of the exponent e in the univariate representation $F(x)=x^e$, while the third column describes the conditions that need to be satisfied in order for $F(x)=x^e$ to be APN over $\mathbb{F}_{2^n}$ (and AB for odd dimensions n in the case of the Gold, Kasami, Welch, and Niho families).

It is conjectured by Dobbertin that Table 1.2 is complete up to CCZ-equivalence [43]; that is, any monomial APN function must be CCZ-equivalent to an instance from one of the families in Table 1.2. The conjecture has been verified computationally up to dimension $n \leq 24$ by Canteaut according to [43], and later up to $n \leq 34$ and up to $n \leq 42$ for even n by Edel (unpublished). Despite these results, this conjecture remains one of the oldest and best known open problems in the area. This makes new methods of constructing, expressing, and analyzing monomial functions an important direction of research. In Paper IX, we investigate a construction that allows us to compose two monomials from the same CCZ-equivalence class with a linear polynomial and to obtain a monomial APN function that is CCZ-inequivalent to the ones used in

the composition. We hope that this novel method of expressing power APN functions may i.a. lead towards a resolution of Dobbertin's conjecture in the future.

The first systematic construction of polynomial (as opposed to monomial) APN functions was achieved by a constructive application of CCZ-equivalence [25]. More precisely, the authors constructed APN functions CCZ-equivalent to APN monomials, but EA-inequivalent to them; in particular, the work presented in this paper showed that CCZ-equivalence is strictly more general than EA-equivalence and taking inverses of permutations. Prior to this work, APN functions were typically only considered up to EA-equivalence and taking inverses; so, in a way, this paper justified the importance of CCZ-equivalence for the study of APN functions; as discussed in Section 1.3, CCZ-equivalence is now the "standard" equivalence relation used in the classification of APN and AB functions. The construction from [25] also disproved a conjecture from [35] that all AB functions are EA-equivalent to permutations.

The first APN functions CCZ-inequivalent to monomials were given in [45]. The idea was to consider the sum of two Gold APN power functions in order to obtain new APN functions, and this approach produced sporadic APN instances CCZ-inequivalent to monomials in dimensions 10 and 12. The first infinite family of APN functions CCZ-inequivalent to monomials (given as Family F1-F2 in Table 1.3) was then constructed in [22]. The functions from family F1-F2 generalize the sporadic APN function $x^3 + ux^{528}$ over $\mathbb{F}_{2^{12}}$ from [45] (which is APN for some particular choices of $u \in \mathbb{F}_{2^{12}}$) in two ways: for dimensions n divisible by 3, and for dimensions n divisible by 4. Thus, depending on the point of view, F1-F2 may be considered as two distinct infinite families, or as one general infinite family that unifies both constructions. Besides making up the first infinite family of APN functions CCZ-inequivalent to monomials, the functions from F1-F2 serve as the first counterexample disproving a conjecture from [35] stating that any quadratic AB function must be CCZ-equivalent to a Gold function; and also show that AB functions do not necessarily have to be CCZ-equivalent to monomials.

The idea of constructing new APN functions by adding terms to existing ones was further exploited in [10, 12] where the authors generalized the binomials from [22] for n divisible by 3 into trinomials and quadrinomials (families F7-F9 in Table 1.3). More recently, a similar approach was used in Paper IV, in which we generalized the sporadic APN binomial $x^3 + ux^{36}$ over $\mathbb{F}_{2^{10}}$ from [45] (which had remained unclassified into any infinite family since its discovery in 2006) into an infinite family of APN quadrinomials; the result is family F13 in Table 1.3.

Very recently, our approach from Paper IV was adapted to further constructions of infinite families in [72], where the authors investigate functions of the form $a\mathrm{Tr}_m^n(F(x)) + a^{2^m}\mathrm{Tr}_m^n(G(x))$ over $\mathbb{F}_{2^n}$ for $n = 2m$; we note that the quadrinomials from family F13 are of this form. The authors discover a new infinite family of APN functions, and obtain some sporadic APN instances through theoretical constructions. Since the paper is only available as a preprint at the time of writing, we do not include this family in Table 1.3. Despite this, we believe this is a result worth mentioning.

The construction of Family F4 from Table 1.3 is based on the idea of adding a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ to a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ [23]. This led to the infinite family of APN functions $x^3 + \mathrm{Tr}(x^9)$ (APN over $\mathbb{F}_{2^n}$ for any n, and AB for odd values of n), which can be further generalized to the form $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$; we recall that the absolute trace $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a Boolean function. This is the first infinite family of APN polynomial (as opposed to monomial) functions with binary

coefficients, i.e. with all their coefficients in the prime field $\mathbb{F}_2$. Furthermore, the idea from [23] gave rise to a more general construction of (n,n)-functions of the form $L_1(x^3)+L_2(x^9)$ (where L_1, L_2 are linear (n,n)-functions) [24]; this latter construction resulted in families F5 and F6 from Table 1.3.

The idea of adding a Boolean function to an (n,n)-function was generalized into the so-called switching construction [46], which was used to computationally find new sporadic instances of APN functions in dimensions 6, 7, and 8. The switching construction (along with other methods of finding sporadic APN instances) is discussed in more detail in the following Section 1.6.

Further infinite constructions were derived from studying quadratic functions with a special polynomial form. More precisely, Dillon et al. suggested in [15] polynomials of the form

$$x(Ax^2+Bx^q+Cx^{2q})+x^2(Dx^q+Ex^{2q})+Gx^{3q}$$

over $\mathbb{F}_{2^n}$ with $n=2m$, $q=2^m$, as good candidates for i.a. APN functions. In the same paper, the authors were able to obtain new sporadic APN instances of this form in dimension 6 and 8 that are CCZ-inequivalent to power functions. A general construction of functions of this form [20] resulted in the infinite family given as F3 in Table 1.3.

Recently, another family of APN functions was constructed based on the principle of isotopic equivalence [18]. The notion of isotopic equivalence can only be defined in the case of quadratic planar functions, which are themselves objects that only exist over finite fields of odd characteristic; since the work presented in this dissertation exclusively concerns functions over binary fields (that is, finite fields of even characteristic), we omit giving definitions or going into further details regarding the notions of planar functions and isotopic equivalence. We only mention that in the case of quadratic planar functions, isotopic equivalence is strictly more general than CCZ-equivalence (which can be defined for functions over fields of odd characteristic analogically to the way this is done in the binary case); and that there is no straightforward analogue of isotopic equivalence for e.g. quadratic APN functions. In [18], the authors investigate the possibility of adapting the notion of isotopic equivalence to the APN case, and obtain a construction of APN functions over $\mathbb{F}_{2^n}$ of the form $L(x)^{2^i}x+L(x)x^{2^i}$ (where L is some (n,n)-linear function); they then formulate conditions ensuring that functions of this form are APN. The resulting construction is given as family F11 in Table 1.3.

The remaining infinite families of APN functions known to date rely on the bivariate representation of (n,n)-functions. The approach of constructing APN functions in bivariate form was first introduced in [33], and was used to construct an infinite family of APN functions; unfortunately, this family was later shown to coincide with family F3 from Table 1.3 [19, 29]. However, two further infinite families of APN functions have been constructed in bivariate form that are CCZ-inequivalent to the rest of the known families. In both cases, the functions $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ have the form $F(x,y)=(xy,G(x,y))$, where $G:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$ for $n=2m$. This is the same form as that of the family of functions constructed in [33], and all of these constructions differ according to the exact form of $G(x,y)$. In [73], functions of the form $G(x,y)=x^{2^i+1}+\alpha y^{2^j(2^i+1)}$ are considered, and are shown to be APN for certain choices of $i,j\in\mathbb{N}$ and $\alpha\in\mathbb{F}_{2^m}$; this results in family F10 from Table 1.3. More recently, functions of the form $G(x,y)=x^{2^{2i}+2^{3i}}+ax^{2^{2i}}y^{2^i}+by^{2^{i+1}}$ with $a\in\mathbb{F}_2$ were considered in [67], and gave rise to family F12 in Table 1.3. We note that while the original construc-

tions of families F10 and F12 are given in bivariate form, the functions in Table 1.3 are given in the univariate representation.

An infinite family of APN functions in bivariate form was recently constructed by Göloğlu; the functions in the construction are referred to as "Gold-hybrid functions", and can be seen as an extension of some of the functions from Family F13 in Table 1.3. The construction has been submitted to IEEE Transactions on Information Theory, but has not been published yet (as a preprint, or otherwise), which is why we have not added it as an entry in Table 1.3 (Faruk Göloğlu, personal communication). As with the infinite family constructed in [72], however, we strongly believe that it deserves to be mentioned here.

1.6 Known instances of APN and AB functions

While the construction of infinite families of APN and AB functions represents one of the ultimate goals of their study, we know many CCZ-inequivalent sporadic instances of APN functions (and AB functions) that have not been classified into infinite families. In fact, the vast majority of known APN functions belong to the category of such sporadic instances: for example, at the time of writing, we know more than 20 000 CCZ-inequivalent APN instances over $\mathbb{F}_{2^8}$, while instances from the monomial and polynomial families in Tables 1.2 and 1.3 cover only around 10 of these. This fact is important per se, as it convincingly shows that representatives from the known infinite families constitute only a miniscule fraction of all APN functions. Furthermore, some of the sporadic instances possess properties (such as being bijective, being CCZ-inequivalent to a quadratic function or monomial, or having an extended Walsh spectrum distinct from that of any power function) that none of the instances belonging to the known families do. This makes it quite worthwhile to study the properties of such sporadic instances, and to develop new methods for finding such instances.

1.6.1 Existing classifications

Despite the fact that the majority of sporadic APN functions have not been generalized into infinite families, classification results up to CCZ-equivalence for APN (and hence, for AB) functions over $\mathbb{F}_{2^n}$ are known for small values of n. In the following, we give a brief summary of such results.

All APN functions over $\mathbb{F}_{2^n}$ for $n \leq 5$ have been classified up to both EA- and CCZ-equivalence via computational search [14]. For dimensions $n \leq 4$, all APN functions are CCZ-equivalent; while for $n = 5$, all APN functions are CCZ-equivalent to monomials, and fall into three distinct CCZ-equivalence classes, represented by x^3, x^5, and x^{-1}. In the case of EA-equivalence, the APN functions over $\mathbb{F}_{2^4}$ fall into two classes; while in the case of $\mathbb{F}_{2^5}$, they comprise seven EA-equivalence classes.

For $n = 6$, the classification up to CCZ-equivalence is complete for quadratic and cubic APN functions [56]. The quadratic and cubic APN functions in this dimension fall into 14 distinct CCZ-equivalence classes; 13 of them contain quadratic representatives, while the fourteenth class corresponds to the only known instance of an APN function CCZ-inequivalent to quadratic and monomial functions [46]. A complete description of the EA-equivalence classes contained in the CCZ-equivalence classes of

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[22]
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[20]
F4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$	[23]
F5	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[24]
F6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$	[24]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1,3\|(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[12]
F10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m, m\geq 2$ even, $\gcd(k,m)=1$ and $i\geq 2$ even, u primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube	[73]
F11	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd, $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [18]	[18]
F12	$u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q=2^m, n=2m, \gcd(i,m)=1$, $x^{2^i+1}+ax+b$ has no roots in $\mathbb{F}_{2^m}$	[67]
F13	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n=2m=10$, $(a,b,c)=(\beta,1,0,0)$, $i=3$, $k=2$, β primitive in $\mathbb{F}_{2^2}$ $n=2m$, m odd, $3\nmid m$, $(a,b,c)=(\beta,\beta^2,1)$, β primitive in $\mathbb{F}_{2^2}$, $i\in\{m-2,m,2m-1,(m-2)^{-1} \bmod n\}$	[26]

Table 1.3: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^n}$

the known APN functions over $\mathbb{F}_{2^6}$ is given in [28]; some partial results on the same kind of classification for $n = 7, 8, 9$ are also given in the paper.

The classification of quadratic APN functions up to CCZ-equivalence for $n = 7$ was completed just recently [53]; the quadratic APN functions over $\mathbb{F}_{2^7}$ fall into 488 CCZ-equivalence classes. The majority of these were discovered using the matrix method presented in [71]; the last instance was found in [53], where it is also shown that the 488 classes exhaust all possibilities.

In the case of quadratic APN functions with binary coefficients (that is, having all coefficients in the finite field $\mathbb{F}_2$), the classification up to CCZ-equivalence is complete up to $n = 9$. This result is presented in Paper III.

1.6.2 Methods for constructing APN and AB functions

The majority of known APN instances have been obtained by computational search. The vast number of APN functions over $\mathbb{F}_{2^n}$ even for small values of the dimension n makes it impossible to conduct an exhaustive search over all (n,n)-functions, and so such searches typically target functions of a particular form, e.g. functions whose polynomial representation consists of only a few terms with non-zero coefficients (that is: binomials, trinomials, quadrinomials, etc.) Indeed, some of the earliest known instances of APN functions CCZ-inequivalent to monomials were discovered in this way: one of the first known such instances is the binomial $x^3 + \beta x^{36}$ for $n = 10$ from 2006 [45] which we have generalized into an infinite family in Paper IV; and early lists of CCZ-inequivalent APN instances for $n \in \{6, 7, 8\}$ are given in [15]. The latter paper lists 13, 18, and 12 CCZ-inequivalent APN functions for $n = 6, 7, 8$, respectively; these numbers include the previously known monomial APN functions.

The so-called switching method [46] is based on the idea used in the construction of family F4 in [23], and involves modifying a given APN (n,n)-function by adding a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ to it multiplied by a fixed constant $v \in \mathbb{F}_{2^n}$ in order to obtain a new function $G(x) = F(x) + vf(x)$ (in fact, the switching construction as presented in [46] is somewhat more general; but the case of adding a Boolean function is the only case that we know of so far where it can be applied efficiently; furthermore, all the computational results from [46] are obtained in this way, and so we do not go into further details about this more general theoretical framework). It is shown how the values of f for which $G(x)$ is APN can be efficiently found. This approach is then applied to the lists of functions from [15] to obtain new, CCZ-inequivalent instances. The number of CCZ-inequivalent classes rises to 14, 19, 23 for $n = 6, 7, 8$, respectively. As expected, the new functions have a rather complicated univariate form. Most remarkably, the only known APN function CCZ-equivalent to neither monomials nor quadratic functions can be obtained using this method. The construction of further APN instances with this property is an important open problem.

Functions having a simple form under one representation (for instance, the univariate representation) will typically have a very complicated form under most other representations. This is the reason that many constructions exploit representations other than the ones typically used in the literature. Another significant advantage that a representation might provide when searching for APN functions is for it to behave predictably under CCZ- and EA-equivalence (that is, to allow us to easily characterize when two dis-

tinct functions belong to the same CCZ- or EA-equivalence class); this allows branches in the search tree leading to functions that are equivalent to ones that have already been processed to be cut out, thereby reducing both the time for running the search procedure, and that for classifying the resulting functions up to CCZ-equivalence.

A correspondence between quadratic APN functions and algebraic structures called "APN algebras" was introduced in [68], and computationally exploited to obtain 285 new instances of quadratic APN functions for $n = 7$, and 10 new instances of quadratic APN functions for $n = 8$.

A further breakthrough was made possible by the representation of quadratic functions in matrix form introduced in [71]. The authors derived a characterization of matrices that correspond to quadratic APN functions (more precisely, to purely quadratic ones, i.e. quadratic functions without linear and constant terms), and exploited this computationally to find many new instances of APN functions for $n = 7$ and $n = 8$. Combined with the results from [68], all but one of the quadratic APN functions on $\mathbb{F}_{2^7}$ were discovered in this way. Furthermore, more than 8 000 new CCZ-inequivalent APN functions were obtained over $\mathbb{F}_{2^8}$, which was a tremendous improvement compared to the 30 or so CCZ-inequivalent APN functions previously known over this field. Some of the newly discovered functions possess interesting properties: for instance, they exhibit an extended Walsh spectrum distinct from that of the Gold APN functions, in contrast to all the previously known polynomial (as opposed to monomial) instances.

The method from [71] is specialized in Paper III to the case of functions with binary coefficients, and is used to find two new (up to CCZ-equivalence) instances of such functions for $n = 9$; more importantly, this completes the classification of this type of functions over $\mathbb{F}_{2^n}$ for $n \leq 9$.

The last instance of a quadratic APN function over $\mathbb{F}_{2^7}$ is found by a somewhat differently formulated matrix representation in [53]; furthermore, the authors show that the currently known quadratic APN functions over $\mathbb{F}_{2^7}$ exhaust all possibilities.

The next big batch of APN functions was found just recently [3] by utilising methods from [2] to construct 12 923 new (up to CCZ-equivalence) quadratic APN functions for $n = 8$, 35 for $n = 9$, and 10 for $n = 10$. Besides providing a huge number of new quadratic APN instances, these results reveal three previously unknown Walsh spectra of APN functions over $\mathbb{F}_{2^8}$, bringing the total number of distinct Walsh spectra (that we know can be attained by APN functions in this dimension) to six. This accumulated corpus of APN functions has yet to be studied in detail.

As is clear from the above discussion, we know a very large number of CCZ-inequivalent APN functions, especially for $n = 7$ and $n = 8$. This has the advantage of providing us with a huge number of samples on which to test potential conjectures and hypotheses, but has the obvious disadvantage that it becomes difficult to identify those instances that are unusual or remarkable in some way. We briefly accent two of the most notable APN instances; surprisingly, both of them are over $\mathbb{F}_{2^6}$.

The **Kim function** is defined over $\mathbb{F}_{2^6}$ as

$$K(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$ satisfying $u^6 + u^4 + u^3 + u + 1 = 0$, i.e. having $x^6 + x^4 + x^3 + x + 1$ as a minimal polynomial. The function $K(x)$ is known to

be APN [15], and is otherwise unremarkable by itself. What makes it noteworthy is that it is CCZ-equivalent to a permutation; namely, the only known (up to CCZ-equivalence) APN permutation over a finite field $\mathbb{F}_{2^n}$ of even extension degree, which was discovered by Browning, Dillon, McQuistan, and Wolfe in 2009 by exploring the CCZ-equivalence class of $K(x)$ [16]. The permutation itself is of algebraic degree 4 (while $K(x)$ is quadratic), and has a very complicated univariate polynomial form; namely

$$\begin{aligned} &w^{45}x^{60}+w^{41}x^{58}+w^{43}x^{57}+w^{4}x^{56}+w^{50}x^{54}+w^{20}x^{53}+w^{45}x^{52}+w^{20}x^{51}+w^{23}x^{50}+\\ &w^{36}x^{49}+w^{56}x^{48}+w^{21}x^{46}+w^{5}x^{45}+w^{21}x^{44}+w^{28}x^{43}+w^{3}x^{42}+w^{59}x^{41}+w^{58}x^{40}+\\ &w^{57}x^{39}+w^{53}x^{38}+w^{37}x^{37}+w^{40}x^{36}+w^{18}x^{35}+w^{41}x^{34}+w^{54}x^{33}+w^{3}x^{32}+w^{49}x^{30}+\\ &w^{41}x^{29}+w^{42}x^{28}+w^{50}x^{27}+w^{53}x^{26}+w^{58}x^{25}+w^{9}x^{24}+x^{23}+w^{28}x^{22}+w^{3}x^{21}+\\ &w^{21}x^{20}+w^{52}x^{19}+w^{60}x^{17}+w^{59}x^{16}+w^{10}x^{15}+w^{42}x^{13}+w^{8}x^{12}+w^{35}x^{11}+w^{44}x^{10}+\\ &w^{45}x^{8}+w^{8}x^{7}+w^{61}x^{6}+w^{59}x^{5}+w^{20}x^{4}+w^{12}x^{3}+w^{37}x^{2}+w^{2}x, \end{aligned}$$

where $w=\alpha^{-2}$ and α is a primitive element of $\mathbb{F}_{2^6}$. This complicated univariate form makes it even more surprising that its equivalence class can be represented by a function as simple as a trinomial. To date, no other instances of APN permutations over $\mathbb{F}_{2^n}$ have been found in the case of even n; despite the abundance of newly discovered quadratic APN functions for $n=8$ and $n=10$, it has been computationally verified that none of them can be CCZ-equivalent to a permutation [3]. The "big APN problem" of the existence of APN permutations for even n greater than 6 thus remains open.

Another remarkable instance over $\mathbb{F}_{2^6}$ is the only known APN polynomial that is CCZ-inequivalent to both monomial and quadratic functions. It was independently discovered in [14] as a result of the partial classification of APN functions over $\mathbb{F}_{2^6}$, and by the switching method in [46]. As with most functions obtained in this way, its univariate representation is quite complex, namely

$$\begin{aligned} x^3+\alpha^{17}(x^{17}+x^{18}+x^{20}+x^{24})+\alpha^{14}[&\alpha^{18}x^9+\alpha^{36}x^{18}+\alpha^9x^{36}+x^{21}+x^{42}+\\ &\mathrm{Tr}(\alpha^{27}x+\alpha^{52}x^3+\alpha^6x^5+\alpha^{19}x^7+\alpha^{28}x^{11}+\alpha^2x^{13})], \end{aligned}$$

where α is a primitive element of $\mathbb{F}_{2^6}$. We note that there is a typo in the polynomial form given in [46]. The representation above is correct, which can be easily checked by computing its differential uniformity and Δ-rank (see the following paragraph) on a computer (for instance, with the *Magma* computer algebra system).

This function is provably CCZ-inequivalent to any quadratic function due to its Δ-rank: in [46], it is shown that the Δ-rank of any (n,n)-function CCZ-equivalent to a quadratic one is at most 2^{n+1}, while the Δ-rank of the function above is 152, which is strictly greater than $2^{6+1}=128$. Finding other instances of APN functions CCZ-inequivalent to quadratic and monomial functions is one of the most important open problems at the moment.

1.7 Overview of the papers

In this section, we present a brief summary of the nine papers that make up the rest of the dissertation. All the necessary background and most of the relevant definitions

have been presented in the prequel; Section 1.8 provides a brief summary of the results obtained in the papers, and an overview of prospective directions for future work.

1.7.1 Changing APN functions at two points

The first paper considers the problem of whether it is possible to obtain one APN function from another by changing precisely two of its output values. The original motivation for this construction comes from [21] where the authors investigate the open question of whether an APN (n,n)-function can have algebraic degree equal to n. An upper bound on the algebraic degree of AB functions has been known since 1998 [35], while the same question for the case of APN functions has been open since then. We note that APN (n,n)-functions of algebraic degree $n-1$ are known for odd values of n, and so the question of the maximum algebraic degree of APN functions can be equivalently formulated by asking whether it is possible for an APN function over $\mathbb{F}_{2^n}$ to have algebraic degree precisely equal to n.

The connection to modifying the output values of a given function comes from the fact that the only possible term (up to multiplication by a non-zero constant) of algebraic degree n over $\mathbb{F}_{2^n}$ is x^{2^n-1}. As a function of x, the term x^{2^n-1} evaluates to 1 for all non-zero values of $x \in \mathbb{F}_{2^n}$, and evaluate to 0 for $x = 0$; in other words, $x \mapsto x^{2^n-1}$ is an indicator function that signifies whether its input is non-zero. Using this observation, we can easily build an indicator function $1_a(x)$ for any element $a \in \mathbb{F}_{2^n}$, which evaluates to 1 if $x = a$, and evaluates to 0 otherwise. More precisely, it is enough to take

$$1_a(x) = (1 + (x+a)^{2^n-1}),$$

and one can readily verify that 1_a as defined above is indeed the indicator function for a. From this point of view, any function G (APN or not) of algebraic degree n can be written as

$$G(x) = F(x) + 1_a(x)c,$$

where F is of algebraic degree strictly less than n, 1_a is the indicator function for some $a \in \mathbb{F}_{2^n}$, and $0 \neq c \in \mathbb{F}_{2^n}$ is some constant. We then have

$$G(x) = \begin{cases} F(x) & x \neq a \\ F(a) + c & x = a; \end{cases}$$

that is, the values of F and G differ only on $a \in \mathbb{F}_{2^n}$, and coincide everywhere else. The question of the existence of APN functions of algebraic degree n is thus equivalent to that of being able to obtain an APN function G by modifying precisely one output of some function F of algebraic degree strictly less than n.

Besides opening up a new perspective from which to approach the problem of the algebraic degree of APN functions, the above observation suggests a natural procedure to search for new APN functions; namely, start with some given function F, and try to find all APN functions that can be obtained by modifying a few of its values. In [21], the authors attempt to construct APN functions by changing one output value of some known functions, but their investigation suggests that this is most likely not possible. A natural generalization of this method is to modify more than one output of the starting function. In Paper I, we consider a construction in which two of the output values of

a given function are modified. More precisely, given an (n,n)-function F, two distinct elements $u_1, u_2 \in \mathbb{F}_{2^n}$, and two shifts $v_1, v_2 \in \mathbb{F}_{2^n}$ (not necessarily distinct), we set

$$G(x) = \begin{cases} F(x) + v_1 & x = u_1 \\ F(x) + v_2 & x = u_2 \\ F(x) & x \notin \{u_1, u_2\}. \end{cases}$$

Thus, the values $F(x)$ and $G(x)$ coincide for all $x \in \mathbb{F}_{2^n}$ except for $x \in \{u_1, u_2\}$; and for each $i \in \{1,2\}$, the shift v_i expresses the difference between $F(u_i)$ and $G(u_i)$. Using indicator functions, the univariate representation of G can be expressed as

$$G(x) = F(x) + 1_{u_1}(x)v_1 + 1_{u_2}(x)v_2.$$

In the paper, we provide two main characterizations of the APN-ness of G constructed in this way: one in terms of the derivatives $D_a F$ of the starting function F, and one in terms of the moments of the Walsh transform of F and G. Some nonexistence results are derived from these two characterizations. Furthermore, the special case of "swapping" two outputs (that is, when $G(u_1) = F(u_2)$ and $G(u_2) = F(u_1)$) is investigated in greater detail in terms of the Walsh transform, and additional results are obtained. The case of modifying the outputs of power functions is also treated in more detail, and some computational results are given that suggest that it is impossible to obtain APN functions from known ones by modifying two output values, except in trivially small dimensions.

1.7.2 On the distance between APN functions

This paper generalizes the construction from the previous one by allowing an arbitrary number of outputs of the starting function F to be modified. Before transitioning to this more general setting, we attempted to construct APN functions by modifying a small number (three or four) of the outputs of known ones. As in the case of modifying two outputs, this was only successful in very small dimensions. In Paper II, we consider the general construction

$$G(x) = \begin{cases} F(x) + v_i & x = u_i \\ F(x) & x \notin \{u_1, u_2, \ldots, u_K\}, \end{cases}$$

where K is a natural number, $u_1, u_2, \ldots, u_K$ are distinct elements of $\mathbb{F}_{2^n}$, and $v_1, v_2, \ldots, v_K$ are (not necessarily distinct) elements of $\mathbb{F}_{2^n}$. The constructions investigated in [21] and Paper I are the particular cases for $K = 1$ and $K = 2$, respectively. Recalling that the Hamming distance between two functions is the number of inputs for which their values differ, we can see that $d_H(F,G) \leq K$ for F and G as constructed above; and that $d_H(F,G)$ is exactly K if all the shifts $v_1, v_2, \ldots, v_K$ are non-zero. We derive a lower bound on the Hamming distance between any given APN function F and a closest (in terms of Hamming distance) APN function G distinct from F. The bound is obtained by first calculating the multiset of cardinalities (already discussed in Section 1.4)

$$\Pi_F = \{\pi_F(b,c) : b, c \in \mathbb{F}_{2^n}\},$$

where

$$\pi_F(b,c) = \#\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n}) F(x) + F(a+x) + F(a+c) = b\}$$

for any $b, c \in \mathbb{F}_{2^n}$. Based on the results obtained in the paper, the minimum value in Π_F, denoted by m_F, can be used to express a lower bound on the Hamming distance between F and any other APN function G as

$$d_H(F,G) \geq \left\lceil \frac{m_F}{3} \right\rceil + 1.$$

The value of m_F can be computed very efficiently for all practically relevant dimensions n, and its values are quite high. For instance, the value of m_F for the Gold function appears to be very close in magnitude to that of all known APN functions in dimensions $n \leq 8$ (for instance, this value varies between 15 and 27 for the functions over $\mathbb{F}_{2^6}$ tested in Paper II, with the value for the Gold function being 27; and it varies from 99 to 111 for the tested functions over $\mathbb{F}_{2^8}$, with the value for the Gold function being 111). As one of our contributions in Paper II, we have derived a formula for the exact value of m_F for $F(x) = x^3$ over $\mathbb{F}_{2^n}$ for any dimension n, namely

$$m_F = \begin{cases} 2^{n-1} - 1 & n \text{ odd;} \\ 2^{n-1} - 2^{n/2-1} - 1 & n \text{ even}, n/2 \text{ odd;} \\ 2^{n-1} - 2^{n/2} - 1 & n \text{ even}, n/2 \text{ even.} \end{cases}$$

Evidently, the value of m_F (and hence that of the bound on $d_H(x^3, G)$ for any APN function $G \neq x^3$) increases exponentially with the dimension n; for dimension $n = 8$, the value of the bound is already 38, meaning that at least 38 of the outputs of x^3 have to be changed in order to obtain an APN function. As mentioned above, our computational results suggest that the value of the lower bound for all known APN functions is roughly of the same magnitude as that of the Gold function x^3 over the same field. This explains why we failed to find APN functions using the approach of changing a small number of outputs. Unfortunately, our result implies that constructing APN functions in this way is not feasible (unless some further investigation identifies some structure and patterns in the set of points $u_1, u_2, \ldots, u_K$ and the sequence of shifts $v_1, v_2, \ldots, v_K$ that would significantly reduce the search space), and other methods have to be considered.

An equally important result is that the multiset Π_F associated with an (n,n)-function F is shown to be invariant under CCZ-equivalence. Based on computational experiments, we can see that it takes a lot of distinct values across the known APN functions. For instance, it takes 6 669 distinct values for the 8 181 known CCZ-inequivalent APN functions from [71]. A consequence of this invariance is that the bound on the Hamming distance to the closest APN function is a CCZ-invariant as well; thanks to this, we were able to compute this lower bound for all known CCZ-equivalence classes, and to compute it for all quadratic APN functions over those dimensions in which the classification of quadratic APN functions up to CCZ-equivalence was complete at the time. The multiset Π_F is, to the best of our knowledge, the first useful invariant for APN functions under CCZ-equivalence to have been introduced in the past 10 years. We also show that in the case of a quadratic function F, the computation time for Π_F

can be reduced by a factor of 2^n by fixing e.g. $c = 0$ and computing only the reduced multiset

$$\Pi_F^0 = \{\pi_F(b,0) : b \in \mathbb{F}_{2^n}\}.$$

It is worth noting that the actual minimum distance to the closest APN function is not itself a CCZ-invariant, and it is easy to find counterexamples. Another remarkable observation is that although Π_F can take many distinct values for the known APN functions, its value is the same for all instances belonging to the currently known infinite families (with the exception of the Dobbertin and inverse power APN functions). It would thus be very interesting to construct an infinite family of APN polynomials having a non-Gold-like value of Π_F.

Finally, we develop a filtering algorithm based on the characterizations obtained in the paper which allows us to drastically reduce the number of possible choices for $v_1, v_2, \ldots, v_K$ if the set of elements $u_1, u_2, \ldots, u_K$ whose output values will be changed in a given (n,n)-function F is known. This reduces the search space sufficiently and allows us to computationally find the exact minimum distance between representatives from the EA-equivalence classes of the known APN functions in dimension 5 and the closest APN functions to them; based on these results, we see that the lower bound is not tight.

1.7.3 Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9

A matrix representation of quadratic (n,n)-functions is developed in [71], in which any purely quadratic (n,n)-function F can be identified with a symmetric $n \times n$ matrix H_F over $\mathbb{F}_{2^n}$. The details of this matrix representation have already been discussed in Section 1.1. In [71], it is shown that a purely quadratic F is APN if and only if any nonzero linear combination of the rows of its associated matrix H_F has rank $n-1$. To make this more precise, we clarify that a linear combination of the rows of H_F is an n-dimensional vector $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{2^n})^n$; and that the rank of v is the dimension of the linear subspace of $\mathbb{F}_{2^n}$ spanned by $\{v_1, v_2, \ldots, v_n\} \subseteq \mathbb{F}_{2^n}$. A matrix H that is symmetric, has a zero main diagonal, and satisfies the aforementioned rank condition, is referred to as a **QAM**, or **quadratic APN matrix**.

Thus, constructing quadratic APN functions becomes equivalent to constructing QAM's. This is computationally exploited in [71] to construct new QAM's from existing ones. Unlike in the case of the representation of (n,n)-functions by a truth table, where, as we show in Paper II, changing a few of the values of the truth table of an APN function cannot give another APN function, it is possible to change a few of the values of a QAM and obtain another QAM. More concretely, the computational approach used in [71] starts with the QAM corresponding to a known quadratic APN function, and tries to replace a few of its entries with different ones so that the resulting matrix is once again a QAM. This method has proved to be quite fruitful, and has led to the construction of a few hundred CCZ-inequivalent and previously unknown APN functions over $\mathbb{F}_{2^7}$, and more than 8 000 new CCZ-inequivalent APN functions over $\mathbb{F}_{2^8}$. Until the publication of [3] in 2020, this was the largest known corpus of CCZ-inequivalent APN instances.

In Paper III, we specialise this method to the case of functions with binary coefficients in their univariate representation, i.e. to functions represented by polynomials of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_i \in \mathbb{F}_2$; such an (n,n)-function $F(x)$ then satisfies $F(x^2) = F(x)^2$ for any $x \in \mathbb{F}_{2^n}$. We note that quite a few of the known APN instances, including ones from infinite families (including all monomial families from Table 1.2, and families F4, F5, F6 from Table 1.3) are of this form. The advantage is that in the case of binary coefficients, it is possible to derive additional restrictions on the matrix H_F. More precisely, denoting by $(H_F)_{i,j}$ the entry in the i-th row and j-th column of H_F for $0 \leq i, j \leq n-1$, we obtain that when an (n,n)-function F has binary coefficients, H_F must satisfy

$$(H_F)_{i+1,j+1} = (H_F)_{i,j}^2$$

for all $0 \leq i, j \leq n-1$, with the indices i and j taken modulo n. This means that we have much fewer "degrees of freedom" when selecting the entries of H_F, and so the complexity of traversing all such matrices drops significantly. For instance, guessing the matrix H_F corresponding to a $(6,6)$-function F (with arbitrary coefficients) involves guessing the values of 15 entries; while if F has binary coefficients, it is enough to guess 3 values to obtain the entire matrix.

This allows us to conduct exhaustive searches for dimensions much higher than in the general case; in particular, we obtain all quadratic APN functions with binary coefficients over $\mathbb{F}_{2^n}$ for $n \leq 9$. For comparison, the classification of quadratic functions in the general case is only finished for $n \leq 7$, with the classification for $n = 7$ having been published only last year [53].

The classification of the resulting functions proves to be the most computationally intense part of the process: we obtain 21 504 functions in total, and use the linear code test to partition them into CCZ-equivalence classes (the algorithms for testing EA-equivalence from Paper V and from [31] had not been discovered yet; and neither had the orthoderivatives, which would have probably reduced the computation time by quite a bit). This takes slightly less than a full year on our department server, even when running several processes in parallel. As a result, we find two previously unknown APN instances over $\mathbb{F}_{2^9}$, namely

$$x \mapsto x^{136} + x^{132} + x^{96} + x^{80} + x^{36} + x^{34} + x^{18} + x^{17} + x^{12}$$

and

$$x \mapsto x^{288} + x^{272} + x^{264} + x^{160} + x^{144} + x^{130} + x^{48} + x^{34}.$$

Furthermore, we confirm that the known instances of quadratic APN functions with binary coefficients for $n \leq 8$ exhaust all possible cases; we do, however, discover shorter representatives (in the sense of having fewer terms) for two of the known instances over $\mathbb{F}_{2^7}$, namely: $x^3 + x^6 + x^{72}$ is CCZ-equivalent to $x^3 + \mathrm{Tr}(x^9)$, and $x^3 + x^6 + x^{144}$ is CCZ-equivalent to $x^9 + \mathrm{Tr}(x^3)$. Finally, we have computationally verified that none of the newly discovered functions can be CCZ-equivalent to a permutation.

1.7.4 A new family of APN quadrinomials

The binomial $B(x) = x^3 + \beta x^{36}$ (for some appropriate value of β) has been known to be APN over $\mathbb{F}_{2^{10}}$ since 2006, and is one of the two earliest instances of APN functions CCZ-inequivalent to monomials [45]. Consequently, it has attracted a lot of attention from the Boolean functions community; despite this, it had not been generalized into any infinite construction until now. For comparison, the sporadic APN binomial $x^3 + wx^{258}$ (for an appropriate value of w) over $\mathbb{F}_{2^{12}}$ introduced in the same paper was previously generalized into two infinite APN families: one for n divisible by 3, and one for n divisible by 4 [22]. It has been conjectured that the aforementioned infinite families and the sporadic $B(x)$ exhaust all quadratic APN binomials up to CCZ-equivalence [6].

In order to extend an APN instance to an infinite construction, one typically conducts a computational search for functions with the same polynomial form over higher dimensions. In our attempt to extend $x^3 + \beta x^{36}$, we take a different approach, and attempt to add more terms to $B(x)$ in order to obtain further APN functions; that is, we search for APN functions of the form

$$x^3 + \beta x^{36} + c_1 x^{i_1} + c_2 x^{i_2} + \cdots + c_K x^{i_K}$$

for some natural number K, where $c_j \in \mathbb{F}_{2^n}$ and $3 \leq i_j \leq 2^n - 1$ for $j = 1, 2, \ldots, K$. The intuition is that the binomial $B(x)$ might be a special case of a general construction with more terms, which vanish in the particular case of $n = 10$.

Using this approach, we find APN quadrinomials over $\mathbb{F}_{2^{10}}$ of the form

$$x^3 + \beta x^{36} + \beta^2 (x^3)^{2^5} + (x^{36})^{2^5} \tag{1.11}$$

that are CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$, including the binomial $B(x)$. Here, we assume that β is a primitive element of $\mathbb{F}_{2^2}$, although it can be taken to have other values as well (which lead to functions that are CCZ-equivalent to the ones that we obtain when β is a primitive element of $\mathbb{F}_{2^2}$). These quadrinomials display a clear structure, and we are able to find instances with the same form in dimensions $14, 22, 26, 34, 48, 52$. Consequently, we are able to formulate an infinite construction of the form

$$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k} \tag{1.12}$$

for $n = 2m$ with n not divisible by 3, and k even, and to describe choices of a, b, c and i for which this function is APN. In this way, we generalize $B(x)$ to an infinite family. By computing the Γ- and Δ-ranks of these functions for $\mathbb{F}_{2^{10}}$ (which is the highest dimension for which we can do this with our current computational resources), we are able to conclude that the instances of this family in $\mathbb{F}_{2^{10}}$ belong to four distinct CCZ-classes; two of them are equivalent to known APN functions, while the other two are new. This is, to the best of our knowledge, the first infinite APN family given in univariate form to have been published since 2013.

In the proof, we characterize the APN-ness of the quadrinomials by the solvability of a system of equations (or, to be more precise, inclusions) of the form

$$\begin{cases} a^3(x^2 + x) \in \beta \cdot \mathbb{F}_{2^m} \\ a^{2^i+1}(x^{2^i} + x) \in \beta \cdot \mathbb{F}_{2^m}. \end{cases}$$

The quadrinomial in (1.12) is APN if and only if the above system does not have a solution $x \notin \mathbb{F}_2$ for any $0 \neq a \in \mathbb{F}_{2^n}$. The actual proof of the unsolvability of the system is somewhat technical, and we do not go into details here. We remark that the characterization of the APN-ness of (1.12) by the solvability of this system allows one to check whether a function of this form is APN much faster than by conventional means; this proved very helpful for searching for APN functions of this form over fields of high extension degree (up to 52) during the initial phase of our investigation.

1.7.5 Deciding EA-equivalence via invariants

As pointed out in Section 1.3, deciding the CCZ-equivalence of two given functions is a problem of great practical importance since it is a prerequisite for classifying APN functions and, in particular, for verifying that newly discovered instances are not equivalent to known ones. Since two quadratic or monomial APN functions are CCZ-equivalent if and only if they are EA-equivalent (see Section 1.3), and since the vast majority of known APN functions (with a single known exception over $\mathbb{F}_{2^6}$) are CCZ-equivalent to quadratic functions or monomials; and since most known constructions and search procedures tend to output quadratic functions (which, in turn, is due to the fact that constructing non-quadratic APN functions is very difficult), being able to test EA-equivalence is almost as useful in practice as being able to test the more general CCZ-equivalence. Traditionally, the only known tests for CCZ-equivalence and EA-equivalence in the general case reduce the problem to that of testing the isomorphism of their associated linear codes. As previously discussed, this has a number of shortcomings, including a high time and space complexity, and the possibility (depending on the implementation) of false negatives. Algorithms for testing EA-equivalence in some specialized cases without going through linear codes have been developed [8, 27, 60], but these are not useful for performing classification since they only concern very specific cases of EA-equivalence.

In Paper V, we propose a direct algorithm for testing the EA-equivalence of two given (n,n)-functions. To the best of our knowledge, this is the first such algorithm that does not rely on coding theory, along with a very recently presented algorithm for testing EA-equivalence by means of the so-called Jacobian matrices [31], which was developed independently, is based on fundamentally different principles, and can be applied to different cases than the one from Paper V (the algorithm from [31] works for quadratic functions over $\mathbb{F}_{2^n}$ with n of any parity, while the one from Paper V works for functions of any algebraic degree, but only in the case of even dimensions). Our algorithm is based on the computation of an EA-invariant (the multiplicities of the multiset Σ_F^k, which is also introduced in the same paper). In contrast to the code-theoretic tests, it uses only basic arithmetic and logic operations, which makes it easy and efficient to implement on any general-purpose programming language. The design of the algorithm is naturally parallelizable, and the results of a number of the operations that it performs can be precomputed for representatives from the known APN functions to further reduce the computation time.

The algorithm works for (n,n)-functions of any dimension n, but is only useful for even n since it defaults to an exhaustive search over all affine functions A_1, A_2, A from (1.8) in the odd case; for even dimensions, on the other hand, the running time is quite

good, and the algorithm can readily be used in practice.

Given an (n,n)-function F, the multiset Σ_F^k is defined as

$$\Sigma_F^k = \left\{ \sum_{i=1}^{k} F(x_i) : (x_1, x_2, \ldots, x_k) \in (\mathbb{F}_{2^n})^k : \sum_{i=1}^{k} x_i = 0 \right\};$$

that is, Σ_F^k consists of the sums of F over all k-tuples $(x_1, x_2, \ldots, x_k)$ of elements from $\mathbb{F}_{2^n}$ that add up to zero. We show that the multiplicities of the elements in this multiset are invariant under EA-equivalence for any even value of k. Since for $k = 2$ all k-tuples trivially add up to 0 under F, $k = 4$ is the smallest even value of k for which the invariant makes sense; for this reason, we mostly concentrate on Σ_F^4 in our paper.

Let $m_F^4(x)$ denote the multiplicity of an element $x \in \mathbb{F}_{2^n}$ in Σ_F^4. The idea of the algorithm is that if two (n,n)-functions F and G are EA-equivalent via $A_1 \circ F \circ A_2 + A = G$ as in (1.8), then A_1 must map x to an element y such that $m_F^4(x) = m_G^4(y)$. This allows us to quite significantly reduce the number of possible choices for A_1 in (1.8); in some cases, this reduction is so significant that only one or two possible choices for A_1 remain.

For each guess of A_1 among the remaining choices, we can compose both sides of (1.8) with A_1^{-1} to obtain a relation of the form

$$F \circ A_2 + A' = G',$$

where $A' = A_1^{-1} \circ A$ and $G' = A_1^{-1} \circ G$. We can further reduce A_2 to a linear function L_2 by guessing the constant term $A_2(0)$; in the case of quadratic functions, we can, in fact, assume that A_2 is linear without loss of generality. We thus have

$$F' \circ L_2 + L = G'',$$

where $F'(x) = F(x + A_2(0))$, $G''(x) = G'(x) + A'(0)$, and $L_2(x) = A_2(x) + A_2(0)$ and $L(x) = A(x) + A(0)$ are the linear parts of A_2 and A, respectively. A similar strategy to the one used when guessing A_1 can now be employed to reduce the number of choices for L_2. More precisely, for F' and G'' as given above, we have for any $t \in \mathbb{F}_{2^n}$ that

$$O_{F'}(t) = \{(L_2(x_1), L_2(x_2), L_2(x_3)) : (x_1, x_2, x_3) \in O_{G''}(t)\},$$

where

$$O_F(t) = \{(x_1, x_2, x_3) \in \mathbb{F}_{2^n}^3 : F(x_1) + F(x_2) + F(x_3) = t\}.$$

Once again, this provides us with enough information about L_2 to reduce the number of possibilities sufficiently in order for an exhaustive search over the remaining candidates to be feasible. Once the values of A_1 and A_2 are known, the value of A in (1.8) (and thus, the exact form of the EA-equivalence between F and G, if it exists) can be uniquely reconstructed. Furthermore, the algorithm can be used to obtain all triples (A_1, A_2, A) that satisfy (1.8) for a given pair of (n,n)-functions F and G.

We remark that the choice of using quadruples in the definition of Σ_F^4 and the choice of using triples in the definition of O_F is not the only possibility, and we could have used larger tuples in both cases instead. Numbers smaller than 4 and 3, respectively, do not provide any useful information, since the sums in both cases collapse to a constant value. We have chosen k-tuples with the smallest possible values of k that make

sense since this typically corresponds to a faster computation, and since in our limited experiments we did not observe any advantage in using higher values of k. In this respect, we remark that in the paper we also show how the multiplicities $m_F^k(x)$ can be expressed and computed via the Walsh transform of F. This is advantageous when k is large (since the computation of $m_F^k(x)$ from the Walsh transform does not depend on the value of k, unlike a computation directly from the definition of Σ_F^k), or when one has a lookup table of the Walsh coefficients of F already available.

1.7.6 Generalization of a class of APN binomials to Gold-like functions

The Gold APN functions $F(x) = x^{2^i+1}$ over $\mathbb{F}_{2^n}$ with $\gcd(i,n) = 1$ are remarkable in many ways, even besides the fact that they provide some of the earliest known instances, and form one of the first known infinite families of APN functions. The Gold functions have a number of interesting properties that they share with many other known instances of APN functions; perhaps the most eloquent example of such a property is the extended Walsh spectrum whose value, as we have remarked in Section 1.4.1, is Gold-like for all but a very small number of APN instances that we currently know. We have also observed in Section 1.7.2 that the value of the CCZ-invariant Π_F introduced in Paper II is Gold-like for representatives from all currently known infinite families of quadratic APN functions (despite Π_F taking a very large number of distinct values over all known sporadic instances of quadratic APN functions). Another "Gold-like" property worth noting is that of the Gold functions being permutations over finite fields of odd extension degree, and being 3-to-1 functions when the extension degree is even.

The condition $\gcd(i,n) = 1$ is necessary for x^{2^i+1} to be APN over $\mathbb{F}_{2^n}$. Relaxing the condition to $\gcd(i,n) = t$, it can be seen that x^{2^i+1} is differentially 2^t-uniform over $\mathbb{F}_{2^n}$. What is more, all derivatives of x^{2^i+1} are 2^t-to-1 functions in this case. Functions having the property that all their derivatives are 2^t-to-1 for some natural number t are sometimes referred to as differentially two-valued (referring to the fact that their differential spectrum contains only two distinct values, viz. 0 and 2^t). It is clear that any quadratic power function (and the "relaxed" Gold functions, in particular) must be differentially two-valued. More interestingly, there are polynomial (as opposed to monomial) functions that have this property. Studying such functions is important for several reasons, one of which is that they might correspond to a relaxation of an APN construction, and therefore point the way to new families and instances of APN functions.

The binomial $x^3 + wx^{258}$ (for some appropriate choice of w) is APN over $\mathbb{F}_{2^{12}}$, and is one of the earliest known instances of APN functions CCZ-inequivalent to monomials. In [22], this instance is generalized into two infinite families of APN functions: one (which we shall refer to as $\mathcal{F}_3$) over $\mathbb{F}_{2^n}$ with $3 \mid n$, and one (which we shall designate $\mathcal{F}_4$) over $\mathbb{F}_{2^n}$ with $4 \mid n$; these were the first infinite APN families CCZ-inequivalent to monomials. More precisely, both families have the univariate form

$$F(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}},$$

where i, s and k are positive integers; the conditions on i, s and k then differ between

$\mathcal{F}_3$ and $\mathcal{F}_4$. In the former case, we have $s \leq 4k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, $i = sk \pmod 3$, $m = 3-i$, and w is a primitive element of $\mathbb{F}_{2^n}$. In the latter case, we must have $s \leq 4k-1$, $\gcd(k,2) = \gcd(s,2k) = 1$, $i = sk \pmod 4$, $m = 4-i$, and w is (once again) a primitive element of $\mathbb{F}_{2^n}$. The Walsh spectra of both families are completely determined in [11].

In [13], it is shown that family $\mathcal{F}_3$ can be generalized into a family of differentially 2^t-uniform differentially two-valued functions by relaxing the condition $\gcd(s,3k) = 1$ to $\gcd(s,3k) = t$. In this sense, $\mathcal{F}_3$ behaves in the same way as the Gold functions. The question of whether the same is possible for family $\mathcal{F}_4$ has, to the best of our knowledge, remained open since the publication of [13] in 2012.

In Paper VI, we show that $\mathcal{F}_4$ can be generalized into a family of 2^t-differentially uniform and differentially two-valued functions in a manner similar to $\mathcal{F}_3$ by relaxing the condition $\gcd(s,2k) = 1$ to $\gcd(s,2k) = t$. We also compute an upper bound on the magnitude of the Walsh coefficients of F from this family, showing that $|W_F(a,b)| \leq 2^{2k+t}$ for any $a,b \in \mathbb{F}_{2^n}$ with $a \neq 0$; and, consequently, that the nonlinearity of any function from the described relaxation of $\mathcal{F}_4$ over $\mathbb{F}_{2^n}$ satisfies $\mathcal{NL}(F) \geq 2^{n-1} - 2^{2k+t-1}$.

Furthermore, we present a counterexample showing that such a generalization of APN families into differentially two-valued functions is not possible in general, and so the families $\mathcal{F}_3$ and $\mathcal{F}_4$ are exceptional in this respect. In order to do this, we consider the infinite family of APN quadrinomials introduced in Paper IV and given in (1.12) in Section 1.7.4. We note that this family behaves like the Gold functions in a number of ways, such as being 3-to-1, and having a Gold-like value of the extended Walsh spectrum and the multiset Π_F. We attempt to generalize it in a similar way by relaxing the conditions on the parameters i and k. We computationally go through all functions of the form

$$F(x) = x^{2^j+1} + \beta \left(x^{2^i+1}\right)^{2^k} + \beta^2 \left(x^{2^j+1}\right)^{2^m} + (x^{2^i+1})^{2^{m+k}}$$

over $\mathbb{F}_{2^{2n}}$ with $6 \leq 2n \leq 14$, for all possible choices of i, j, and k; we also disregard the condition $3 \nmid 2n$, and allow the extension degree $n = 2m$ to be a multiple of three. We restrict the choice of k to $k \in \{0,1\}$ since, as we have computationally observed in Paper IV, distinct choices of k having the same parity always give CCZ-equivalent functions over $\mathbb{F}_{2^{10}}$. Over all choices of k,n,i,j, we do not find any differentially two-valued functions (except APN functions, which all belong to the known CCZ-classes); the only exception is for $n = 12$, where every pair (i,j) with $2 \leq i,j \leq 12$ and i,j even gives a 4-to-1 function. Since we do not observe the same behavior over any other of the tested dimensions, this suggests that a generalization is not possible. Thus, we have strong computational evidence that generalizations of quadratic APN functions to differentially two-valued ones like in the case of $\mathcal{F}_3$, $\mathcal{F}_4$ and the Gold functions are not, in general, possible.

1.7.7 Partially APN Boolean functions and classes of functions that are not APN infinitely often

Recall that an (n,n)-function F is APN if and only if

$$D_a F(x) = D_a F(y)$$

implies $x = y$ or $x = a + y$ for any $x, y \in \mathbb{F}_{2^n}$ and any $0 \neq a \in \mathbb{F}_{2^n}$. This naturally leads to a notion of partial APN-ness, originally introduced in Paper VII. We say that an (n,n)-function F is x_0**-APN** for some $x_0 \in \mathbb{F}_{2^n}$, or simply **partially APN (pAPN)**, when the exact value of x_0 is irrelevant or is understood from the context, if the equation

$$D_a F(x) = D_a F(x_0)$$

only has $x \in \{x_0, a + x_0\}$ as solutions for any $0 \neq a \in \mathbb{F}_{2^n}$. From the above discussion, it is clear that an (n,n)-function F is APN if and only if it is x_0-APN for all $x_0 \in \mathbb{F}_{2^n}$.

Our original motivation for investigating pAPN functions was as an auxiliary tool for approaching the problem of the maximum algebraic degree of (n,n)-functions (see Sections 1.7.1 and 1.7.2). Since pAPN-ness is a weaker condition than APN-ness (in the sense that any APN function must also be x_0-APN for all possible values of x_0), non-existence results on pAPN functions automatically imply non-existence results on APN functions; however, characterizing pAPN-ness may be easier due to its simpler definition. The same approach could potentially also be applied to non-existence results for e.g. APN permutations. On the other hand, constructing pAPN-functions of higher algebraic degree may prove to be a natural step in the direction of finding new instances of APN functions CCZ-inequivalent to monomials and quadratic functions (in the sense that we might expect to find necessary or sufficient conditions for e.g. cubic or quartic functions to be x_0-APN, and only search for APN functions among the ones that satisfy these conditions).

After introducing the notion of an x_0-APN function, we characterize this property by means of the Walsh transform as in the case of APN functions. These results are used to investigate the properties of functions obtained from x_0-APN ones by modifying one of their outputs (similar to the approach applied to APN functions discussed in [21] and generalized in Papers I and II).

Further, we consider the case of monomials, and show that for any two non-zero $x_0, x_1 \in \mathbb{F}_{2^n}$, a monomial (n,n)-function F is x_0-APN if and only if it is x_1-APN. We find several constructions of 0-APN (but not necessarily APN) monomial functions. Furthermore, we show that any 1-APN monomial must necessarily be 0-APN, and therefore APN as well. In this sense, APN-ness coincides with x_0-APN-ness for monomials for any non-zero value of x_0. We show that a similar property holds for quadratic functions, i.e. if F is a quadratic (n,n)-function and $x_0 \in \mathbb{F}_{2^n}$, we show that F is APN if and only if F is x_0-APN (note that here x_0 can also be zero). The notions of APN-ness and partial APN-ness therefore coincide in the case of quadratic functions. This is not true in general, and we computationally find examples of functions that are x_0-APN for various numbers of elements $x_0 \in \mathbb{F}_{2^n}$. Finally, in a similar vein to the work of Rodier and his collaborators, e.g. [1, 47, 64], we construct classes of functions that are not 0-APN over $\mathbb{F}_{2^n}$ for infinitely many dimensions n.

1.7.8 Partially APN functions with APN-like polynomial representations

This paper builds upon the foundations laid out in Paper VII and explores further properties and constructions of partially APN functions. A notable result presented in the paper is that the number of elements $x_0 \in \mathbb{F}_{2^n}$ for which an (n,n)-function F is x_0-APN

is invariant under CCZ-equivalence. Although this invariant is clearly not useful for classifying APN and AB functions (which is why we do not mention it in Section 1.4), it has the potential to be helpful in the classification of other types of functions (say, differentially 4-uniform functions). More importantly, this invariance shows that it is not possible to increase (or reduce) the number of $x_0 \in \mathbb{F}_{2^n}$ for which a given function F is x_0-APN by traversing its CCZ-equivalence class.

Further, we investigate partially APN (but not APN) monomials; by the discussion in Section 1.7.7, this is equivalent to 0-APN but not APN monomials. As a motivating example, we show that $x \mapsto x^{21}$ is 0-APN over $\mathbb{F}_{2^n}$ if and only if n is not a multiple of 6. We then obtain further conditions and non-existence results on the 0-APN-ness of monomials. In particular, we show that generalizations of some of the known infinite families of power APN functions (in which conditions are relaxed so that the functions are not APN) cannot be 0-APN either.

We then investigate binomials, and construct an infinite family of 1-APN but not 0-APN, differentially 4-uniform binomials. These binomials serve as a counterexample showing that the behavior of partially APN quadratic functions (which are x_0-APN if and only if they are x_1-APN for any two values x_0 and x_1) does not extend to the general case.

Finally, we investigate functions of the form

$$F(x) = x(Ax^2 + Bx^{2^k} + Cx^{2^{k+1}}) + x^2(Dx^{2^k} + Ex^{2^{k+1}}) + Gx^{2^{k+1}+2^k}$$

over $\mathbb{F}_{2^n}$ with $n = 2k$ and $A, B, C, D, E, F, G \in \mathbb{F}_{2^n}$, and prove that this function is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$ in a number of cases (mostly, when all but two of the coefficients A, B, C, D, E, F, G are zero). This particular polynomial form was suggested by Dillon [15] as a potential source of APN and differentially 4-uniform functions, so it would be reasonable to consider it as a source of partially APN functions as well.

1.7.9 On a relationship between Gold and Kasami functions and other power APN functions

As we remarked in Section 1.5, the monomial APN functions from Table 1.2 are the earliest known instances of APN functions and infinite families, and are some of the most well studied by far. Despite this, a number of questions remain open even here. For one, a well-known conjecture by Dobbertin from 2000 states that the list of APN monomials in Table 1.2 is complete up to CCZ-equivalence [43]; that is, any APN monomial (whether it belongs to an infinite family or not) must be CCZ-equivalent to an instance from one of the families in Table 1.2. Despite its simple formulation, this has proved to be an extremely complicated problem. It has been shown that any exponent t for which x^t is APN over $\mathbb{F}_{2^n}$ for infinitely many n must be of the form $t = 2^i + 1$ or $t = 2^{2i} - 2^i + 1$, i.e. x^t must belong to either the Gold or the Kasami power families [50]. Furthermore, Dobbertin's conjecture has been computationally verified for a number of dimensions n: for $n \leq 24$ by Canteaut according to [43]; and for $n \leq 34$ and $n = 36, 38, 40, 42$ by Edel (unpublished).

Another conspicuous open problem is that of computing the Walsh spectrum of the Dobbertin power function. What makes this particularly noteworthy is that the Walsh spectra of the remaining five infinite families of APN monomials have already been

computed, while in the case of the Dobbertin function we did not previously even have a conjecture about the form of its Walsh spectrum.

One of the reasons that working with the infinite families of APN monomials (with the notable exception of the Gold functions) is difficult, is that they have a high algebraic degree, which makes their univariate representations difficult to handle. In fact, a quick inspection of Table 1.2 reveals that the Gold and Welch families are the only ones with a constant algebraic degree; the former being quadratic, and the latter being cubic. The degree of the Kasami functions $x^{2^{2i}-2^i+1}$ is $i+1$, and thus depends on the parameter i; while the degree of the Niho, inverse, and Dobbertin functions depends on (and grows with) the dimension n.

As in the general case of e.g. APN functions, one potential method for approaching this problem is to consider alternative representations of the monomial functions. In Paper IX, we investigate several ways of simplifying the representations of the known infinite families of APN monomials; we focus particularly on the Welch, Niho, and Dobbertin functions, whose "canonical" definition as given in Table 1.2 is particularly difficult to work with in proofs and theoretical arguments due to the high algebraic degree.

We recall that in the case of odd n, the exponent of the Kasami function $2^{2i} - 2^i + 1$ can be written as $(2^{3i}+1)/(2^i+1)$, i.e. as the composition of the quadratic function $x^{2^{3i}+1}$ and the inverse of the quadratic function x^{2^i+1}, and that this can be used to give a simple proof of the AB-ness of the Kasami functions over $\mathbb{F}_{2^n}$ [35]. We proceed to investigate whether a similar simplified representation can be found for the remaining infinite families of APN monomials. We obtain such representations (as the composition of a power function and the inverse of another power function) for the Niho and Dobbertin functions, and show that they are optimal in the sense that taking any combination of two power functions of lesser algebraic degree cannot represent the function in question. In particular, we show that the "canonical" representation of the Welch function is already optimal; that the Niho functions can be expressed as the composition of x^3 and the inverse of a cubic power function; and that the Dobbertin function is cyclotomic-equivalent to the composition of a cubic power function and the inverse of a quadratic power function.

We also present a construction in which two power functions x^i and x^j are composed with a linear polynomial L to obtain a new function G via

$$G(x) = x^i \circ L \circ x^j. \tag{1.13}$$

Note that this composition somewhat resembles the definition (1.8) of EA-equivalence in which a function F is composed with two affine (or linear, in particular cases) functions on the left and on the right. We observe, however, that even when x^i and x^j belong to the same CCZ-equivalence class, (1.13) can give an APN function G that is CCZ-equivalent to a monomial APN function, but CCZ-inequivalent to x^i and x^j. For instance, we observe that taking x^i to be the Gold function x^{2^i+1} and x^j to be its inverse $(x^{2^i+1})^{-1}$, the composition $x^i \circ L \circ x^j$ is CCZ-equivalent to the Kasami function $x^{2^{2i}-2^i+1}$ for some appropriate choice of L. When $i = 1$, the Gold and Kasami functions with parameter i are both x^3; but for values of i greater than 1, the Gold and Kasami functions are distinct and CCZ-inequivalent. In this way, the composition (1.13) allows us to express in a simple way a representative from one infinite family of APN power

functions using representatives from another infinite family of power APN functions that are CCZ-inequivalent to it. We conduct a computational search over all possible choices of i and j in (1.13) and all linear polynomials L with coefficients in $\mathbb{F}_2$. Based on the experimental data, we formulate several theoretical constructions that describe how two power functions can be combined to obtain an APN function in this way. Besides the case described above (in which a Gold function and its inverse give a Kasami function), we can combine a Gold function and the inverse of another Gold function (satisfying certain conditions) and obtain a Kasami function (in one case) or the inverse of a Kasami function (in another case); we can combine a Gold function and its inverse to obtain the same CCZ-class of the input Gold function; and, likewise, we can combine the inverse function with itself to go back to the inverse function (up to CCZ-equivalence). We note that our theoretical observations completely exhaust all cases found by computational search.

Finally, we compute the Walsh spectrum of the Dobbertin function over $\mathbb{F}_{2^n}$ for all dimensions up to $n = 5m = 35$, and conjecture its exact form. More precisely, we conjecture that the Walsh spectrum of the Dobbertin power function over $\mathbb{F}_{2^n}$ for $n = 5m$ has the form

$$\{0, 2^{2m}(2^m+1), \pm 2^{5k-2}, \pm a \cdot 2^{2m} \ : \ 1 \le a \le k \cdot (k+1), a \text{ odd}\}$$

for any natural number k, where $m = 2k-1$; and it has the form

$$\{0, -2^{2m}(2^m+1), \pm 2^{5k}, \pm 2^{5k+1}, \pm a \cdot 2^{2m} \ : \ 1 \le a \le k \cdot (k+2), a \text{ odd}\}$$

for any natural number k, where $m = 2k$. As far as we know, no conjectures or computational data of this kind are known to date, and so the above is a step towards computing the Walsh spectrum of the Dobbertin functions, and resolving this open problem.

1.8 Conclusion and future work

The aim of the PhD project was to investigate the properties of cryptographically optimal functions (and APN and AB functions, in particular) and to find new constructions thereof. The work presented in the included papers documents our results and efforts to this end. In particular, in Paper IV we have constructed a new infinite family of APN functions that generalizes the binomial $x^3 + \beta x^{36}$ over $\mathbb{F}_{2^{10}}$ known since 2006. This provides the first new infinite family of APN functions in univariate form since 2013; and, at the same time, resolves the problem of classifying the aforementioned binomial into an infinite APN family (which had been open since its introduction in 2006).

Besides this new infinite construction, we have obtained many further results on the properties, structure, and classification of APN and AB functions. Most significantly, we have:

- found a new, useful, and very efficiently computable invariant under CCZ-equivalence, viz. the multiset Π_F (Paper II); based on this, we have
- found a lower bound on the Hamming distance between a given APN function and its closest APN "neighbors" (Paper II), and computed its value for the list of known APN functions; in addition, we have given an exact formula for the value of this bound in the case of the Gold APN function x^3;

- specialized the matrix method from [71] to the case of functions with binary coefficients in their univariate representations, and obtained a complete classification of APN functions of this type up to dimension 9; in particular, we have found two previously unknown instances of such functions for $n = 9$ (Paper III);
- developed an approach in which power APN functions from one infinite family can be expressed using (CCZ-inequivalent) power APN functions from another family (Paper IX); this promises to be a good approach for investigating Dobbertin's conjecture on the non-existence of APN power functions CCZ-inequivalent to the known families;
- developed an efficient algorithm operating from first principles for computationally deciding the EA-equivalence of two vectorial Boolean functions over any finite field of even extension degree; as a byproduct, we have also introduced a new invariant under EA-equivalence, namely, the multiplicities of the multiset Σ_F^k;
- introduced a new class of functions, viz. partially APN functions, that can potentially be used to approach complex non-existence problems for APN functions, and developed theoretical and computational tools for characterizing and investigating such functions (Papers VII and VIII).

Nonetheless, there are many open questions and avenues for further research. In the following, we highlight some of the most interesting topics left for future work.

1.8.1 On the distance between APN functions

The lower bound shown in Paper II on the Hamming distance from a given APN function to a closest (but distinct) APN function is not tight (although we have observed some particular APN functions over small finite fields when it can be attained with equality); the bound thus stands to be improved. What is particularly interesting is that while the lower bound is invariant under CCZ-equivalence, the actual distance to the closest APN function is not.

Proposition 2 in Paper II provides six necessary and sufficient (when taken together) conditions for a function G obtained from F by changing K of its output values to be APN. In the paper, we have developed a simple (but quite effective) algorithm for filtering out the possible shifts; that is, given a function F and a set $U = \{u_1, u_2, \ldots, u_K\}$, the algorithm can rule out a lot of values of the shifts $v_1, v_2, \ldots, v_K$ for which the resulting function can never be APN. This algorithm is based on one of the conditions in Proposition 2. A more sophisticated search procedure can be developed by incorporating the remaining conditions from Proposition 2 in a similar way. This is more technically challenging, but once such a search procedure is available, it could be used to search for new APN functions by changing outputs in known ones despite the large Hamming distance between them.

For the above algorithm, we assume that the set $U = \{u_1, u_2, \ldots, u_K\}$ for which the outputs of F will be modified is known. In practice this is, of course, not the case, and so a further natural question is to find conditions describing those sets U that lead to an APN function via some combination of shifts $v_1, v_2, \ldots, v_K$.

In the case of the Gold function x^3 over $\mathbb{F}_{2^n}$, we have derived an exact formula for the lower bound on the Hamming distance for any value of n. Doing the same for other functions would be an interesting result, although we expect that the calculation will be more involved.

We have observed that although the multiset Π_F can take many distinct values when evaluated over the known APN instances, it appears to always take the same value for all representatives from the known infinite families (except the Dobbertin and inverse power functions). It would thus be interesting to find an infinite family of APN polynomial (as opposed to monomial) functions taking some other value of Π_F.

Finally, it might be possible to derive a lower bound on the Hamming distance between other types of functions, such as planar functions, differentially 4-uniform functions, etc. using similar techniques.

1.8.2 On the matrix method

The general matrix method considered in [71] can be used to construct any purely quadratic function (and thus, any quadratic function up to EA-equivalence). In Paper III, we have specialized this method to the case of quadratic functions with binary coefficients in their univariate representation; thus, these are (n,n)-functions F satisfying $F(x^2) = F(x)^2$ for all $x \in \mathbb{F}_{2^n}$. This restriction of the general method to a specific subclass of functions drastically reduces the size of the search space, and makes it possible to classify (up to CCZ-equivalence) all such functions up to dimension 9 (for comparison, quadratic APN functions have only been classified up to dimension 7).

A natural idea is thus to specialize the method to a different subclass of functions, e.g. functions over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^k}$, where $k > 1$ is some divisor of n; these functions would then satisfy $F(x^{2^k}) = F(x)^{2^k}$, which could be used to impose restrictions on the matrices representing functions of this type, and to reduce the search complexity in the same way as in the case of $k = 1$. Another natural extension of the same principle would be to consider other known representations of (n,n)-functions (for instance, some of the ones discussed in Section 1.1) and to see if restricting to a subclass of functions makes an exhaustive search based on those other representations feasible in practice.

In addition, some of the newly found invariants described in Section 1.4 are very efficient and discriminating; in particular, the orthoderivatives, discussed in Section 1.4.2, are an extremely useful tool for classifying quadratic APN functions under EA-equivalence that appears to have almost the same distinguishing capability as an actual test for EA-equivalence. This suggests that the classification of functions found by such methods up to CCZ-equivalence is realistic even for relatively large dimensions. The issue is then to restrict the representation enough so that the total number of functions that can be expressed is sufficiently small to be computationally exhausted.

1.8.3 On the composition of power functions

The method from Paper IX that allows us to obtain the CCZ-equivalence class of one power APN function from that of another is a promising development that may provide new constructions of APN and, possibly, other classes of functions. Furthermore, the

method could be used to simplify proofs of certain properties (including APN-ness) of power functions that are very technical otherwise, and it could be used to approach Dobbertin's conjecture that the infinite monomial families from Table 1.2 exhaust all possible APN power functions (up to cyclotomic equivalence).

Since this composition method is at a rather early stage, there is a lot of room for future work. The method can be extended in several different ways, e.g. by allowing arbitrary polynomials (instead of merely power functions) to be used in the composition; by allowing the linear polynomials in the construction to have non-binary coefficients; by adapting the method to classes of functions other than APN; and so forth.

1.8.4 On partially APN functions

Since the notion of partial APN-ness was introduced only very recently in Papers VII and VIII, it is natural that there are many open questions and directions of research. One particularly interesting direction would be finding constructions of partially APN permutations. As previously noted, constructing APN permutations is quite difficult; in particular, only a single instance of an APN permutation of $\mathbb{F}_{2^n}$ for even n is known (for $n = 6$), and resolving the existence of such permutations for larger values of n is arguably the biggest open problem in the study of APN functions. Since the concept of a partially APN function is a weakening of that of an APN function, it would be natural to expect that the construction of partially APN permutations would be more feasible than that of APN permutations. On the other hand, since any APN function is partially APN as well, properties and non-existence results observed in the partially APN case may be applied to the APN case. In particular, it is reasonable to think that one of the reasons that we know so little about APN permutations is that we have very few examples of them. Finding instances of partially APN permutations would provide us with a lot more data, and make it easier to extrapolate useful properties and constructions. We have been able to find instances of partially APN permutations computationally but, so far, we have not succeeded in extending them to more general constructions.

More generally, any problem that is considered very hard in the APN case may be more tractable in the partial APN case; and resolving it might provide further insights into the structure and properties of APN functions. For instance, an interesting problem would be to find a secondary construction of partially APN functions; to the best of our knowledge, no such construction is known in the APN case, and obtaining a method to construct a partially APN function from another (CCZ-inequivalent to it) would be a remarkable result.

Bibliography

[1] Yves Aubry, Gary McGuire, and François Rodier. A few more functions that are not APN infinitely often. In *Finite fields: theory and applications*, volume 518, pages 23–31. Amer. Math. Soc. Providence, RI, 2010.

[2] Christof Beierle, Marcus Brinkmann, and Gregor Leander. Linearly self-equivalent APN permutations in small dimension. *IEEE Transactions on Information Theory*, 2021.

[3] Christof Beierle and Gregor Leander. New instances of quadratic APN functions. *arXiv preprint arXiv:2009.07204*, 2020.

[4] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 65–76. Springer, 1993.

[5] Thomas Beth, Deiter Jungnickel, and Hanfried Lenz. *Design Theory: Volume 1*. Cambridge University Press, 1999.

[6] Jürgen Bierbrauer. A family of crooked functions. *Designs, Codes and Cryptography*, 50(2):235–241, 2009.

[7] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, Jan 1991.

[8] Alex Biryukov, Christophe De Canniere, An Braeken, and Bart Preneel. A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In *International conference on the theory and applications of cryptographic techniques*, pages 33–50. Springer, 2003.

[9] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[10] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[11] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. Fourier spectra of binomial APN functions. *SIAM Journal on Discrete Mathematics*, 23(2):596–608, 2009.

[12] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[13] Carl Bracken, Chik How Tan, and Yin Tan. Binomial differentially 4 uniform permutations with high nonlinearity. *Finite Fields and Their Applications*, 18(3):537–546, 2012.

[14] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49:273–288, 2008.

[15] KA Browning, JF Dillon, MT McQuistan, and AJ Wolfe. APN polynomials and related codes. *Special volume of Journal of Combinatorics, Information and System Sciences*, 34:135–159, 2009.

[16] KA Browning, JF Dillon, MT McQuistan, and AJ Wolfe. An APN permutation in dimension six. *Finite Fields: theory and applications*, 518:33–42, 2010.

[17] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert Coulter, and Irene Villa. Generalized isotopic shift construction for APN functions. *Designs, Codes and Cryptography*, pages 1–14, 2020.

[18] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S Coulter, and Irene Villa. Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8):5299–5309, 2020.

[19] Lilya Budaghyan, Marco Calderini, and Irene Villa. On equivalence between known families of quadratic APN functions. *Finite Fields and Their Applications*, 66:101704, 2020.

[20] Lilya Budaghyan and Claude Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[21] Lilya Budaghyan, Claude Carlet, Tor Helleseth, Nian Li, and Bo Sun. On upper bounds for algebraic degrees of APN functions. *IEEE Transactions on Information Theory*, 64(6):4399–4411, 2018.

[22] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[23] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[24] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378, 2009.

[25] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[26] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.

[27] Lilya Budaghyan and Oleksandr Kazymyrov. Verification of restricted EA-equivalence for vectorial boolean functions. In *International Workshop on the Arithmetic of Finite Fields*, pages 108–118. Springer, 2012.

[28] Marco Calderini. On the EA-classes of known APN functions in small dimensions. *Cryptography and Communications*, 12(5):821–840, 2020.

[29] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *Rad HAZU, Matematičke znanosti*, 2021. to appear.

[30] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1):105–138, 2000.

[31] Anne Canteaut, Alain Couvreur, and Léo Perrin. Recovering or testing extended-affine equivalence. *arXiv preprint arXiv:2103.00078*, 2021.

[32] Anne Canteaut and Léo Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields and Their Applications*, 56:209–246, 2019.

[33] Claude Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes and Cryptography*, 59(1):89–109, 2011.

[34] Claude Carlet. *Boolean functions for cryptography and coding theory*. Cambridge University Press, 2021.

[35] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[36] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT 94*, volume 950, pages 356–365, 1994.

[37] Charles J Colbourn and Jeffrey H Dinitz. *Handbook of combinatorial designs*. CRC press, 2006.

[38] Joan Daemen and Vincent Rijmen. AES proposal: Rijndael, 1999.

[39] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[40] Itai Dinur and Adi Shamir. Breaking Grain-128 with dynamic cube attacks. In *International Workshop on Fast Software Encryption*, pages 167–187. Springer, 2011.

[41] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information & Computation*, 151(1):57–72, 1999.

[42] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[43] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5. *International Conference on Finite Fields and Applications*, pages 113–121, 2001.

[44] Daniel Edel and Alexander Pott. On the equivalence of nonlinear functions. In *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, volume 23, pages 87–103. IOS Press, 2009.

[45] Yves Edel, Gohar Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52(2):744–747, 2006.

[46] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.

[47] Eric Férard, Roger Oyono, and François Rodier. Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents. *Arithmetic, geometry, cryptography and coding theory*, pages 27–36, 2012.

[48] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[49] Faruk Göloğlu and Jiří Pavlů. On CCZ-inequivalence of some families of almost perfect nonlinear functions to permutations. *Cryptography and Communications*, pages 1–15, 2021.

[50] Fernando Hernando and Gary McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and apn functions. *Journal of algebra*, 343(1):78–92, 2011.

[51] Xiang-dong Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Discrete applied mathematics*, 154(2):313–325, 2006.

[52] Heeralal Janwa and Richard M Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.

[53] Konstantin Kalgin and Valeriya Idrisova. The classification of quadratic APN functions in 7 variables. *Cryptology ePrint Archive, Report 2020/1515*, 2020.

[54] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information & Computation*, 18(4):369–394, 1971.

[55] Lars R Knudsen. Truncated and higher order differentials. In *International Workshop on Fast Software Encryption*, pages 196–211. Springer, 1994.

[56] Philippe Langevin, Elif Saygi, and Zulfukar Saygi. Classification of APN cubics in dimension 6 over GF (2). http://langevin.univ-tln.fr/project/apn-6/apn-6.html.

[57] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[58] Kaisa Nyberg. Perfect nonlinear s-boxes. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 378–386, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[59] Kaisa Nyberg. Differentially uniform mappings for cryptography. *Lecture Notes in Computer Science*, 765:55–64, 1994.

[60] Ferruh Özbudak, Ahmet Sınak, and Oğuz Yayla. On verification of restricted extended affine equivalence of vectorial boolean functions. In *International Workshop on the Arithmetic of Finite Fields*, pages 137–154. Springer, 2014.

[61] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[62] Léo Perrin. How to take a function apart with SboxU. The 5th International Workshop on Boolean Functions and their Applications (BFA 2020), 2020.

[63] Gilles Piret, Thomas Roche, and Claude Carlet. PICARO–a block cipher allowing efficient higher-order side-channel resistance. In *International Conference on Applied Cryptography and Network Security*, pages 311–328. Springer, 2012.

[64] François Rodier. Functions of degree 4e that are not APN infinitely often. *Cryptography and Communications*, 3(4):227–240, 2011.

[65] Ana Sălăgean. Discrete antiderivatives for functions over $\mathbb{F}_p^n$. *Designs, Codes and Cryptography*, 88(3):471–486, 2020.

[66] V.M. Sidelnikov. On the mutual correlation of sequences. *Soviet Math. Dokl.*, 12:197–201, 1971.

[67] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes and Cryptography*, pages 1–11, 2019.

[68] Guobiao Weng, Yin Tan, and Guang Gong. On quadratic almost perfect nonlinear functions and their related algebraic object. In *Workshop on Coding and Cryptography*, pages 57–68. Citeseer, 2013.

[69] Satoshi Yoshiara. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics*, 35(3):461–475, 2012.

[70] Satoshi Yoshiara. Equivalences of power APN functions with power or quadratic APN functions. *Journal of Algebraic Combinatorics*, 44(3):561–585, 2016.

[71] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, codes and cryptography*, 73(2):587–600, 2014.

[72] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new APN functions through relative trace functions. *arXiv preprint arXiv:2101.11535*, 2021.

[73] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.

Chapter 2

Papers

Paper I

Changing APN Functions at Two Points

Nikolay S. Kaleyski
Cryptography and Communications, **vol.11, pp.1165 - 1184** (2019)

Changing APN Functions at Two Points

Nikolay Kaleyski

Department of Informatics, University of Bergen

Abstract

We investigate a construction in which a vectorial Boolean function G is obtained from a given function F over $\mathbb{F}_{2^n}$ by changing the values of F at two points of the underlying field. In particular, we examine the possibility of obtaining one APN function from another in this way. We characterize the APN-ness of G in terms of the derivatives and in terms of the Walsh coefficients of F. We establish that changing two points of a function F over $\mathbb{F}_{2^n}$ which is plateaued (and, in particular, AB) or of algebraic degree $deg(F) < n - 1$ can never give a plateaued (and AB, in particular) function for any $n \geq 5$.

We also examine a particular case in which we swap the values of F at two points of $\mathbb{F}_{2^n}$. This is motivated by the fact that such a construction allows us to obtain one permutation from another. We obtain a necessary and sufficient condition for the APN-ness of G which we then use to show that swapping two points of any power function over a field $\mathbb{F}_{2^n}$ with $n \geq 5$ can never produce an APN function. We also list some experimental results indicating that the same is true for the switching classes from [10], and conjecture that the Hamming distance between two APN functions cannot be equal to two for $n \geq 5$.

I. Introduction

A construction in which a given vectorial Boolean function is modified at one point are investigated in [2] in the context of the problem of the maximum algebraic degree of an APN function: given a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $u, v \in \mathbb{F}_{2^n}$, the one-point modification of F is defined as $G(x) = F(x) + (1 + (x + u)^{2^n-1})v$ so that $G(u) = F(u) + v$ and $G(x) = F(x)$ for $x \neq u$; the reasoning behind this is that any G with algebraic degree $\deg(G) = n$ can be expressed in this form. Although the question of the existence of an APN function of algebraic degree n over $\mathbb{F}_{2^n}$ remains open in general, a multitude of non-existence results are derived in [2] which support the conjecture that this is impossible. In this paper we examine a similar construction involving two points. More precisely, given $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we select $u_1, u_2 \in \mathbb{F}_{2^n}^*$ and $v_1, v_2 \in \mathbb{F}_{2^n}$, and define $G(x) = F(x) + (1 + (x + u_1)^{2^n-1})v_1 + (1 + (x + u_2)^{2^n-1})v_2$. We examine under what conditions G can be APN, especially when F itself is APN. We see that if F is plateaued or has $\deg(F) < n-1$, then G is not plateaued for $n \geq 5$; in particular, G is not AB if F is AB for $n \geq 5$. We also observe that if F is quadratic and not APN, then changing two points of F cannot produce an APN function either.

We also examine a special case in which the values of F at u_1 and u_2 are swapped, so that $G(u_1) = F(u_2)$ and $G(u_2) = F(u_1)$; under EA-equivalence, we also assume $u_1 = 0$ and $u_2 = 1$. This case is more tractable and is interesting in that it allows us to obtain one permutation from another. We characterize the APN-ness of $G(x) = F(x) + x^{2^n-1} + (x+1)^{2^n-1}$ in terms of the values $\sum_{y \in \mathbb{F}_{2^n}} \Delta_F(y, F(y)+1)$ and $\sum_{y \in \mathbb{F}_{2^n}} \Delta_F(y+1, F(y))$, where $\Delta_F(a, b)$ is the number of solutions x to $D_a F(x) = b$. We demonstrate how a formula for the first of these values can be derived for $F(x) = x^3$. More generally, we show that no APN function can be obtained by swapping the values at $u_1 = 0$ and $u_2 = 1$ of any power function over $\mathbb{F}_{2^n}$ for $n \geq 5$, and verify that this is also true for all APN functions from [10]. Based on these results, we

conjecture that swapping two points in an arbitrary APN function can never produce an APN function for $n \geq 5$.

The method of swapping two points has previously been investigated in the context of constructing 4-differentially uniform permutations from the inverse function [16]. Some basic properties are given in [16], and the authors generalize the construction by changing the values of points lying on a cycle of length greater than two [13]; in particular, they obtain some involutions using the method (see [9]).

II. Preliminaries

A. Representation of Vectorial Functions

An *n-dimensional Boolean function* is any function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. A *vectorial Boolean (n, m)-function* is any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. We focus only on the case $m = n$, in which it is more convenient to identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and to consider functions from $\mathbb{F}_{2^n}$ to itself. Any (n, n)-function has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, a_i \in \mathbb{F}_{2^n}.$$

Given a natural number $0 \leq i \leq 2^n - 1$ and its binary expansion $i = \sum_{k=0}^{n-1} 2^k i_k$ with $i_k \in \{0, 1\}$, its *two-weight* $w_2(i)$ is the number of nonzero terms in its binary expansion, i.e. $w_2(i) = \sum_{k=0}^{n-1} i_k$. The *algebraic degree* of F is then

$$\deg(F) = \max\{w_2(i) : 0 \leq i \leq 2^n - 1, a_i \neq 0\}.$$

Given an (n, n)-function F, its *component functions* are the functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ of the form $\mathrm{Tr}_1^n(bF(x))$ for $b \in \mathbb{F}_{2^n}$, where Tr_1^n is the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, which we denote simply by Tr if the dimension n is clear from the context.

B. Almost Perfect Nonlinear Functions and Bent Functions

Let F be an (n, n)-function. The *derivative of F in direction a* for any $a \in \mathbb{F}_{2^n}$ is the function $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined as $D_aF(x) = F(x) + F(a + x)$. The *differential sets* H_aF are the image sets of the derivatives of F, i.e. the sets of the form $H_aF = \{D_aF(x) : x \in \mathbb{F}_{2^n}\} = \{F(x) + F(a + x) : x \in \mathbb{F}_{2^n}\}$.

For convenience, we also define the *shifted derivative* $D_a^\beta F$ in direction $a \in \mathbb{F}_{2^n}$ with shift $\beta \in \mathbb{F}_{2^n}$ as the function $D_a^\beta F(x) = F(x) + F(a + x) + F(a + \beta)$ and the *shifted differential set* $H_a^\beta F$ in direction a with shift β as its image set, i.e. as $H_a^\beta F = \{D_a^\beta F(x) : x \in \mathbb{F}_{2^n}\} = \{F(x) + F(a + x) + F(a + \beta) : x \in \mathbb{F}_{2^n}\}$.

For any $a, b \in \mathbb{F}_{2^n}$, define $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}|$. Then, the *differential uniformity* of F is defined as $\Delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$. An (n, n)-function F is called *differentially δ-uniform* if $\Delta_F \leq \delta$. If $\delta = 2$, then F is called *almost perfect nonlinear* (APN). Note that $\Delta_F \geq 2$ for any (n, n)-function and hence APN functions are those with optimal differential uniformity.

APN functions over $\mathbb{F}_{2^n}$ can be characterized in several different ways. In this paper we focus on characterizations by means of the differential properties and the

power moments of the function's Walsh transform. The *Walsh transform* of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)}, \quad a \in \mathbb{F}_2$$

for any $a \in \mathbb{F}_{2^n}$. Also useful is the inverse Walsh transform formula

$$\sum_{a \in \mathbb{F}_{2^n}} W_f(a) = 2^n (-1)^{f(0)}. \tag{1}$$

The *Walsh transform* of an (n, n)-function F is defined by

$$W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(x))+\mathrm{Tr}_1^n(ax)} \tag{2}$$

for any $a, b \in \mathbb{F}_{2^n}$.

The Boolean functions $\mathrm{Tr}_1^n(bF(x))$ for $b \in \mathbb{F}_{2^n}^*$ are said to be the *component functions of* F. In this way, the values of the Walsh transform of an (n, n)-function can be seen as the values of the Walsh transform of the component functions of F.

In order to simplify notation, we will use $\eta(X)$, resp. $\eta_b(X)$ as shorthand for $(-1)^{\mathrm{Tr}_1^n(X)}$, resp. $(-1)^{\mathrm{Tr}_1^n(bX)}$ where X is an arbitrary expression and $b \in \mathbb{F}_{2^n}$. We also define the *equality indicator* $I(A, B)$, where A and B are some arbitrary expressions, as $I(A, B) = 1$ if $A = B$ and $I(A, B) = 0$ otherwise.

Given a set S, its characteristic function is denoted by $1_S(x)$ so that we have $1_S(x) = 1$ for $x \in S$ and $1_S(x) = 0$ for $x \notin S$. For a finite set $S = \{s_1, s_2, \ldots, s_k\}$ we write $1_{s_1,s_2,\ldots,s_k}(x)$ as shorthand for $1_{\{s_1,s_2,\ldots,s_k\}}(x)$.

With the above background, we can give the following classic characterizations of APN functions in terms of their Walsh transform.

Lemma 1 (see e.g. [8])**.** *Let F be an (n, n)-function. Then F is APN if and only if*

$$\sum_{a \in \mathbb{F}_{2^n}} \sum_{b \in \mathbb{F}_{2^n}^*} W_F^4(a, b) = 2^{3n+1}(2^n - 1).$$

Lemma 2 ([4], [5])**.** *Let F be an APN function over $\mathbb{F}_{2^n}$ satisfying $F(0) = 0$. Then*

$$\sum_{a,b \in \mathbb{F}_{2^n}} W_F^3(a, b) = 3 \cdot 2^{3n} - 2^{2n+1}.$$

If F is plateaued , this condition is necessary and sufficient for F to be APN (plateaued functions are defined in subsection II-C below).

The nonlinearity N_F of an (n, n)-function F is the minimum Hamming distance between its component functions and the affine functions. It measures the function's resistance to linear cryptanalysis [14] and equals

$$N_F = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |W_F(a, b)|. \tag{3}$$

An (n, m)-function F is called *bent* if $W_F(a, b) \in \{\pm 2^{n/2}\}$ for all $a \in \mathbb{F}_{2^n}$ and nonzero $b \in \mathbb{F}_{2^m}^*$. Clearly, bent functions can exist only for even values of n in which case they achieve optimum nonlinearity. Nyberg in [15] proved that (n, m)-bent functions exist if and only if n is even and $m \leq n/2$. When n is odd or $n = m$, the optimal functions

with respect to nonlinearity are the almost bent functions. An (n,n)-function F is called *almost bent* (AB) if its Walsh transform satisfies $W_F(a,b) \in \{0, \pm 2^{(n+1)/2}\}$ for any $a \in \mathbb{F}_{2^n}$ and nonzero $b \in \mathbb{F}_{2^n}$. Any AB function is APN, but not vice versa. However, for n odd, every quadratic APN function is also AB [6]; more generally, every plateaued APN function is also AB.

C. Plateaued Functions

A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called *plateaued* if its Walsh transform satisfies $W_f(a) \in \{0, \pm\mu\}$ for some positive integer μ called the *amplitude* of f. An (n,n)-function F is called *plateaued* if all of its component functions are plateaued and it is called *plateaued with single amplitude* if all of its component functions are plateaued and have the same amplitude.

The amplitude of a plateaued Boolean function f is always of the form 2^λ for some $\lambda \geq \frac{n}{2}$, due to the well-known *Parseval's identity* $\sum_{a \in \mathbb{F}_{2^n}} W_f^2(a) = 2^{2n}$.

Since the algebraic degree of a Boolean plateaued function in n variables with amplitude μ is upper bounded by $n - \lambda + 1$ [12], the algebraic degree of a plateaued (n,n)-function F is upper bounded by $\max_{b \in \mathbb{F}_{2^m}^*}(n - \lambda_b + 1)$ where λ_b is the amplitude of $\mathrm{Tr}_1^m(bF(x))$, $b \neq 0$, so that $W_F(a,b) \in \{0, \pm 2^{\lambda_u}\}$ for any $a \in \mathbb{F}_{2^n}$. Since there exists no bent (n,n)-function, this maximum is less than or equal to $n - (n+1)/2 + 1 = (n+1)/2$. Hence a plateaued function can have algebraic degree n, resp. $n-1$ only if $n \leq 1$, resp. $n \leq 3$.

D. Equivalence Relations of Functions

There are several equivalence relations of functions for which differential uniformity and nonlinearity are invariant. Due to these equivalence relations, having only one APN (respectively, AB) function, one can generate a huge class of APN (respectively, AB) functions.

Two (n,n)-functions F and F' are said to be

- *affine equivalent* (*linear equivalent*) if $F' = A_1 \circ F \circ A_2$, where A_1 and A_2 are affine (linear) permutations of $\mathbb{F}_{2^n}$;
- *extended affine equivalent* (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where A, A_1, A_2 are affine mappings over $\mathbb{F}_{2^n}$ and A_1, A_2 are permutations;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

It is obvious that linear equivalence is a particular case of affine equivalence, and that affine equivalence is a particular case of EA-equivalence. As shown in [6], EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence. The following proposition illustrates how EA-equivalence can be expressed in terms of CCZ-equivalence.

Proposition 1. *[3] Let F and F' be functions from $\mathbb{F}_{2^n}$ to itself. The function F' is EA-equivalent to the function F or to the inverse of F (if it exists) if and only if there*

exists an affine permutation $\mathcal{L} = (L_1, L_2)$ on $\mathbb{F}_2^{2n}$ such that $\mathcal{L}(G_F) = G_{F'}$ and the function L_1 depends only on one variable, i.e. $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.

It is worth mentioning some properties that remain invariant under CCZ-equivalence. Assuming that F and F' are CCZ-equivalent, we have:

- $\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\} = \{\Delta_{F'}(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ [1];
- if F is APN then F' is APN too;
- $N_F = N_{F'}$ [6];
- if F is AB then F' is AB too;
- if F is plateaued with single amplitude λ then F' is plateaued with the same single amplitude λ;
- if F is plateaued with different amplitudes then F' is not necessarily plateaued: it can happen that F' has no plateaued components at all. However, if F and F' are EA-equivalent then F' is plateaued with the same multi-set of amplitudes.

III. Changing two points of a given function

The properties of a construction that involves changing precisely one value of given function F in order to obtain a new function G are investigated in [2]. The main point of interest is the possibility of obtaining an APN function G in this manner, and particular attention is paid to the case when the given F is itself APN. This is motivated by the open problem of the existence of APN functions of algebraic degree n over the field $\mathbb{F}_{2^n}$, since if two functions F and G are at distance one, then at least one of them must be of algebraic degree n. Two main characterizations of the APN-ness of such functions G are obtained in [2], one involving the Walsh coefficients of F, and one based on the properties of the derivatives D_aF of F themselves. These characterizations are then applied in order to conclude that any G obtained by such a one-point change from a given F cannot be APN (except possibly for $n < 3$ in some cases) if F is a power, plateaued, quadratic or almost bent function . A number of additional non-existence results are also shown, which also agree with the conjecture that no APN function of algebraic degree n exists over $\mathbb{F}_{2^n}$.

This construction can naturally be generalized so as to encompass more than one point. Even for a small, fixed number of points $u_1, u_2, \ldots u_K$ at which the function is to be changed, however, the problem of the APN-ness of the resulting function seems very hard.

In the following we investigate whether, and under what conditions it is possible to obtain an APN function by changing the values of two distinct points in a given APN function F. More precisely, given two distinct elements u_1, u_2 from $\mathbb{F}_{2^n}$ and two arbitrary elements v_1, v_2 from $\mathbb{F}_{2^n}$, we are interested in the APN-ness of the function

$$G(x) = F(x) + 1_{u_1}(x)v_1 + 1_{u_2}(x)v_2 =$$

$$F(x) + (1 + (x + u_1))^{2^n-1}v_1 + (1 + (x + u_2))^{2^n-1}v_2 = \begin{cases} F(x) + v_1 & x = u_1 \\ F(x) + v_2 & x = u_2 \\ F(x) & x \notin \{u_1, u_2\}. \end{cases} \tag{4}$$

We take $v_1 = v_2$ and denote both v_1 and v_2 by v since assuming otherwise leads to the problem of the existence of APN functions of algebraic degree n already

discussed in [2]. We will also assume $v_1, v_2 \neq 0$ so that the distance between F and G is indeed equal to two.

A natural way to investigate the differential properties of G is to examine the derivatives D_aG and their expression via the derivatives D_aF of F. From the definition of G in (4) we can immediately see that for any $a \in \mathbb{F}_{2^n}^*$, the derivative D_aG takes the form

$$D_aG(x) = D_aF(x) + 1_{u_1,a+u_1}(x)v_1 + 1_{u_2,a+u_2}(x)v_2. \tag{5}$$

Recall that a function F over $\mathbb{F}_{2^n}$ is APN if and only if there do not exist elements $a \in \mathbb{F}_{2^n}^*$ and $x, y \in \mathbb{F}_{2^n}$ such that $D_aF(x) = D_aF(y)$ and $x + y \notin \{0, a\}$; this follows immediately from the definition. A characterization of the conditions under which G is APN can then be derived immediately from (5) by examining under what conditions such a triple of elements $(a, x, y) \in \mathbb{F}_{2^n}^3$ violating this condition may exist.

Proposition 2. *Let F be an (n, n)-function and let u_1, u_2 be two distinct points from $\mathbb{F}_{2^n}$. Let also v_1, v_2 be arbitrary elements from $\mathbb{F}_{2^n}$. Then the function*

$$G(x) = F(x) + 1_{u_1}(x)v_1 + 1_{u_2}(x)v_2$$

is APN if and only if all of the following conditions are satisfied for every derivative direction $a \in \mathbb{F}_{2^n}^*$:

(i) D_aF is 2-to-1 on $\mathbb{F}_{2^n} \setminus \{u_1, u_2, a + u_1, a + u_2\}$;
(ii) $D_aF(u_1) + D_aF(u_2) \neq v_1 + v_2$ unless $a = u_1 + u_2$;
(iii) $D_aF(x) + D_aF(u_i) \neq v_i$ unless $a = u_1 + u_2$ or $x \in \{u_1, u_2, a + u_1, a + u_2\}$, for $i \in \{1, 2\}$;
(iv) $D_{u_1+u_2}F(u_i) + D_{u_1+u_2}F(x) \neq v_1 + v_2$ unless $x \in \{u_1, u_2\}$, for $i \in \{1, 2\}$.

Proof. From the definition, G is APN if and only if $D_aG(x) = D_aG(y)$ implies $a = 0$ or $x + y \in \{0, a\}$ for any $a, x, y \in \mathbb{F}_{2^n}$. We now examine under what circumstances such an equality may occur.

Suppose that $D_aG(x) = D_aG(y)$ for some $a, x, y \in \mathbb{F}_{2^n}$ with $a \neq 0$, $x \neq y$ and $x \neq a + y$. Depending on whether x and y are in $\{u_1, u_2, a + u_1, a + u_2\}$, we examine the following cases:

(i) If neither x nor y is in $\{u_1, u_2, a+u_1, a+u_2\}$, then $D_aG(x) = D_aG(y)$ is equivalent to $D_aF(x) = D_aF(y)$. However, due to the assumption $x \notin \{y, a+y\}$, this means that D_aF itself is not 2-to-1.
(ii) If say $x \in \{u_1, a + u_1\}$ and $y \in \{u_2, a + u_2\}$, then $D_aG(x) = D_aG(y)$ becomes $D_aF(u_1) + D_aF(u_2) = v_1 + v_2$ since $x \neq y + a$ implies that $a \neq u_1 + u_2$.
(iii) If say $x \in \{u_1, a + u_1\}$ but $y \notin \{u_1, u_2, a + u_1, a + u_2\}$ and $a \neq u_1 + u_2$, then $D_aG(x) = D_aG(y)$ is equivalent to $D_aF(u_1) + D_aF(y) = v_1$.
(iv) If $a = u_1 + u_2$ and say $x \in \{u_1, u_2\}$, $y \notin \{u_1, u_2\}$, then $D_aG(x) = D_aG(y)$ becomes $D_aF(u_1) + D_aF(y) = v_1 + v_2$.

Thus, all of the four conditions listed in the statement of the proposition are clearly necessary for G to be APN. However, they are also sufficient since if $D_aG(x) = D_aG(y)$ is true for some $a, x, y \in \mathbb{F}_{2^n}$, with $a \neq 0$ and $x + y \notin \{0, a\}$, then one of these four cases must necessarily occur. □

One can easily find functions F and elements u_1, u_2, v_1, v_2 satisfying the conditions of Proposition 2 in $\mathbb{F}_{2^n}$ with $n \leq 4$. For example, taking $F(x) = x^3$ over $\mathbb{F}_{2^4}$, $u_1 = 0$,

$u_2 = \alpha^k$ and $v_1 = v_2 = \alpha^{3k}$ for some positive integer k, it is obvious that conditions (i) and (ii) of the proposition are immediately satisfied (on account of F being APN), and it can be checked computationally that conditions (iii) and (iv) are satisfied as well. Note that due to $v_1 = v_2$, this corresponds to the case of "swapping" two points described in Section V. More generally, for any $u_1, u_2 \in \mathbb{F}_{2^4} \times \mathbb{F}_{2^4}$ with $u_1 \neq u_2$, there exists precisely one pair v_1, v_2 such that G from the statement of Proposition 2 is APN; furthermore, $v_1 = v_2$ in all such cases.

For dimensions $n \geq 5$, the question of whether an APN function can be obtained by changing (or, in particular, swapping) two of the values of a another APN function remains unsolved. We present some partial negative results in Sections V and VI, but the problem of the minimum distance between APN functions remains open.

Corollary 1. *Let F be a quadratic function over $\mathbb{F}_{2^n}$. If F is not APN then $G(x) = F(x) + 1_{u_1}(x)v_1 + 1_{u_2}(x)v_2$ is not APN either.*

Proof. If F is quadratic, then all derivatives D_aF for $a \neq 0$ are 2^{s_a}-to-1 functions, with $1 \leq s_a \leq n$. Furthermore, if F is not APN, then for some a we must have $s_a > 1$. Hence G is not APN by condition (i) in Proposition 2. □

IV. Characterization by Means of the Walsh Transform

From (4) and assuming $v_1 = v_2 = v$, the Walsh coefficients of G can be expressed as $W_G(a,b) = W_F(a,b) + [\eta(bv) - 1][\eta(bF(u_1) + au_1) + \eta(bF(u_2) + au_2)]$. The difference of $W_F(a,b)$ and $W_G(a,b)$ can thus take only a limited number of different values:

$$W_G(a,b) - W_F(a,b) = \begin{cases} 4 & \mathrm{Tr}(bv) = \mathrm{Tr}(bF(u_1) + au_1) = \mathrm{Tr}(bF(u_2) + au_2) = 1 \\ -4 & \mathrm{Tr}(bv) = 1, \mathrm{Tr}(bF(u_1) + au_1) = \mathrm{Tr}(bF(u_2) + au_2) = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

In light of (3) this then implies that the nonlinearity of G can differ from that of F by at most two.

Recall that at least one of F and G must have algebraic degree equal to $(n-1)$. Since the algebraic degree of AB functions is upper bounded by $\frac{n+1}{2}$ [6] then G is not AB when F is (for $n \geq 4$), and, therefore, $N_G = 2^{n-1} - 2^{\frac{n-1}{2}} - 2$. Moreover if F is plateaued then its algebraic degree is upper bounded by $\max_{b \in \mathbb{F}_{2^n}^*}(n - \lambda_b + 1)$ where 2^{λ_b} is the amplitude of $\mathrm{Tr}_1^m(bF(x))$, $b \neq 0$, and, therefore, G cannot be plateaued for $n \geq 5$. The upper bound on algebraic degree also implies that if $deg(F) < n - 1$ then G is not plateaued, and, in particular, not AB.

Note also that if F is APN, then G is differentially 6-uniform since the equation $D_aG(x) = b$ may have only $u_1, u_2, a + u_1$ and $a + u_2$ as solutions in addition to the two solutions of $D_aF(x) = b$. When $v_1 = v_2 = v$, G is in fact differentially 4-uniform because $D_aG(x) = b$ is equivalent to $D_aF(x) = b$ for $a = u_1 + u_2$, and for $a \neq u_1 + u_2$, $D_aG(u_1) = D_aG(u_2)$ implies

$$F(u_1) + F(u_2) = F(a + u_1) + F(a + u_2) + v + v = F(a + u_1) + F(a + u_2)$$

which contradicts the APN-ness of F.

Proposition 3. *Let F be an (n,n)-function satisfying $deg(F) < n$ and let $G(x) = F(x) + v(1_{u_1}(x) + 1_{u_2}(x))$. Then:*

(i) the degree of G *is* $2^n - 2$ *and* $deg(G) = n - 1$ *unless* F *contains a term* cx^{2^n-2} *for some* $c \in \mathbb{F}_{2^n}^*$*;*
(ii) $W_G(a,b) \in \{ W_F(a,b),\ W_F(a,b) \pm 4 \}$*;*
(iii) $N_G \in \{0, N_F \pm 2\}$*;*
(iv) for $n \geq 4$*, if* F *is AB then* G *is not AB and* $N_G = 2^{n-1} - 2^{\frac{n-1}{2}} - 2$
(v) for $n \geq 5$*, if* F *is plateaued then* G *is not plateaued;*
(vi) for $n \geq 4$*, if* $deg(F) < n - 1$ *then* G *is not plateaued, and, in particular, not AB.*

For investigating more complex conditions on the APN-ness of G, it can be useful to consider a simplified formulation wherein some of the values u_1, u_2, v_1, v_2 are fixed to e.g. 0 or 1. This can be done without loss of generality by constructing a function F' EA-equivalent to F and a function G' EA-equivalent to G as shown in the following two observations (recall that the property of a function being APN is invariant under EA-equivalence). Note that there are two cases depending on whether the values $F(u_1)$ and $F(u_2)$ are identical or not.

Observation 1. *Let* F *be an* (n,n)*-function and let* G *be defined as*

$$G(x) = F(x) + 1_{u_1}(x)v_1 + 1_{u_2}(x)v_2$$

for some $u_1, u_2, v_1, v_2 \in \mathbb{F}_{2^n}$ *with* $u_1 \neq u_2$ *and* $F(u_1) \neq F(u_2)$*. Then there exists a function* F' *EA-equivalent to* F *satisfying* $F'(0) = 0$ *and* $F'(1) = 1$*, as well as* $v_1', v_2' \in \mathbb{F}_{2^n}$ *such that the function* $G'(x)$ *defined as*

$$G'(x) = F'(x) + 1_0(x)v_1' + 1_1(x)v_2' \tag{7}$$

is EA-equivalent to G*.*

Proof. Given F and G as above, the construction of G' is performed as follows: take $A_1(x) = \frac{x}{F(u_1)+F(u_2)}$, $A_2(x) = x(u_1+u_2)+u_1$ and $A(x) = x + \frac{F(u_1)}{F(u_1)+F(u_2)}$; note that A_1 is indeed defined correctly due to $F(u_1) \neq F(u_2)$, that all three functions are affine and that A_1 and A_2 are bijective. Then the function $(A_1 \circ F \circ A_2 + A)$ is EA-equivalent to $G(x)$ and takes the form

$$\begin{aligned}[F(x(u_1+u_2)+u_1) + (1 + (x(u_1+u_2)+u_1+u_1)^{2^n-1})v_1 + \\ (1 + (x(u_1+u_2)+u_1+u_2)^{2^n-1})v_2 + F(u_1)] \cdot \frac{1}{F(u_1)+F(u_2)}.\end{aligned} \tag{8}$$

Denoting $F'(x) = \frac{F(x(u_1+u_2)+u_1)+F(u_1)}{F(u_1)+F(u_2)}$, this becomes

$$F'(x) + (1 + x^{2^n-1})\left(\frac{v_1}{F(u_1)+F(u_2)}\right) + (1 + (x+1)^{2^n-1})\left(\frac{v_2}{F(u_1)+F(u_2)}\right). \tag{9}$$

If we now take $v_i' = \frac{v_i}{F(u_1)+F(u_2)}$ for $i \in \{1,2\}$, the above becomes

$$F'(x) + (1 + x^{2^n-1})v_1' + (1 + (x+1)^{2^n-1})v_2'. \tag{10}$$

It remains to observe that $F'(0) = 0$ and $F'(1) = 1$ which follows directly from the definition of F'. □

A similar approach can be used when $F(u_1) = F(u_2)$.

Observation 2. *Let F be an (n,n)-function and let G be defined as*

$$G(x) = F(x) + 1_{u_1}(x)v_1 + 1_{u_2}(x)v_2$$

for some $u_1, u_2, v_1, v_2 \in \mathbb{F}_{2^n}$ with $u_1 \neq u_2$ satisfying $F(u_1) = F(u_2)$, $v_i \neq 0$ for $i = 1, 2$. Then there exists a function F' EA-equivalent to F with $F'(0) = F'(1) = 0$, as well as some $v \in \mathbb{F}_{2^n}$ such that the function G' defined as

$$G'(x) = F'(x) + 1_0(x) + 1_1(x)v$$

is EA-equivalent to G.

Proof. Given G as above, take $A_1(x) = \frac{x}{v_1}$, $A_2(x) = (u_1 + u_2)x + u_1$ and $A(x) = x + \frac{F(u_1)}{v_1}$; note that all of these functions are well-defined linear permutations under the hypothesis. Then

$$\begin{aligned}(A_1 \circ G \circ A_2 + A)(x) = \frac{1}{v_1}[F(A_2(x)) + (1 + (x(u_1 + u_2))^{2^n-1})v_1 + \\ (1 + ((x+1)(u_1 + u_2))^{2^n-1})v_2 + F(u_1)] = \\ (A_1 \circ F \circ A_2 + A)(x) + (1 + x^{2^n-1}) + (1 + (x+1)^{2^n-1})\frac{v_1}{v_2} = \\ (A_1 \circ F \circ A_2 + A)(x) + (1 + x^{2^n-1}) + (1 + (x+1)^{2^n-1})v \quad (11)\end{aligned}$$

for $v = v1/v2$; taking $F' = A_1 \circ F \circ A_2 + A$, it then suffices to verify that we have $F'(0) = F'(1) = 0$:

$$F'(0) = \frac{F(u_1) + F(u_1)}{v_1} = 0$$

and

$$F'(1) = \frac{F(u_2) + F(u_1)}{v_1} = 0$$

due to $F(u_1) = F(u_2)$. This completes the proof. □

V. Swapping Two Points

A significant simplification in the case of $F(u_1) \neq F(u_2)$ consists in examining the particular case of *swapping* the values of F at u_1 and u_2. This is a weaker construction, which makes it somewhat easier to obtain results. Furthermore, such a construction is of particular interest as it leaves the property of being a permutation invariant, i.e. if F is a permutation then G is a permutation too. In this case, the resulting function becomes (by substituting $v_1 = 1$ and $v_2 = 1$ into (7))

$$G(x) = F(x) + x^{2^n-1} + (x+1)^{2^n-1} \quad (12)$$

with $F(0) = 0$ and $F(1) = 1$.

Example 1. To see that swapping the values of a function F at two points is indeed weaker than the general case of changing two points, consider the function $F(x) = x^3 + (x^2 + x + 1)\mathrm{Tr}_1^n(x^3)$ over $\mathbb{F}_{2^4}$ of algebraic degree 3. All APN functions obtained by swapping two values of F have algebraic degree 2. On the other hand, taking e.g. $u_1 = \alpha^4$, $u_2 = \alpha^2$ and $v_1 = v_2 = 1$ (where α is a primitive element of $\mathbb{F}_{2^4}$) results in an APN function of algebraic degree 3.

In the following, we see how Lemmas 1 and 2 can be applied to the case of swapping two points. To facilitate the discussion, we define the following sets:

$$S = \{ (a,b) \in \mathbb{F}_{2^n} \ \mathrm{Tr}_1^n(a) = \mathrm{Tr}_1^n(b) = 1\}, \tag{13}$$

$$S' = \mathbb{F}_{2^n}^2 \setminus (S \cup \{(0,0)\}). \tag{14}$$

The following lemma is known as the "two-tuple balance property" [11].

Lemma 3. *For $c \in \mathbb{F}_{2^n}$, we have*

$$\sum_{\substack{x \in \mathbb{F}_{2^n} \\ \mathrm{Tr}(x)=1}} (-1)^{\mathrm{Tr}(cx)} = \begin{cases} 2^{n-1} & c = 0 \\ -2^{n-1} & c = 1 \\ 0 & c \notin \{0,1\}. \end{cases}$$

The following results easily follow by application of the above lemma.

Observation 3. *Let F be an (n,n)-function. Then*

$$\sum_{(a,b)\in S} W_F(a,b) = 2^{n-1} \sum_{\substack{b \in \mathbb{F}_{2^n} \\ \mathrm{Tr}(b)=1}} (-1)^{\mathrm{Tr}(bF(0))} - (-1)^{\mathrm{Tr}(bF(1))}.$$

In particular, if $F(0) = 0$ and $F(1) = 1$, the above simplifies to

$$\sum_{(a,b)\in S} W_F(a,b) = 2^{2n-1}. \tag{15}$$

Proof. From the definition, we have

$$\begin{aligned} \sum_{(a,b)\in S} W_F(a,b) &= \sum_{(a,b)\in S} \sum_{x\in\mathbb{F}_{2^n}} \eta(\mathrm{Tr}(bF(x) + ax)) = \\ &\sum_{x\in\mathbb{F}_{2^n}} \sum_{\mathrm{Tr}(b)=1} \eta_b(F(x)) \sum_{\mathrm{Tr}(a)=1} \eta_a(x) = \\ &2^{n-1} \cdot \left(\sum_{\mathrm{Tr}(b)=1} \eta_b(F(0)) - \sum_{\mathrm{Tr}(b)=1} \eta_b(F(1)) \right) = \\ &2^{n-1} \sum_{\mathrm{Tr}(b)=1} \left(\eta_b(F(0)) - \eta_b(F(1)) \right). \end{aligned} \tag{16}$$

The particular statement follows by substituting $F(0) = 0$ and $F(1) = 1$. □

Proposition 4. *Let F be an (n,n)-function. Then*

$$\sum_{(a,b)\in S} W_F^2(a,b) = 2^{3n-2} - 2^{2n-2}(\Delta_F(1,0) - \Delta_F(1,1)). \tag{17}$$

Proof. From the definition we can easily obtain

$$\sum_{(a,b)\in S} W_F^2(a,b) = \sum_{x,y} \sum_{\mathrm{Tr}(b)=1} \eta_b(F(x) + F(y)) \sum_{\mathrm{Tr}(a)=1} \eta_a(x+y). \tag{18}$$

By Lemma 3, this is equivalent to

$$\sum_{(a,b)\in S} W_F^2(a,b) = 2^{n-1}\sum_x \left(\sum_{\mathrm{Tr}(b)=1} \eta_b(F(x)+F(x)) - \sum_{\mathrm{Tr}(b)=1} \eta_b(F(x)+F(x+1)) \right) = 2^{3n-2} - 2^{2n-2}(\Delta_F(1,0) - \Delta_F(1,1)) \quad (19)$$

which is what we wanted to show. □

Proposition 5. *Let F be an (n,n)-function satisfying $F(0)=0$ and $F(1)=1$. Then*

$$\sum_{a\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(a)=0} W_F(a,b) = 0, \quad (20)$$

$$\sum_{a\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(a)=1} W_F(a,b) = 2^n. \quad (21)$$

Proof. Let $b \in \mathbb{F}_{2^n}$ satisfy $\mathrm{Tr}_1^n(b) = 1$ and $G(x) = x^{2^n-1} + (x+1)^{2^n-1} + F(x)$. By Parseval's relation and by (6)

$$\begin{aligned} 2^{2n} = \sum_{a\in\mathbb{F}_{2^n}} W_G^2(a,b) &= \sum_{\mathrm{Tr}_1^n(a)=0} W_F^2(a,b) + \sum_{\mathrm{Tr}_1^n(a)=1} (W_F(a,b)-4)^2 \\ &= \sum_{a\in\mathbb{F}_{2^n}} W_F^2(a,b) - 8\sum_{\mathrm{Tr}_1^n(a)=1} W_F(a,b) + 2^{n+3} \\ &= 2^{2n} + 2^{n+3} - 8\sum_{\mathrm{Tr}_1^n(a)=1} W_F(a,b). \end{aligned}$$

Hence $\sum_{a\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(a)=1} W_F(a,b) = 2^n$. Besides, since $F(0)=0$ we have

$$\sum_{a\in\mathbb{F}_{2^n}} W_F(a,b) = 2^n$$

by the inverse Walsh transform (1) and thus $\sum_{a,\mathrm{Tr}_1^n(a)=0} W_F(a,b) = 0$. □

Proposition 6. *Let F be any function over $\mathbb{F}_{2^n}$ satisfying $F(0)=0$ and $F(1)=1$ and let G be defined as $G(x) = x^{2^n-1} + (x+1)^{2^n-1} + F(x)$. Then G is APN if and only if*

$$\sum_{(a,b)\in S} (W_F^3(a,b) - 6W_F^2(a,b)) = 2^{-4}\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_F^4(a,b) - 2^{4n-3} + 2^{3n-3} - 2^{2n+2}, \quad (22)$$

where S is defined as in (13). In particular, if F is APN, then G is APN if and only if

$$\sum_{(a,b)\in S} (W_F^3(a,b) - 6W_F^2(a,b)) = -2^{2n+2}. \quad (23)$$

Proof. By (6) we get

$$\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_G^4(a,b) = \sum_{(a,b)\in S'} W_F^4(a,b) + \sum_{(a,b)\in S} \left(W_F(a,b)-4\right)^4 =$$
$$\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_F^4(a,b) + \sum_{(a,b)\in S} \left(-16W_F^3(a,b) + 96W_F^2(a,b) - 256W_F(a,b) + 256\right),$$

where S' is defined as in (14).

Hence, by (15) and Proposition 5

$$\sum_{(a,b)\in S} \left(W_F^3(a,b) - 6W_F^2(a,b)\right) =$$
$$2^{-4}\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_F^4(a,b) - 2^{-4}\sum_{a\in\mathbb{F}_{2^n}}\sum_{b\in\mathbb{F}_{2^n}^*} W_G^4(a,b) - 2^{2n+2},$$

and, by Lemma 1, G is APN if and only if (22) holds. If, in addition, F is APN then by Lemma 1, G is APN if and only if (15) is satisfied. □

We can now substitute the formula from Proposition 4 into Proposition 6 in order to obtain the following characterization.

Observation 4. *Let F be over $\mathbb{F}_{2^n}$ with $F(0)=0$ and $F(1)=1$, and let $G(x) = x^{2^n-1} + (x+1)^{2^n-1} + F(x)$. Then G is APN if and only if*

$$\sum_{(a,b)\in S} W_F^3(a,b) + 3\cdot 2^{2n-1}\left(\Delta_F(1,0) - \Delta_F(1,1)\right) =$$
$$2^{-4}\sum_{a}\sum_{b\neq 0} W_F^4(a,b) + 13\cdot 2^{3n-3} - 2^{4n-3} - 2^{2n+2}. \quad (24)$$

If, in addition, F is APN, then G is APN if and only if

$$\sum_{(a,b)\in S} W_F^3(a,b) + 3\cdot 2^{2n-1}\left(\Delta_F(1,0) - \Delta_F(1,1)\right) = 3\cdot 2^{3n-1} - 2^{2n+2}. \quad (25)$$

By means of mechanical computations similar to the ones in the proof of Proposition 4, we can obtain the following identity.

Proposition 7. *For any vectorial Boolean function F over $\mathbb{F}_{2^n}$ we have*

$$\sum_{(a,b)\in S} W_F^3(a,b) = 2^{2n-2}\sum_{y\in\mathbb{F}_{2^n}} \left(\Delta_F(y,F(y)) - \Delta_F(y,F(y)+1) - \right.$$
$$\left. \Delta_F(y+1,F(y)) + \Delta_F(y+1,F(y)+1)\right). \quad (26)$$

In particular, if F is APN and satisfies $F(0)=0$ and $F(1)=1$, this becomes

$$\sum_{(a,b)\in S} W_F^3(a,b) = 3\cdot 2^{3n-1} - 2^{2n} - 2^{2n-2}\sum_{y\in\mathbb{F}_{2^n}} \left(\Delta_F(y,F(y)+1) + \Delta_F(y+1,F(y))\right). \quad (27)$$

Proof. From the definition we have

$$\sum_{(a,b)\in S} W_F^3(a,b) = \sum_{x,y,z\in\mathbb{F}_{2^n}} \sum_{\substack{b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}(b)=1}} \eta_b(F(x)+F(y)+F(z)) \sum_{\substack{a\in\mathbb{F}_{2^n}\\ \mathrm{Tr}(a)=1}} \eta_a(x+y+z) =$$

$$2^{n-1} \sum_{x,y\in\mathbb{F}_{2^n}} \left(\sum_{\substack{b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}(b)=1}} \eta_b(F(x)+F(y)+F(x+y)) \right.$$

$$\left. - \sum_{\substack{b\in\mathbb{F}_{2^n}\\ \mathrm{Tr}(b)=1}} \eta_b(F(x)+F(y)+F(x+y+1)) \right). \quad (28)$$

The main statement then follows by Lemma 3. The particular statement follows by observing that $\sum_{y\in\mathbb{F}_{2^n}} \Delta_F(y,F(y)) = \sum_{y\in\mathbb{F}_{2^n}} \Delta_F(y+1,F(y)+1) = 2^{n+1}+2^n-2$. □

Assuming that F is APN, we can combine equations (25) and (27) to obtain the following:

Theorem 1. *Let F be APN with $F(0)=0$ and $F(1)=1$. Then G is APN if and only if*

$$6\Delta_F(1,0) = \sum_{y\in\mathbb{F}_{2^n}} (\Delta_F(y,F(y)+1) + \Delta_F(y+1,F(y))). \quad (29)$$

This characterization allows us to show that a given G is not APN by computing a very weak lower bound on the number of pairs (x,y) satisfying $F(x)+F(x+y)+F(y)=1$ or $F(x)+F(x+y+1)+F(y)=0$. In Section VI we derive a lower bound on the number of such pairs in the case of power functions. Experimental results show that the number of these solutions grows very quickly for APN functions as the dimension of the underlying field increases. Despite this, a theoretical lower bound appears difficult to prove in the general case; in Section VI.

Table I gives the values of both $\sum_y \Delta_F(y,F(y)+1)$ and $\sum_y \Delta_F(y+1,F(y))$ for all APN functions from the known switching classes over $\mathbb{F}_{2^n}$ with $5\le n\le 8$ as given in [10]. The functions in the table are indexed using the notation from Tables 3, 5, 7 and 9 from [10]. Since the sum of the two values, $\sum_y \Delta_F(y,F(y)+1)$ and $\sum_y \Delta_F(y+1,F(y))$, is greater than 12 in all cases, we can immediately apply Theorem 1 to obtain the following result.

Since the sum of the two values $\sum_y \Delta_F(y,F(y)+1)$ and $\sum_y \Delta_F(y+1,F(y))$ for the functions in Table I in all cases is greater than 12, we can immediately apply Theorem 1 to get the following result.

Observation 5. *Let F be any APN function from those given in [10], and let G be defined as*

$$G(x) = F(x) + x^{2^n-1} + (x+1)^{2^n-1}.$$

Then G is not APN.

Example 2. In some cases an explicit formula for the values $\sum_y \Delta_F(y,F(y)+1)$ and $\sum_y \Delta_F(y+1,F(y))$ can be found. Consider, for example, the function $F(x)=x^3$

TABLE I
THE VALUES $S_1 = \sum_y \Delta_F(y, F(y)+1)$ AND $S_2 = \sum_y \Delta_F(y+1, F(y))$ FOR ALL FUNCTIONS F FROM [10]

n	F	S_1	S_2	n	F	S_1	S_2
5	1.1	30	30		11.1	126	382
	1.2	30	30		12.1	126	382
	2.1	30	30		13.1	126	126
6	1.1	78	78		14.1	126	126
	1.2	78	78		14.2	126	382
	2.1	54	66		14.3	126	126
	2.2	54	78	8	1.1	222	222
	2.3	54	54		1.2	222	222
	2.4	54	54		1.3	222	222
	2.5	54	66		1.4	222	222
	2.6	42	54		1.5	270	222
	2.7	66	66		1.6	270	222
	2.8	78	54		1.7	270	222
	2.9	66	90		1.8	222	222
	2.10	54	42		1.9	270	222
	2.11	66	66		1.10	222	222
	2.12	54	66		1.11	270	222
7	1.1	126	126		1.12	222	222
	1.2	126	382		1.13	270	222
	2.1	126	126		1.14	270	270
	2.2	126	382		1.15	222	222
	3.1	126	126		1.16	222	222
	4.1	126	126		1.17	222	222
	5.1	126	126		2.1	270	222
	6.1	126	126		3.1	270	222
	7.1	126	126		4.1	318	766
	8.1	126	126		5.1	318	318
	9.1	126	382		6.1	318	318
	10.1	126	382		7.1	222	222
	10.2	126	126				

over $\mathbb{F}_{2^n}$. The sum $\sum_y \Delta_F(y, F(y)+1)$ is equal to the number of pairs $(x, y) \in \mathbb{F}_{2^n}^2$ satisfying $x^3 + (x+y)^3 + y^3 = 1$, which easily simplifies to

$$x^2 y + x y^2 = 1. \tag{30}$$

Note that if $y = 0$, no pair $(x, 0)$ can satisfy (30). Consider some fixed nonzero $y \in \mathbb{F}_{2^n}^*$. Dividing both sides of (30) by the cube of its inverse yields

$$\left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right) = \frac{1}{y^3}. \tag{31}$$

For this fixed y, define the function $g_y(x) = \left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right)$. Observe that $g_y(x_1) = g_y(x_2)$ implies

$$\left(\frac{x_1 + x_2}{y}\right)^2 = \left(\frac{x_1 + x_2}{y}\right)$$

which is certainly satisfied when $x_1 = x_2$. If $x_1 \neq x_2$, however, we can divide both sides by $(x_1 + x_2)/y$ in order to obtain

$$x_1 + x_2 = y. \tag{32}$$

Thus, $g_y(x)$ is a 2-to-1 function on $\mathbb{F}_{2^n}$ for any $y \in \mathbb{F}_{2^n}^*$. Taking into account that $\mathrm{Tr}_n(g_y(x)) = 0$ for any $x \in \mathbb{F}_{2^n}$, we can see that $\{g_y(x) : x \in \mathbb{F}_{2^n}\} = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_n(x) = 0\}$. This means that for any fixed $y \in \mathbb{F}_{2^n}^*$, (30) has two solutions if $\mathrm{Tr}_n(y^{-3}) = 0$, and no solutions otherwise. The value $\sum_y \Delta_F(y, F(y)+1)$ is then equal to twice the number of nonzero elements $y \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_n(y^3) = 0$, i.e.

$$\sum_y \Delta_F(y, F(y)+1) = 2(wt(f) - 1) \tag{33}$$

where f is the function $f(a) = \mathrm{Tr}_n(a^3)$, and $wt(f) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq 0\}|$ is the Hamming weight of f.

The weight of any function of the form $x \mapsto \mathrm{Tr}_n(\lambda x^3)$, where $\lambda \in \mathbb{F}_{2^n}$ is a constant, is known from [7]. Adapting this slightly more general result to our particular case and substituting in (33), we have

$$\sum_y \Delta_F(y, F(y)+1) = \begin{cases} 2(2^{n-1}-1) & n \text{ is odd} \\ 2(2^{n-1}+2^{n/2}-1) & n \text{ is even and } n/2 \text{ is odd} \\ 2(2^{n-1}-2^{n/2}-1) & n \text{ is even and } n/2 \text{ is even.} \end{cases} \tag{34}$$

This formula then allows us to compute the values of $\sum_y \Delta_F(y, F(y)+1)$ for $F(x) = x^3$ for any dimension n. Table II lists the values obtained for all dimensions up to 20. Since these values are at least 30 for $n \geq 5$, we can make the following observation.

Observation 6. *Let $F(x) = x^3$ over $\mathbb{F}_{2^n}$ and let G be defined as*

$$G(x) = F(x) + x^{2^n-1} + (x+1)^{2^n-1},$$

i.e. by swapping the values of F at 0 and 1. Then G is not APN unless $n \leq 4$.

We have experimentally verified that all power APN functions over fields $\mathbb{F}_{2^n}$ of dimension $1 \leq n \leq 10$ have the same exact values for $\sum_y \Delta_F(y, F(y)+1)$ as those in Table II. We thus formulate the following conjecture.

Conjecture 1. For any power APN function F over $\mathbb{F}_{2^n}$, the two values $\sum_y \Delta_F(y, F(y)+1)$ and $\sum_y \Delta_F(y+1, F(y))$ are equal to $\sum_y \Delta_{x^3}(y, y^3+1)$ and are given by (34).

Furthermore, the results in Table I suggest that even in the case of a general APN function, the values do not differ too much from that of the power APN function x^3 over the same field. Seeing as how the latter form a sequence that monotonically increases with the dimension n, we formulate the following conjecture.

Conjecture 2. Let F be any APN function over $\mathbb{F}_{2^n}$ with $n \geq 5$. Then no function G obtained by swapping two points of F can be APN.

Note also that a similar computation can be performed in order to obtain an explicit formula for the value $\sum_y \Delta_F(y+1, F(y))$. In the case of $F(x) = x^3$, we obtain the same formula as for $\sum_y \Delta_F(y, F(y)+1)$ so that in this case the two values are always the same. Based on our experimental results, this is also true for all power APN functions over $\mathbb{F}_{2^n}$ with $1 \leq n \leq 10$. As can be seen from Table I, however, the two values may differ in the general case.

VI. Power functions

In this section we apply the conditions from Section V to show that for $n \geq 5$ no APN function can be obtained by swapping the values $F(0)$ and $F(1)$ of a power function. A well-known observation is that a power function F is APN if and only if its derivative D_1F is a 2-to-1 function.

Recall that we assume $u_1 = 0$, $u_2 = 1$ and $v_1 = v_2 = v = 1$, as well as $F(0) = 0$ and $F(1) = 1$. Then condition (iii) from Proposition 2 becomes: for $a \neq 1$, the equations $D_aF(x) + F(a) = 1$ and $D_aF(x) + F(a+1) = 0$ have no solution $x \notin \{0, 1, a, a+1\}$. We will show that when F is a power function of sufficiently high dimension, a pair (a, x) violating this condition always exists.

TABLE II
FORMULA (34) APPLIED TO $F(x) = x^3$ FOR DIMENSIONS $1 \leq n \leq 20$

n	$\sum_y \Delta_F(y, F(y)+1)$	n	$\sum_y \Delta_F(y, F(y)+1)$
1	0	11	2046
2	6	12	3966
3	6	13	8190
4	6	14	16638
5	30	15	32766
6	78	16	65022
7	126	17	131070
8	222	18	263166
9	510	19	524286
10	1086	20	1046526

Since $F(x) = x^l$ for some positive integer l, the equation e.g. $D_1F(x) + F(a) = 1$ can be rewritten as

$$x^l + (a+x)^l + a^l = 1.$$

We divide the analysis into several cases depending on the parity of the dimension n. We first show that any field of odd dimension contains at least one pair (a, x) satisfying $D_1F(x) + F(a) = 1$.

Observation 7. *Let $\mathbb{F}_{2^n}$ be a finite field with $n > 1$ odd, and let $F(x) = x^l$ be a power APN function over $\mathbb{F}_{2^n}$. Then there exists a pair $(a, x) \in \mathbb{F}_{2^n}^2$ satisfying $a^l + x^l + (a + x)^l = 1$.*

Proof. Note that the equation $a^l + x^l + (a + x)^l = 1$ can be more succinctly written as $D_a^0F(x) = 1$. Since x^l is a permutation, it suffices to find a pair (a, x) such that $D_a^0F(x) \neq 0$. Since F is APN, the shifted derivative D_a^0 is a 2-to-1 function for any fixed $a \neq 0$, and maps all elements of $\mathbb{F}_{2^n}$ to 0 for $a = 0$. Thus, at most $2^n + 2(2^n - 1)$ pairs (a, x) can satisfy $D_a^0F(x) = 0$. This quantity is strictly less than 2^{2n} for $n > 1$, so that at least one pair (a, x) must exist satisfying $D_a^0F(x) = c$ for some $c \neq 0$. It now suffices to divide both sides by c^{-1}. □

It is easy to show that such a pair (a, x) exists for any APN power function over $\mathbb{F}_{2^2}$ as well.

Observation 8. *Let $F(x) = x^l$ be APN over $\mathbb{F}_{2^2}$. Then there is a pair $(a, x) \in \mathbb{F}_{2^n}^2$ such that $x^l + (a + x)^l + a^l = 1$.*

Proof. Let α be a primitive element of $\mathbb{F}_{2^2}$. Since $F(x) = x^l$ is APN over a field of even dimension n, we must have $\gcd(l, n) = 3$. Then l is a multiple of three, say $l = 3l'$ for some positive integer l'. Now

$$\alpha^l + (\alpha+1)^l + 1^l = \alpha^{3l'} + (\alpha+1)^{3l'} + 1 = 1 + 1 + 1 = 1$$

since $\alpha^3 = (\alpha + 1)^3 = 1$. □

A simple but important observation is that for any two pairs (a_1, x_1) and (a_2, x_2) satisfying $D_{a_1}^0F(x_1) = D_{a_2}^0F(x_2) = 1$, the sets $\{x_1, a_1 + x_1, a_1\}$ and $\{x_2, a_2 + x_2, a_2\}$ either coincide or are disjoint.

Observation 9. *Let F be APN over $\mathbb{F}_{2^n}$ with $F(0) = 0$ and $F(1) = 1$. Let $A_1 = \{a_1, b_1, a_1 + b_1\}$ and $A_2 = \{a_2, b_2, a_2 + b_2\}$ be two sets of elements defining solutions to the equation*

$$F(a_i) + F(a_i + b_i) + F(b_i) = 1 \tag{35}$$

for $i \in \{1, 2\}$. Then A_1 and A_2 are either identical or disjoint.

We can now apply the above observations in order to show that swapping two points in a power function cannot produce an APN function except over $\mathbb{F}_2$, $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^4}$.

Proposition 8. *Let $F(x) = x^l$ be a power function over $\mathbb{F}_{2^n}$ and $G(x) = x^l + x^{2^n-1} + (x + 1)^{2^n-1}$. Then G cannot be APN for any dimension n other than 1, 2 and 4.*

Proof. Let us assume that G is APN. First, observe that the derivatives of F and G in direction 1 coincide since

$$D_1G(x) = F(x) + x^{2^n-1} + (x + 1)^{2^n-1} + F(x + 1) + (x + 1)^{2^n-1} + x^{2^n-1} = D_1F(x).$$

Since $F(x) = x^l$ is APN if and only if D_1F is 2-to-1, if G is APN then F must necessarily be APN as well.

We now examine several cases.

If n is a composite number and p and q are two distinct primes dividing n, then F is APN over $\mathbb{F}_{2^p}$ and $\mathbb{F}_{2^q}$ as well. According to Observations 7 and 8, there exist pairs $(a_1, x_1) \in \mathbb{F}_{2^p}^2$ and $(a_2, x_2) \in \mathbb{F}_{2^q}^2$ such that $D_{a_i}F(x) + F(a_i) = 1$ for $i \in \{1, 2\}$. Since p and q are coprime and therefore $\mathbb{F}_{2^p} \cap \mathbb{F}_{2^q} = \mathbb{F}_2$, the sets $\{a_1, x_1, a_1 + x_1\}$ and $\{a_2, x_2, a_2 + x_2\}$ are disjoint by Observation 9.

Note that if some pair (a, x) solves $D_aF(x) + F(a) = 1$, then so do the pairs (x, a), $(a+x, a)$, $(a+x, x)$, $(a, a+x)$ and $(x, a+x)$. Furthermore, all of these pairs are distinct as can be easily seen by contradiction. Hence the two pairs (a_1, x_1) and (a_2, x_2) above actually yield 12 distinct pairs (a, x) solving $D_aF(x) + F(a) = 1$. This means that the right-hand side of (29) from Theorem 1 is at least 24, while the left-hand side is at most 12 due to F being APN. Then according to Theorem 1, G is not APN.

If n is odd, then by Observation 7, there exists a pair (a, x) solving $D_aF(x)+F(a) = 1$. However, due to n being odd, F is a permutation over $\mathbb{F}_{2^n}$ and thus $\Delta_F(1, 0) = 0$. Thus, the left-hand side of (29) is equal to zero while its right-hand side is positive. Consequently, Theorem 1 implies that G is not APN.

Finally, suppose that n is a power of two, i.e. $n = 2^k$ for some $k > 2$. Since G is APN over $\mathbb{F}_{2^{2^k}}$ it must be APN over $\mathbb{F}_{2^{2^{k'}}}$ for all $k' < k$. In particular, G must be APN over $\mathbb{F}_{2^8}$. However, no power APN function over $\mathbb{F}_{2^8}$ produces an APN function after a two-point swap, which can be verified by an exhaustive search. This means that G cannot be APN in this case either. □

To complete the discussion, it is worth mentioning that $G(x)$ can indeed be APN for $n \in \{1, 2, 4\}$. This can easily be verified by using e.g. Theorem 1 or the definition of APN functions.

Observation 10. *Over the fields $\mathbb{F}_{2^{2^i}}$ for $i \in \{0, 1, 2\}$, the function $G(x) = x^l + x^{2^n-1} + (x + 1)^{2^n-1}$ is APN if and only if $F(x) = x^l$ is APN, where $n = 2^i$.*

VII. Equivalence Relations

In this section we make some observations regarding the EA- and CCZ-equivalence classes of the functions F and G from the two-point construction.

We begin by observing that the possibility of obtaining one EA-equivalence class from another does not depend on the concrete choice of representatives.

Proposition 9. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and G be defined as $G(x) = F(x)+v_1(x+u_1)^{2^n-1}+v_2(x+u_2)^{2^n-1}$ for some $u_1, u_2 \in \mathbb{F}_{2^n}$ and $v_1, v_2 \in \mathbb{F}_{2^n}^*$, and let $G' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be EA-equivalent to G. Then there exist elements $u_1, u_2' \in \mathbb{F}_{2^n}$ and $v_1', v_2' \in \mathbb{F}_{2^n}^*$ and a function $F' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ EA-equivalent to F such that*

$$G'(x) = F'(x) + v_1'(x + u_1')^{2^n-1} + v_2'(x + u_2')^{2^n-1}.$$

Proof. Suppose that G' is EA-equivalent to G via $G' = A_1 \circ G \circ A_2 + A$ where A_1, A_2, A are affine functions over $\mathbb{F}_{2^n}$ and A_1, A_2 are permutations. Assume without loss of generality that A_1 is linear. We can write

$$\begin{aligned} G'(x) = A_1(F(A_2(x))) + A_1(v_1(A_2(x) + u_1)^{2^n-1}) + \\ A_1(v_2(A_2(x) + u_2)^{2^n-1}) + A(x) = (A_1 \circ F \circ A_2 + A)(x) + \\ A_1(v_1)(x + A_2^{-1}(u_1))^{2^n-1} + A_1(v_2)(x + A_2^{-1}(u_2))^{2^n-1}. \quad (36) \end{aligned}$$

If we now take $F' = A_1 \circ F \circ A_2 + A$, $u_i' = A_1(v_i)$ and $v_i' = A_2^{-1}(v_i)$ for $i \in \{1, 2\}$, we have $G'(x) = F'(x) + v_1'(x + u_1')^{2^n-1} + v_2'(x + u_2)^{2^n-1}$ with F' clearly being EA-equivalent to F and with $v_1', v_2' \neq 0$ due to A_2 being a permutation. □

The following proposition is obtained by a similar argument.

Proposition 10. *Let F and F' be EA-equivalent functions over $\mathbb{F}_{2^n}$ and let G be defined by $G(x) = F(x) + v_1(x + u_1)^{2^n-1} + v_2(x + u_2)^{2^n-1}$ for some $u_1, u_2 \in \mathbb{F}_{2^n}$ and $v_1, v_2 \in \mathbb{F}_{2^n}^*$. Then there is a function G' EA-equivalent to G and some elements $u_1', u_2' \in \mathbb{F}_{2^n}$ and $v_1', v_2' \in \mathbb{F}_{2^n}^*$ such that*

$$G'(x) = F'(x) + v_1'(x + u_1')^{2^n-1} + v_2'(x + u_2')^{2^n-1}.$$

We now turn to the more general notion of CCZ-equivalence.

Proposition 11. *Let F be a function over $\mathbb{F}_{2^n}$ and let G be defined over $\mathbb{F}_{2^n}$ as*

$$G(x) = F(x) + v_1(x + u_1)^{2^n-1} + v_2(x + u_2)^{2^n-1}$$

for some $u_1, u_2 \in \mathbb{F}_{2^n}$ and $v_1, v_2 \in \mathbb{F}_{2^n}^*$, and suppose that G' is CCZ-equivalent to G. Then there exists a function F' CCZ-equivalent to F and elements $u_1', u_2', v_1', v_2' \in \mathbb{F}_{2^n}$ such that

$$G'(x) = F'(x) + v_1'(x + u_1')^{2^n-1} + v_2'(x + u_2')^{2^n-1}.$$

Proof. Suppose that G' is CCZ-equivalent to G via the affine permutation $\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y))$ of $\mathbb{F}_{2^n}^2$. Writing $G_i(x) = L_i(x, G(x))$ for $i \in \{1, 2\}$ and $A_1(x, y) =$

$L_1(x) + L_2(y) + a$ and $A_2(x, y) = L_3(x) + L_4(y) + b$ for L_1, L_2, L_3, L_4 linear and $a, b \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} G'(x) = L_3(G_1^{-1}(x)) + L_4(G(G_1^{-1}(x))) + b = L_3 \circ G_1^{-1}(x) + L_4 \circ F \circ G_1^{-1}(x) + \\ L_4((G_1^{-1}(x) + u_1)^{2^n-1} v_1) + L_4((G_1^{-1}(x) + u_2)^{2^n-1} v_2) + b = F'(x) + \\ L_4((G_1^{-1}(x) + u_1)^{2^n-1} v_1 + (G_1^{-1}(x) + u_2)^{2^n-1} v_2) = \\ F'(x) + L_4(v_1)(x + G_1(u_1))^{2^n-1} + L_4(v_2)(x + G_1(u_2)) \end{aligned}$$

where we define $F'(x) = F_2 \circ G_1^{-1}(x)$ with $F_2(x) = L_3(x) + L_4(F(x)) + b$. Now F' is clearly CCZ-equivalent to F by the construction, and it suffices to take $u_i' = G_1(u_i)$ and $v_i' = L_4(v_i)$ for $i \in \{1, 2\}$. □

Note that in the above proposition, we do not guarantee that v_1' and v_2' will be nonzero which means that the functions F' and G' may be at distance less than two. This raises the question of whether the minimum distance between functions belonging to distinct CCZ-equivalence classes depends on the concrete choice of representatives.

VIII. Conclusion

We investigated a construction that involves changing the value of a given function F over $\mathbb{F}_{2^n}$ at precisely two points of $\mathbb{F}_{2^n}$ and, in particular, concentrated on the possibility of obtaining an APN function in this manner when F is APN. We characterized the APN-ness of the resulting function G in terms of the derivatives and in terms of the Walsh coefficients of F. We observed that changing two points in a plateaued function F cannot produce a plateaued function G, and neither can this happen for a function F with $deg(F) < n - 1$ (unless $n < 5$). Furthermore, no two AB functions at distance two may exist for $n \geq 4$.

In addition, we observed that if $deg(F) = 2$ and F is not APN, then any function G obtained by changing two points of F cannot be APN either.

We also examined the less general but more tractable problem of swapping two points in a given function. In particular, we showed that if F is APN and satisfies $F(0) = 0$ and $F(1) = 1$, then G is APN if and only if

$$6\Delta_F(1, 0) = \sum_{y \in \mathbb{F}_{2^n}} \Delta_F(y, F(y) + 1) + \Delta_F(y + 1, F(y)).$$

We applied this characterization in order to show that an APN function can never be obtained by swapping two values in any power function over $\mathbb{F}_{2^n}$ for $n > 4$. We also derived an explicit formula for $\sum_y \Delta_F(y, F(y) + 1)$ in the case of $F(x) = x^3$. Furthermore, we experimentally computed the values $\Delta_F(y, F(y) + 1)$ and $\Delta_F(y + 1, F(y))$ all known APN functions from [10], concluding that no APN function can be obtained by a two-point swap from those functions either.

Despite the fact that the results in Tables I and II suggest that the values of $\Delta_F(y, F(y) + 1)$ and $\Delta_F(y + 1, F(y))$ grow quite quickly with the dimension n of the underlying field, it seems difficult to find a lower bound on those values in the general case. Further results in this direction should provide additional insight into the possibility of obtaining an APN functions by a two-point swap.

The general case of arbitrarily changing two points in a given function also leaves room for further investigation; in particular, an analogue to Theorem 1 is highly desirable.

Finally, as mentioned above, we mostly concentrated on the case when the initial function F is itself APN. The possibility of obtaining an APN function G from a function F belonging to some other class of functions is another potential direction for future work.

ACKNOWLEDGEMENTS

This research was co-funded by the Trond Mohn Foundation (formerly the Bergen Research Foundation). I would like to thank my supervisors Lilya Budaghyan and Claude Carlet, as well as Tor Helleseth and Nian Li for their ongoing interest and support.

REFERENCES

[1] Budaghyan, L.: The Equivalence of Almost Bent and Almost Perfect Nonlinear Functions and their Generalizations. Ph.D. thesis, Otto-von-Guericke-Universität Magdeburg, Universitätsbibliothek (2005)
[2] Budaghyan, L., Carlet, C., Helleseth, T., Li, N., Sun, B.: On Upper Bounds for Algebraic Degrees of APN Functions. IEEE Transactions on Information Theory **64**(6), 4399–4411 (2018)
[3] Budaghyan, L., Carlet, C., Pott, A.: New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. IEEE Transactions on Information Theory **52**(3), 1141–1152 (2006)
[4] Carlet, C.: Boolean Models and Methods in Mathematics, Computer Science, and Engineering: Vectorial Boolean Functions for Cryptography (2010)
[5] Carlet, C.: Boolean and Vectorial Plateaued Functions and APN Functions. IEEE Transactions on Information Theory **61**(11), 6272–6289 (2015)
[6] Carlet, C., Charpin, P., Zinoviev, V.A.: Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. Designs, Codes and Cryptography **15**(2), 125–156 (1998)
[7] Carlitz, L.: Explicit Evaluation of Certain Exponential Sums. Mathematica Scandinavica **44**, 5–16 (1979)
[8] Chabaud, F., Vaudenay, S.: Links between Differential and Linear Cryptanalysis. In: Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT '94, vol. 950, pp. 356–365 (1994)
[9] Charpin, P., Mesnager, S., Sarkar, S.: Involutions over the Galois Field. IEEE Transactions on Information Theory **62**(4), 2266–2276 (2016)
[10] Edel, Y., Pott, A.: A New Almost Perfect Nonlinear Function which is not Quadratic. Advances in Mathematics of Communications **3**(1), 59–81 (2009)
[11] Golomb, S.W., Gong, G.: Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar (2005)
[12] Langevin, P.: Covering Radius of $RM(1,9)$ in $RM(3,9)$. In: EUROCODE'90, pp. 51–59. Springer (1991)
[13] Li, Y., Wang, M., Yu, Y.: Constructing Differentially 4-uniform Permutations over $gf(2^{2k})$ from the Inverse Function Revisited. IACR Cryptology ePrint Archive **2013**, 731 (2013)
[14] Matsui, M.: Linear Cryptanalysis Method For DES Cipher. In: EUROCRYPT '93 Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 386–397 (1994)
[15] Nyberg, K.: Perfect Nonlinear S-boxes. In: EUROCRYPT'91 Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques, pp. 378–386 (1991)
[16] Yu, Yuyin, Wang, Mingsheng, Li, Yongqiang: Constructing Differentially 4 Uniform Permutations from Known Ones. Chinese Journal of Electronics **22**(3), 495–499 (2013)

Paper II

On the distance between APN functions

Lilya Budaghyan, Claude Carlet, Tor Helleseth, Nikolay S. Kaleyski
IEEE Transactions on Information Theory, **vol. 66, no. 9, pp. 5742-5753** (2020)

On the distance between APN functions

Lilya Budaghyan[1], Claude Carlet[1,2], Tor Helleseth[1], and Nikolay Kaleyski[1]

[1]*Department of Informatics, University of Bergen*
[2]*Department of Mathematics, Universities of Paris VIII and XIII*

Abstract

We investigate the differential properties of a vectorial Boolean function G obtained by modifying an APN function F. This generalizes previous constructions where a function is modified at a few points. We characterize the APN-ness of G via the derivatives of F, and deduce an algorithm for searching for APN functions whose values differ from those of F only on a given $U \subseteq \mathbb{F}_{2^n}$.

We introduce a value Π_F associated with any F, which is invariant under CCZ-equivalence. We express a lower bound on the distance between a given APN function F and the closest APN function in terms of Π_F. We show how Π_F can be computed efficiently for F quadratic. We compute Π_F for all known APN functions over $\mathbb{F}_{2^n}$ up to $n \leq 8$. This is the first new CCZ-invariant for APN functions to be introduced within the last ten years.

We derive a mathematical formula for this lower bound for the Gold function $F(x) = x^3$, and observe that it tends to infinity with n.

We describe how to efficiently find all sets U such that taking $G(x) = F(x) + v$ for $x \in U$ and $G(x) = F(x)$ for $x \notin U$ is APN.

I. Introduction

A vectorial (n, m)-Boolean function is any mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, where $\mathbb{F}_{2^n}$ is the finite field with 2^n elements. Such a function can also be seen as mapping sequences of n bits (zeros and ones) to sequences of m bits, which more clearly reveals their practical importance. Vectorial Boolean functions are of central interest in cryptography since they can be used to represent virtually all components of a block cipher; in particular, its non-linear components (whose cryptographic properties directly influence the cipher's security) can be expressed as vectorial Boolean functions. For instance, the Advanced Encryption Standard (AES) and algorithms based on Feistel networks such as the Data Encryption Standard (DES), all utilize vectorial Boolean functions in the role of so-called "substitution boxes". The resistance of the encryption to various categories of cryptanalytic attacks then directly depends on the properties of the underlying Boolean functions (see e.g. [22] for basic background on cryptography and encryption schemes).

Almost Perfect Nonlinear (APN) functions were introduced by Nyberg [20] as the functions that provide optimal resistance to the so-called differential attack invented by Biham and Shamir [2]. More precisely, we say that a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if the equation $F(x) + F(x + a) = b$ in x has at most 2 solutions for any $a \in \mathbb{F}_{2^n}^*$ and any $b \in \mathbb{F}_{2^n}$. Despite the simplicity of this definition, finding and investigating the properties of APN functions, even in finite fields of relatively low dimension, is a challenging task. For this reason, various methods of constructing such functions have been considered by researchers.

This paper was presented in part at the Third International Workshop on Boolean Functions and their Applications (BFA-2018) which took place in Loen, Norway on June 17-22, 2018 [5]

In [6], a construction in which a function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is obtained from a given function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ by modifying one of its values is introduced in an attempt to resolve the open problem of the existence of APN functions over $\mathbb{F}_{2^n}$ of algebraic degree n. A number of nonexistence results are obtained in the paper, which support the conjecture that this is impossible. The idea of the construction is interesting in its own right, however, and it can naturally be generalized to the modification of more than one point.

The particular case of swapping two points of a given function is studied [24] in the context of constructing differentially 4-uniform permutations, and the more general question of arbitrarily modifying the values of a given function at two points, as well as swapping two points in a more general context, is investigated in [17].

In this paper, we consider the general case of arbitrarily changing K points. To be more accurate, given a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, some K distinct field elements $u_1, \ldots, u_K \in \mathbb{F}_{2^n}$ and some K elements $v_1, v_2, \ldots, v_K \in \mathbb{F}_{2^n}^*$, we define G as

$$G(x) = \begin{cases} F(u_i) + v_i & x = u_i \\ F(x) & x \notin \{u_1, u_2, \ldots, u_K\} \end{cases}$$

and try to find some correlation between the properties of F and those of G. We derive sufficient and necessary conditions that the derivatives of F must satisfy in order for G to be APN, and obtain an efficient filtering procedure for finding all possible values of $v_1, v_2, \ldots, v_K$ in the case that $u_1, u_2, \ldots, u_K$ are known. In the case when F is itself APN, we define the values Π_F and m_F, which count the number of derivatives of F satisfying a certain condition, and express a lower bound on the distance between F and the closest APN function in terms of m_F. We further demonstrate that these values are invariant under CCZ-equivalence and that their computation is particularly efficient when F is quadratic. In addition, we show how an exact formula for m_F can be computed in the case of $F(x) = x^3$.

We experimentally compute Π_F and m_F for all known APN functions over $\mathbb{F}_{2^n}$ for $n \leq 8$. We notice that over fields of odd dimension, this new invariant tends to take the same value for all known APN functions except the inverse function, but for fields of even dimension, it can take a large number of distinct values which make it a useful tool for disproving CCZ-equivalence between a given pair of functions. These experimental results are summarized in Section IV and Table II, and a detailed table of the computational results can be found online at *https://boolean.h.uib.no/mediawiki/*.

In the case when $v_1 = v_2 = \cdots = v_K$, we show how all possible combinations of points $u_1, u_2, \ldots, u_K$ can be found (for all values of K) by solving a system of linear equations. We note that constructions of the form $G(x) = F(x) + vf(x)$ for $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ have been investigated in [7], [16].

II. Preliminaries

A. Basic Notation

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements; in particular, $\mathbb{F}_2$ is the field with two elements. For any positive integer m, $\mathbb{F}_2^m$ is the vector space of dimension m over $\mathbb{F}_2$. Given any set S, we denote by S^* the set $S \setminus \{0\}$; in particular, $\mathbb{F}_{2^n}^*$ is the multiplicative group of $\mathbb{F}_{2^n}$.

The characteristic function of the set S is denoted by $1_S(x)$ and is defined as

$$1_S(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S. \end{cases}$$

For a finite set $S = \{s_1, s_2, \ldots, s_k\}$ we will use $1_{s_1,s_2,\ldots,s_k}(x)$ as shorthand for $1_{\{s_1,s_2,\ldots,s_k\}}(x)$.

B. Representation of Vectorial Functions

Given two positive integers n and m, a vectorial Boolean (n, m)-function, or simply (n, m)-function, is any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. It can be uniquely expressed in the so-called *algebraic normal form* (ANF) as follows [10]:

$$F(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq \{1,2,\ldots,n\}} a_I x^I, a_I \in \mathbb{F}_2^m.$$

The *algebraic degree* of $F(x_1, x_2, \ldots, x_n)$ is defined as the degree of its ANF, namely

$$\deg(F) = \max\{|I| : a_I \neq (0, 0, \ldots, 0), I \subseteq \{1, 2, \ldots, n\}\}.$$

Clearly, $\deg(F) \leq n$.

Vectorial Boolean $(n, 1)$-functions, i.e. functions of the form $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, are referred to as *Boolean functions*.

When $m = n$, one can identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$. Note that any basis $\{e_1, e_2, \ldots, e_n\}$ for $\mathbb{F}_{2^n}$, viewed as a vector space over $\mathbb{F}_2$, determines a correspondence between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ via $x = \sum_{i=1}^n x_i e_i$. The algebraic degree does not depend on the choice of the basis since any change of basis corresponds to a linear permutation. Then any (n, n)-function has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, a_i \in \mathbb{F}_{2^n}.$$

Let $x = \sum_{i=1}^n x_i e_i$ and $i = \sum_{s=0}^{n-1} i_s 2^s$ where $i_s \in \{0, 1\}$. Then F can be rewritten as

$$F(x) = \sum_{i=0}^{2^n-1} a_i \left(\sum_{i=1}^n x_i e_i \right)^i = \sum_{i=0}^{2^n-1} a_i \prod_{s=0}^{n-1} \left(\sum_{i=1}^n x_i e_i^{2^s} \right)^{i_s}$$

which, after expansion, gives the ANF of F. Moreover, let $w_2(i) = \sum_{s=0}^{n-1} i_s$ denote the 2-weight of i, where $0 \leq i \leq 2^n - 1$ has binary expansion $i = \sum_{s=0}^{n-1} 2^s i_s$. Then the algebraic degree of F in univariate polynomial form is equal to

$$\deg(F) = \max\{w_2(i) : a_i \neq 0, 0 \leq i \leq 2^n - 1\}.$$

Given two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the *Hamming distance* $d(F, G)$ is defined as the number of points $x \in \mathbb{F}_{2^n}$ on which the values of F and G differ, i.e.

$$d(F, G) = |\{x \in \mathbb{F}_{2^n} : F(x) \neq G(x)\}|.$$

C. Almost Perfect Nonlinear Functions and Bent Functions

Let F be a function from $\mathbb{F}_{2^n}$ to itself. The *derivative of F in direction a* for any $a \in \mathbb{F}_{2^n}$ is the function $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined as

$$D_aF(x) = F(x) + F(a + x).$$

The *differential sets* H_aF are the image sets of the derivatives of F, i.e. the sets

$$H_aF = \{D_aF(x) : x \in \mathbb{F}_{2^n}\} = \{F(x) + F(a + x) : x \in \mathbb{F}_{2^n}\}.$$

Alongside the derivatives D_aF, we define the *shifted derivative* $D_a^\beta F$ of F *in direction a with shift β*, which is a function over $\mathbb{F}_{2^n}$ defined as

$$D_a^\beta F(x) = D_aF(x) + F(a + \beta) = F(x) + F(a + x) + F(a + \beta)$$

for any fixed $a, \beta \in \mathbb{F}_{2^n}$. The *shifted differential sets* $H_a^\beta F$ are then the image sets of the shifted derivatives, i.e.

$$H_a^\beta F = \{D_a^\beta F(x) : x \in \mathbb{F}_{2^n}\} = \{F(x) + F(a + x) + F(a + \beta) : x \in \mathbb{F}_{2^n}\}.$$

For any $a, b \in \mathbb{F}_{2^n}$, define $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}|$; that is, $\Delta_F(a, b)$ is the number of solutions x of the equation $D_aF(x) = b$ for some given a and b. Then the *differential uniformity* of F is defined as

$$\Delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}.$$

A function F from $\mathbb{F}_{2^n}$ to itself is called *differentially δ-uniform* if $\Delta_F \leq \delta$. If $\delta = 2$, then F is called *almost perfect nonlinear* (APN). Note that this is optimal in the case of a finite field of characteristic two, since if some x solves $F(x) + F(a + x) = b$, then so does $(a + x)$, and thus $\Delta_F(a, b)$ is always even.

Note that the definition of differential uniformity can be extended to functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ between fields of different dimensions. A *perfect nonlinear* (PN) function is one whose differential uniformity is 2^{n-m}; as observed above, for $n = m$ such functions cannot exist. In fact, PN functions are the same as bent functions (briefly discussed below) and do not exist whenever $m > n/2$ [19].

A number of useful characterizations of APN functions can be given in terms of the so-called Walsh transform. The Walsh transform of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(ax)}, \quad a \in \mathbb{F}_2,$$

where $\mathrm{Tr}_k^n(x) = \sum_{i=0}^{n-1} x^{2^{ki}}$ is the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^k}$, for $k \mid n$. We will also use the inverse Walsh transform formula, defined as

$$\sum_{a \in \mathbb{F}_{2^n}} W_f(a) = 2^n(-1)^{f(0)}.$$

The Walsh transform of an (n, m)-function is defined in terms of the Walsh transform of its *component functions* $\mathrm{Tr}_1^m(bF(x))$ for $b \in \mathbb{F}_{2^m}^*$ as

$$W_F(a, u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(uF(x)) + \mathrm{Tr}_1^n(ax)}.$$

If the Walsh transform of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfies $W_f(a) \in \{0, \pm\mu\}$ for all $a \in \mathbb{F}_{2^n}$, then f is called a *plateaued* function with *amplitude* μ. An (n, n)-function F is called *plateaued* if all of its component functions are plateaued (possibly with different amplitudes). If all of the component functions of F are plateaued with the same amplitude, then F is called *plateaued with single amplitude*. Plateaued functions are an important class of vectorial Boolean functions since their additional structure makes them more tractable than the general case.

The following characterizations of APN functions by means of the power moments of their Walsh transform are often very useful in the investigation of APN functions.

Lemma 1 ([14])**.** Let F be an (n, n)-function. Then F is APN if and only if

$$\sum_{a\in\mathbb{F}_{2^n}} \sum_{u\in\mathbb{F}_{2^n}^*} W_F^4(a, u) = 2^{3n+1}(2^n - 1).$$

Lemma 2 ([10])**.** Let F be an APN function over $\mathbb{F}_{2^n}$ satisfying $F(0) = 0$. Then

$$\sum_{a,b\in\mathbb{F}_{2^n}} W_F^3(a, b) = 3 \cdot 2^{3n} - 2^{2n+1}.$$

Note that while Lemma 2 expresses only a necessary condition for F to be APN in the general case, in the case of a plateaued function F this condition becomes necessary and sufficient [11].

The following lemma provides an alternative characterization of the APN-ness of a vectorial Boolean function in terms of the second power moments of its derivatives.

Lemma 3 ([21], [1])**.** A function F over $\mathbb{F}_{2^n}$ is APN if and only if for all $a \in \mathbb{F}_{2^n}^*$ we have

$$\sum_{b\in\mathbb{F}_{2^n}} W_{D_aF}(0, b)^2 = 2^{2n+1}.$$

The nonlinearity $\mathcal{NL}_F$ of an (n, m)-function F is the minimum Hamming distance between its component functions and the affine functions. The nonlinearity of any (n, m)-function satisfies the so-called covering radius bound $\mathcal{NL}_F \leq 2^{n-1} - 2^{n/2-1}$. The nonlinearity can be expressed as

$$\mathcal{NL}_F = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_{2^m}, u\in\mathbb{F}_{2^n}^*} |W_F(a, u)|.$$

Functions meeting this bound are called *bent*. These coincide with the class of PN functions and exist only for $m \leq n/2$ [21]. In particular, for $m = n$, which is our case of interest, bent functions do not exist.

When n is odd, the optimal (n, n)-functions from the point of view of nonlinearity are the almost bent functions. An (n, n)-function F is called *almost bent* (AB) if it satisfies $W_F(a, u) \in \{0, \pm 2^{(n+1)/2}\}$ for all $a \in \mathbb{F}_{2^n}$ and nonzero $u \in \mathbb{F}_{2^n}^*$. Any AB function is APN, but not vice versa. However, for n odd, every quadratic APN function is also AB [12]. An (n, n)-function F is AB if and only if all the values $W_F(u, v)$ in its Walsh spectrum are divisible by $2^{\frac{n+1}{2}}$ [9].

D. Equivalence Relations of Functions

There are several equivalence relations of functions for which differential uniformity and nonlinearity are invariant. Due to these equivalence relations, having only one APN (respectively, AB) function, one can generate a huge class of APN (respectively, AB) functions.

Two functions F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ are called

- *affine equivalent* (*linear equivalent*) if $F' = A_1 \circ F \circ A_2$, where the mappings A_1 and A_2 are affine (linear) permutations of $\mathbb{F}_{2^n}$;
- *extended affine equivalent* (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings $A, A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine, and A_1, A_2 are permutations;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

Although different, these equivalence relations are related. It is obvious that linear equivalence is a particular case of affine equivalence, and that affine equivalence is a particular case of EA-equivalence. As shown in [12], EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence. Let us recall why the structure of CCZ-equivalence implies this: for a function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and an affine permutation $\mathcal{L}(x, y) = \big(L_1(x, y), L_2(x, y)\big)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, where $L_1, L_2 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, we have

$$\mathcal{L}(G_F) = \{\big(F_1(x), F_2(x)\big) : x \in \mathbb{F}_{2^n}\} \tag{1}$$

where $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$.

Note that $\mathcal{L}(G_F)$ is the graph of a function if and only if F_1 is a permutation. The function CCZ-equivalent to F whose graph equals $\mathcal{L}(G_F)$ is then $F' = F_2 \circ F_1^{-1}$. The composition by the inverse of F_1 modifies the algebraic degree in general, except, for instance, when $L_1(x, y)$ depends only on x, which corresponds to EA-equivalence of F and F' [8]. It is also proven in [8] that CCZ-equivalence is strictly more general that EA-equivalence combined with taking inverses of permutations.

Proposition 1 ([8])**.** Let F and F' be functions from $\mathbb{F}_2^n$ to itself. The function F' is EA-equivalent to the function F or to the inverse of F (if it exists) if and only if there exists an affine permutation $\mathcal{L} = (L_1, L_2)$ on $\mathbb{F}_2^{2n}$ such that $\mathcal{L}(G_F) = G_{F'}$ and L_1 depends only on one variable, i.e. $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.

It is worth listing some properties that remain invariant under CCZ-equivalence. Let the functions F and F' be CCZ-equivalent. Then

- $\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\} = \{\Delta_{F'}(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ [4], [8];
- if F is APN then F' is APN too;
- $\mathcal{NL}_F = \mathcal{NL}_{F'}$ [12];
- if F is AB then F' is AB too.

III. Changing points in general

A construction in which an (n, n)-function G is obtained by changing a single value of a given (n, n)-function F is investigated in [6]. More precisely, given a function F

over $\mathbb{F}_{2^n}$, the construction is performed by defining a function G over the same field by

$$G(x) = \begin{cases} F(x) & x \neq u \\ v & x = u \end{cases}$$

for some fixed elements $u, v \in \mathbb{F}_{2^n}$. Since G can be written as $G(x) = F(x) + (F(u) + v)(1+(x+u)^{2^n-1})$, it is easy to see that the algebraic degree of at least one of F and G must be equal to n; furthermore, any function G of algebraic degree n can be written in this form for some F of algebraic degree less than n. Indeed, the motivation behind the study of this construction is the unresolved questions of whether APN functions of algebraic degree n can exist over $\mathbb{F}_{2^n}$; the authors investigate the possibility of obtaining an APN function G using the construction, with particular attention being paid to the case when F is itself APN. Two main characterizations of the APN-ness of G are obtained in [6], one involving the Walsh coefficients of F, and one based on the properties of the derivatives D_aF. These characterizations are then applied in order to conclude that no function G obtained by such a one-point change from a given F which is a power, plateaued, quadratic or almost bent function can be APN, except possibly for $n \leq 2$ in the case of plateaued functions. For instance, $F(x) = x$ is plateaued and $G(x) = F(x) + x^{2^n-1} = x^3 + x$ is APN over $\mathbb{F}_{2^2}$; in the case of power, quadratic and almost bent functions, we only have trivial examples over $\mathbb{F}_2$, e.g. when F is the identity function $F(x) = x$ and G is the constant zero function $G(x) = 0$. A number of additional non-existence results are also shown, which support the conjecture that no APN function of algebraic degree n may exist over $\mathbb{F}_{2^n}$; nonetheless, the question in general remains open.

Some properties of the special case when the values of F at two given points are swapped have previously been investigated in [24], and the general case of changing the values of F at two points has been considered in [17]. The authors of the former article have generalized their method to changing points lying on a cycle [18], and have been able to construct involutions over $\mathbb{F}_{2^n}$ using this method [15]. In [17], two main characterizations of the APN-ness of a new function G obtained by modifying two values of a given F are obtained, one in terms of the power moments of the Walsh transform, and one in terms of the differential properties F. We observed that if F and G are at distance two, then at most one of F and G can be AB, and at most one of them can be plateaued; furthermore, if the algebraic degree of F is less than $n-1$, then G can be neither AB nor plateaued for any $n \geq 3$. In the case of swapping the values of a function at 0 and 1, we obtained a sufficient condition for disproving the APN-ness of G by computing a lower bound on the sum $\sum_{y \in \mathbb{F}_{2^n}} \Delta_F(y, F(y)+1) + \Delta_F(y+1, F(y))$. We also showed how to compute a lower bound on this quantity in the case of power functions by finding multiple solutions to the equation $F(x) + F(a+x) + F(a) = 1$ when F is a power function.

The idea of investigating pairs of functions at a small distance to one another is interesting per se, and the aforementioned construction can be naturally extended so that the value of F is changed at more than one point. In the following, we investigate whether, and under what conditions, it is possible to obtain an APN function by changing the values of *multiple* points in a given APN function F. More precisely, given K distinct elements $u_1, u_2, \ldots, u_K$ from $\mathbb{F}_{2^n}$ (referred to as *points*) and K

arbitrary elements $v_1, v_2, \ldots, v_K$ from $\mathbb{F}_{2^n}$ (referred to as *shifts*), we are interested in the APN-ness of the function

$$G(x) = F(x) + \sum_{i=1}^{K} 1_{u_i}(x)v_i = F(x) + \sum_{i=1}^{K}(1 + (x + u_i)^{2^n-1})v_i \tag{2}$$

whose value coincides with the value of F on all points $x \notin \{u_1, u_2, \ldots, u_K\}$ and satisfies $G(u_i) = F(u_i) + v_i$ for $i \in \{1, 2, \ldots, K\}$.

In order to facilitate the following discussion, we introduce some notation related to the construction. We denote by U the set $U = \{u_1, u_2, \ldots, u_K\}$ of points whose value will change. For a given element $a \in \mathbb{F}_{2^n}$, we denote by $a + U$ the set $\{a + u : u \in U\}$. For any given natural number n, we write $[n] = \{1, 2, \ldots, n\}$; in particular, $[K]$ is the set of indices of the points from U. For any given $a \in \mathbb{F}_{2^n}^*$ we define the set $U_a = \{u \in U : a + u \in U\}$, and $\overline{U_a} = U \setminus U_a$. In addition, we define a function p_a on the indices $\{i \in [K] : u_i \in U_a\}$ by the prescription $p_a(i) = j$ where j is such that $u_i + a = u_j$. Since the definition of an APN function is given in terms of differential equations, a natural way to investigate the properties of G is to examine the derivatives D_aG and their relation to the derivatives D_aF of F. From the definition of G in (2) we can immediately see that for any $a \in \mathbb{F}_{2^n}^*$, the derivative D_aG takes the form

$$D_aG(x) = D_aF(x) + \sum_{i=1}^{K} 1_{u_i, a+u_i}(x)v_i. \tag{3}$$

Although all the points u_i are assumed distinct, it is possible that for some $i \neq j$ we have $a + u_i = u_j$ and the sets $\{u_i, a + u_i\}$ and $\{u_j, a + u_j\}$ will coincide. This can be seen more easily if (3) is written in the form

$$D_aG(x) = D_aF(x) + \sum_{i \in U_a : i < p_a(i)} 1_{u_i, u_{p_a(i)}}(x)(v_i + v_{p_a(i)}) + \sum_{i \in \overline{U_a}} 1_{u_i, a+u_i}(x)v_i. \tag{4}$$

A characterization of the conditions under which G is APN can be derived immediately from (3) and the definition of an APN function by examining under what conditions a triple of elements $(a, x, y) \in \mathbb{F}_{2^n}^3$ with $a \neq 0$, $D_aG(x) = D_aG(y)$ and $x + y \notin \{0, a\}$ may exist.

Proposition 2. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, let $u_1, u_2, \ldots, u_K$ be K distinct points from $\mathbb{F}_{2^n}$ and let $v_1, v_2, \ldots, v_K$ be K arbitrary elements from $\mathbb{F}_{2^n}$. Then the function G defined by (2) is APN if and only if all of the following conditions are satisfied for every derivative direction $a \in \mathbb{F}_{2^n}^*$:

(i) D_aF is 2-to-1 on $\mathbb{F}_{2^n} \setminus (U \cup a + U)$;
(ii) $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j + v_{p_a(i)} + v_{p_a(j)}$ for $u_i, u_j \in U_a$ unless $u_i = u_j$ or $u_i + u_j = a$;
(iii) $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j + v_{p_a(i)}$ for $u_i \in U_a, u_j \in \overline{U_a}$;
(iv) $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j$ for $u_i, u_j \in \overline{U_a}$ unless $u_i = u_j$;
(v) $D_aF(u_i) + D_aF(x) \neq v_i + v_{p_a(i)}$ for $u_i \in U_a, x \notin (U \cup a + U)$;
(vi) $D_aF(u_i) + D_aF(x) \neq v_i$ for $u_i \in \overline{U_a}, x \notin (U \cup a + U)$.

Proof. Recall that G is APN if and only if there does not exist a triple $(a, \bar{x}, \bar{y}) \in \mathbb{F}_{2^n}^3$ such that $D_aG(\bar{x}) = D_aG(\bar{y})$ with $a \neq 0$ and $\bar{x} \notin \{\bar{y}, a + \bar{y}\}$. Suppose that such a triple does exist. We will now go through several possible cases, depending on whether $\bar{x}$ and $\bar{y}$ are in $(U \cup a + U)$ or not. In the first case, we will assume that neither $\bar{x}$ nor $\bar{y}$ is in $(U \cup a + U)$; in the second case, we will assume that both $\bar{x}$ and $\bar{y}$ are in $(U \cup a + U)$; and in the third case, we will assume that precisely one of $\bar{x}$ and $\bar{y}$ is in $(U \cup a + U)$:

1) If neither $\bar{x}$ nor $\bar{y}$ belong to $(U \cup a + U)$, then $D_aG(\bar{x}) = D_aF(\bar{x})$ and $D_aG(\bar{y}) = D_aF(\bar{y})$ so that $D_aG(\bar{x}) = D_aG(\bar{y})$ implies $D_aF(\bar{x}) = D_aF(\bar{y})$. Thus D_aF cannot be 2-to-1 over $\mathbb{F}_{2^n} \setminus (U \cup a + U)$. Conversely, if D_aF is 2-to-1 over $\mathbb{F}_{2^n} \setminus (U \cup a + U)$, this guarantees that no such triple can exist with $\bar{x}, \bar{y} \notin (U \cup a + U)$. This leads to the first condition.
2) If both $\bar{x}$ and $\bar{y}$ are points from U or $a + U$, say $\bar{x} = u_i$ and $\bar{y} = u_j$, then we have $D_aG(u_i) = D_aG(u_j)$. We now examine three cases depending on whether one, both or none of u_i and u_j are in U_a:
   a) If $D_aG(u_i) = D_aG(u_j)$ with $u_i, u_j \in U_a$, then we have $D_aF(u_i) + v_i + v_{p_a(i)} = D_aF(u_j) + v_j + v_{p_a(j)}$ from the definition of G (2). If G is APN, this is possible only if $u_i = u_j$ or $u_i = a + u_j$, which leads to the second condition.
   b) If say u_i is in U_a but u_j is not, then $D_aG(u_i) = D_aG(u_j)$ becomes $D_aF(u_i) + D_aF(u_j) = v_i + v_j + v_{p_a(i)}$. Note that we can have neither $u_i = u_j$, nor $u_i + a = u_j$ since u_i is in U_a and u_j is in its complement. This leads to the third condition.
   c) If neither u_i nor u_j is in U_a, then $D_aG(u_i) = D_aG(u_j)$ becomes $D_aF(u_i) + D_aF(u_j) = v_i + v_j$; this can occur if $u_i = u_j$, but $u_i = a + u_j$ is impossible due to $u_j \notin U$. This gives the fourth condition.
3) In the remaining case, we assume that we have $\bar{x} = u_i$ (or $\bar{x} = a + u_i$) but $\bar{y} \notin (U \cup a + U)$, so that we have $D_aG(u_i) = D_aF(\bar{y})$. We examine two sub-cases:
   a) If $D_aG(u_i) = D_aG(\bar{y})$ with $u_i \in U_a$, then $D_aF(u_i) + D_aF(\bar{y}) = v_i + v_{p_a(i)}$. Since both u_i and $u_i + a$ are in U, we cannot have $u_i \in \{y, a + y\}$. This gives the fifth condition.
   b) If, conversely, $D_aG(u_i) = D_aG(\bar{y})$ but $u_i \in \overline{U_a}$, then we have $D_aF(u_i) + D_aF(\bar{y}) = v_i$. As before, we cannot have $u_i \in \{\bar{y}, a + \bar{y}\}$. This gives the sixth and final condition.

The above conditions are clearly necessary for G to be APN, and they are also sufficient since if we have $D_aG(\bar{x}) = D_aG(\bar{y})$ then one of these conditions implies $\bar{x} = \bar{y}$ or $\bar{x} = a + \bar{y}$. □

The following observation shows how condition (vi) of Proposition 2 can be equivalently expressed in terms of the shifted derivatives of F. This is slightly more intuitive in the sense that it allows us to consider the image of a single shifted derivative (instead of the sum of two derivatives as in the original formulation) and is used throughout the next section.

Observation 1. Assume the same notation as in Proposition 2. If G is APN, then for any $a \in \mathbb{F}_{2^n}^*$ for which there exists an $i \in [K]$ such that $D_a^{u_i}F$ maps to $F(u_i) + v_i$ and $a + u_i \notin U$ we must have

$$D_a^{u_i}F(u_j) + F(u_i) = v_i,$$

for some $i \neq j \in [K]$.

Characterizing the APN-ness of G is difficult in the general case due to the large number of choices for the points $u_1, u_2, \ldots, u_K$ and shifts $v_1, v_2, \ldots, v_K$. For this reason, in the following sections we concentrate on various simplifications of this problem, e.g. by assuming that the points $u_1, u_2, \ldots, u_K$ or the number K are fixed.

IV. The case of fixed $u_1, u_2, \ldots, u_K$

If we fix the set U of points to change, we can use Observation 1 to dramatically reduce the number of potential candidate values for the shifts $v_1, v_2, \ldots, v_K$. Besides filtering out impossible candidates for the shifts v_i, this allows us to obtain a lower bound on the distance between a given APN function F and its closest APN neighbor. This lower bound is given in terms of the number of shifted derivatives of F that map to the elements of $\mathbb{F}_{2^n}$. This quantity can be computed efficiently in practice and can be used to bound from below the number of points K that need to be changed in order to obtain an APN function G. Finally, we observe that this lower bound is invariant under CCZ-equivalence.

A. Filtering out shift candidates

We can immediately apply Observation 1 in practice by fixing some function F over $\mathbb{F}_{2^n}$ along with K points $u_1, u_2, \ldots, u_K$ and then, for every $i \in [K]$, making a list of all values $\bar{v} \in \mathbb{F}_{2^n}$ for which setting $v_i = \bar{v}$ violates the necessary condition from Proposition 2. Then only values v_i which are not in this list have to be examined, and their number is typically much smaller than the number 2^n of all possible values. In many cases, no values at all are left for some v_i, which then immediately indicates that no APN functions can be obtained by shifting the points in U.

A more precise description of this procedure is given as Algorithm 1.

Algorithm 1: Reducing the domains of v_i using Observation 1

Data: A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and a set of K distinct points $U = \{u_1, u_2, \ldots, u_K\} \subseteq \mathbb{F}_{2^n}$.
Result: A domain $D_i \subseteq \mathbb{F}_{2^n}$ for every v_i such that if $G(x)$ is APN, then $v_i \in D_i$ for every $i \in [K]$.
begin
  for *every* $i \in [K]$ **do**
    set $D_i \leftarrow \mathbb{F}_{2^n}$
    compute
    $A \leftarrow \{D_a^{u_i} F(x) + F(u_i) : x, a \in \mathbb{F}_{2^n}, a \neq 0, a + u_i \notin U, x \notin (U \cup a + U)\}$
    update $D_i \leftarrow D_i \setminus A$

As already mentioned, the efficiency of this method is particularly prominent in cases when the points $u_1, u_2, \ldots, u_K$ cannot be shifted into an APN function (in the sense that G is never APN regardless of the choice of $v_1, v_2, \ldots, v_K$). For example, given the function $F(x) = x^3$ over $\mathbb{F}_{2^5}$ and the set of points $U = \{\alpha^i : i \in \{0\} \cup [5]\}$, where α is a primitive element of $\mathbb{F}_{2^5}$, checking every combination of shifts $(v_1, \ldots, v_K) \in \mathbb{F}_{2^5}^6$ using an exhaustive search (that is, generating G as defined in (2) and testing whether it is APN for every such combination of shifts) is estimated to take about 75 hours; using the filtering approach described above, however, we can conclude that no APN function G can be obtained by any combination of shifts

after only about 0.140 seconds of computation. These experiments were performed on our department server, with the search procedures implemented in the *Magma* programming language.

On the contrary, in some situations (especially when the set of points U can be shifted into an APN function) the filtering procedure may leave rather large domains for the shift candidates, which necessitates long computations. As two contrasting examples, we examine the function x^3 over $\mathbb{F}_{2^5}$ and over $\mathbb{F}_{2^6}$. In the case of $\mathbb{F}_{2^5}$, taking the set U of the eight points generated (in the sense of additive closure) by $\{\alpha^i : i \in \{0\} \cup [2]\}$ leaves the singleton domain $\{\alpha^{25}\}$ for all v_i; indeed, the function G obtained by shifting every point from U by α^{25} is APN and is CCZ-equivalent to x^5. However, when we take $F(x) = x^3$ over $\mathbb{F}_{2^6}$ with U being generated by $\{1, \beta, \beta^4, \beta^{21}\}$ (with β primitive in $\mathbb{F}_{2^n}$), the domains for each v_i after filtering become $D = \{\beta^7, \beta^{14}, \beta^{28}, \beta^{35}, \beta^{49}, \beta^{56}\}$. Taking $v_1 = v_2 = \cdots = v_{16} = v$ for any $v \in D$ then yields an APN function G that is CCZ-equivalent to $x^6 + x^9 + \beta^7 x^{48}$. Conversely, if at least two different values are selected for the shifts, the resulting function is not APN; thus, there are only $|D| = 6$ possible shift combinations that lead to an APN function, but 6^{16} potential combinations that are left after filtering and need to be "manually" checked. Therefore, although our method reduces the size of the domains from $2^6 = 64$ to just 6, the resulting search space is still quite large and requires a significant amount of time in order to be completely explored.

However, additional restrictions may be imposed on the values of v_i by applying conditions (i)-(v) from Proposition 2 which allow the search to be performed more efficiently. More precisely, condition (iv) allows us to remove pairs, condition (iii) allows us to remove triples and condition (ii) allows us to remove quadruples of incompatible elements from the domains. Condition (i) depends entirely on the function F and the set U and can be used to reject a given set U entirely, although it cannot be used for filtering the domains.

These conditions do not allow us to remove any values from the domains of v_i directly, but they do make it possible to restrict some domains after a first few initial choices. For example, having selected a concrete value $\bar{v}_i$ for v_i from its domain, we can for all $j \neq i$, remove values $\bar{v}_j$ from the domain of v_j for which condition (iv) is violated. It is worth noting that this is the most useful of the three conditions given above in the case that the number of points U is relatively small, since it encompasses the greatest number of derivative directions; as K increases, the latter two conditions become more useful. In any case, ensuring that all the conditions from Proposition 2 are satisfied is sufficient to ensure that G is APN.

Coming back to the example of $F(x) = x^3$ over $\mathbb{F}_{2^6}$ discussed above, we can see how much this improves the search efficiency: evaluating all combinations of shifts from the domains (without any filtering) would require approximately 110 years; applying conditions (i)-(iv) from Proposition 2 as described, however, finds all six possibilities in about two seconds.

B. Lower bound on the distance between APN functions

Note that in the statement of Observation 1, we assume that the resulting function G is APN but we do not make any assumptions about F. If, in addition to the hypothesis of the theorem, we assume that F is itself APN, we can obtain the following corollary

which gives a lower bound on the Hamming distance between a given APN function and its nearest APN "neighbor".

Corollary 1. Let F and G be as in the statement of Observation 1 with $v_i \neq 0$ for $i \in [K]$, and assume, in addition, that F is APN; consider some fixed $i \in [K]$. Then no more than $3(K-1)$ derivatives of the form $D_a^{u_i}F$ map to $G(u_i)$.

Proof. First, consider all derivative directions $a \in \mathbb{F}_{2^n}^*$ with $a + u_i \notin U$. By Observation 1 we must have

$$D_a^{u_i}F(u_j) = G(u_i)$$

for some $j \neq i$ if $D_a^{u_i}F$ maps to $G(u_i)$. We now determine for how many $a \in \mathbb{F}_{2^n}$ we may have $D_a^{u_i}F(u_j) = G(u_i)$ for fixed i and j. Suppose that we have both $D_a^{u_i}F(u_j) = G(u_i)$ and $D_{a'}^{u_i}F(u_j) = G(u_i)$ for some $a \neq a'$. Then $D_a^{u_i}F(u_j) = D_{a'}^{u_i}F(u_j)$ can be rewritten as $F(u_j) + F(a + u_j) + F(a + u_i) = F(u_j) + F(a' + u_j) + F(a' + u_i)$ so that we have $D_{u_i+u_j}F(a + u_i) = D_{u_i+u_j}F(a' + u_i)$.

Since i and j (and therefore u_i and u_j) are fixed and since F is APN, this implies either $a = a'$ or $a+a' = u_i+u_j$. In other words, at most two distinct shifted derivatives may map u_j to $G(u_i)$.

Now suppose that i is fixed and j ranges over $[K]$. Since we consider only $j \neq i$ and since there are K indices in total, there are $(K-1)$ choices for j for any fixed i. For each such j, there are at most two shifted derivatives $D_a^{u_i}F$ mapping u_j to $G(u_i)$. Therefore, at most $2(K-1)$ shifted derivatives may take $G(u_i)$ as value when $a + u_i \notin U$.

We now consider the derivative directions $a \in \mathbb{F}_{2^n}$ for which $a + u_i \in U$. There are precisely K such directions a, viz. $u_1 + u_i$, $u_2 + u_i$, $\ldots$, $u_K + u_i$. Furthermore, $D_0^{u_i}F$ cannot map to $G(u_i)$ unless $v_i = 0$, so that there are at most $(K-1)$ derivatives of this type which may map to $G(u_i)$.

Thus, in total, there can be no more than $2(K-1) + (K-1) = 3(K-1)$ derivative directions a for which $D_a^{u_i}F$ maps to $G(u_i)$. □

Note that in the proof above, the number of derivative directions a (with $a+u_i \notin U$) such that $D_a^{u_i}F(u_j) = G(u_i)$ for some fixed i and j is limited to two because F is assumed to be APN. If we take F to be differentially δ-uniform instead, the upper bound on the number of derivatives $D_a^{u_i}F$ mapping to $G(u_i)$ will be $(\delta+1)(K-1)$.

Corollary 1 can now be used to compute a lower bound on the distance between a given F and its nearest APN "neighbor". In order to facilitate the following discussion, we introduce some notation related to the shifted derivatives. In particular, we define $\Pi_F^\beta(b)$ to be the set of derivative directions a for which $D_a^\beta F$ maps to b, i.e.

$$\Pi_F^\beta(b) = \{a \in \mathbb{F}_{2^n} : b \in H_a^\beta F\} = \{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_a^\beta F(x) = b)\}.$$

By Corollary 1, we need to count the numbers $|\Pi_F^{u_i}(G(u_i))|$ for $i \in [K]$ and ensure that none of them is greater than $3(K-1)$. The minimum value of $|\Pi_F^\beta(b)|$ through all possible values of β and b is certainly a lower bound on $\min_{i\in[K]} |\Pi_F^{u_i}(G(u_i))|$; if this minimum value is greater than $3(K-1)$ for some given K, then no function G within distance K of F can be APN.

Thus, we can apply the lower bound from Corollary 1 by computing the minimum value of $|\Pi_F^\beta(b)|$ through all $\beta, b \in \mathbb{F}_{2^n}$. In certain cases, such as for quadratic functions (see Proposition 5 below), it suffices to consider a fixed value of β and to only go through all $b \in \mathbb{F}_{2^n}$. For this reason, we define the set Π_F^β as the spectrum of the values of $|\Pi_F^\beta(b)|$ for a fixed shift β, i.e.

$$\Pi_F^\beta = \{|\Pi_F^\beta(b)| : b \in \mathbb{F}_{2^n}\}$$

and Π_F as the spectrum of $|\Pi_F^\beta(b)|$ for all shifts β and all values b:

$$\Pi_F = \bigcup_{\beta \in \mathbb{F}_{2^n}} \Pi_F^\beta = \{|\Pi_F^\beta(b)| : \beta, b \in \mathbb{F}_{2^n}\}.$$

For convenience, we also denote by m_F the minimal element of Π_F, i.e. $m_F = \min\{|\Pi_F^\beta(b)| : \beta, b \in \mathbb{F}_{2^n}\}$. The lower bound on the distance between APN functions can now be stated as follows.

Corollary 2. Let F be an APN function over $\mathbb{F}_{2^n}$ and let m_F be the number

$$m_F = \min \Pi_F = \min_{b,\beta \in \mathbb{F}_{2^n}} |\Pi_F^\beta(b)| = \min_{b,\beta \in \mathbb{F}_{2^n}} |\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_a^\beta F(x) = b)\}|.$$

Then for any APN function $G \neq F$ over $\mathbb{F}_{2^n}$, the Hamming distance $d(F, G)$ between F and G satisfies

$$d(F, G) \geq \left\lceil \frac{m_F}{3} \right\rceil + 1. \tag{5}$$

Proof. By Corollary 1, if F and G are APN functions at distance K of one another, than no more than $3(K-1)$ shifted derivatives $D_a^{u_i} F$ may map to $G(u_i)$ for any fixed $i \in [K]$. For a fixed i, this quantity can be written as $|\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_a^{u_i}(x) = G(u_i))\}|$. If we now go through all possible values of $i \in [K]$, we get that

$$\min_{i \in [K]} |\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_a^{u_i}(x) = G(u_i))\}| \leq 3(K-1).$$

Deriving a lower bound on K from this expression, however, would require knowledge of $D_a^{u_i}(x)$ and $G(u_i)$ for each $i \in [K]$. However, since u_i and $G(u_i)$ are elements of the finite field $\mathbb{F}_{2^n}$, going through all possible choices β for u_i and all possible choices b for $G(u_i)$, we clearly have

$$\min_{b,\beta} |\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_a^\beta(x) = b)\}| \leq$$
$$\min_{i \in [K]} |\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(D_a^{u_i}(x) = G(u_i))\}| \leq 3(K-1).$$

If we denote the left-most quantity by m_F, as in the statement of the Corollary, we then have

$$m_F \leq 3(K-1)$$

which immediately implies the lower bound. □

C. Invariance Properties

As discussed above, the lower bound on the Hamming distance between a given APN function F and its closest APN "neighbor" is given in terms of the number m_F which in turn can be expressed via the sets $\Pi_F^\beta(b)$, Π_F^β and Π_F. It is therefore interesting to observe that the set Π_F is invariant under CCZ-equivalence, as shown in the following proposition. This then makes the lower bound obtained via Corollary 2 for some given function F valid for all members of its CCZ-equivalence class.

Proposition 3. Suppose F is APN and is CCZ-equivalent to F' via the affine permutation $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n}^2$. Then $\Pi_F^\beta(t) = \Pi_{F'}^{L_1(\beta,t)}(L_2(\beta,t))$ for any $\beta, t \in \mathbb{F}_{2^n}$. Consequently, the set Π_F is invariant under CCZ-equivalence.

Proof. To show the first part of the statement, define $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$ as in (1); then F_1 is a permutation and $F' = F_2 \circ F_1^{-1}$.

If we consider the set of all pairs (a, x) such that $D_a^\beta F(x) = t$, we can obtain using the affinity of $\mathcal{L}$:

$$\begin{aligned}
&|\{(a,x) \in \mathbb{F}_{2^n} : F(x) + F(a+x) + F(a+\beta) = t\}| = \\
&|\{(x,y,z) \in \mathbb{F}_{2^n}^3 : (x,F(x)) + (y,F(y)) + (z,F(z)) = (\beta,t)\}| = \\
&|\{(x,y,z) : (F_1(x),F_2(x)) + (F_1(y),F_2(y)) + (F_1(z),F_2(z)) = \mathcal{L}(\beta,t)\}| = \\
&|\{(x,y,z) : (x,F'(x)) + (y,F'(y)) + (z,F'(z)) = (L_1(\beta,t),L_2(\beta,t))\}| = \\
&|\{(a,x) : F'(x) + F'(a+x) + F'(a+L_1(\beta,t)) = L_2(\beta,t)\}|.
\end{aligned} \tag{6}$$

In the third step we use the fact that F_1 is a permutation and go through all triples $(F_1^{-1}(x), F_1^{-1}(y), F_1^{-1}(z))$ instead of (x, y, z).

Now, since $|\Pi_F^\beta(t)|$ counts the number of derivative directions a for which $D_a^\beta F$ maps to t, and since all (shifted) derivatives of F and F' are 2-to-1 due to F and F' being APN, we have

$$\begin{aligned}
&2|\Pi_F^\beta(t)| = |\{(a,x) \in \mathbb{F}_{2^n} : F(x) + F(a+x) + F(a+\beta) = t\}| = \\
&|\{(a,x) : F'(x) + F'(a+x) + F'(a+L_1(\beta,t)) = L_2(\beta,t)\}| = 2|\Pi_{F'}^{L_1(\beta,t)}(L_2(\beta,t))|.
\end{aligned} \tag{7}$$

The invariance of Π_F then follows from the fact that $\mathcal{L} = (L_1, L_2)$ is a permutation and $\Pi_F = \{|\Pi_F^\beta(t)| : \beta, t \in \mathbb{F}_{2^n}\}$, so that when computing Π_F we go through all possible pairs (β, t). □

As EA-equivalence is a special case of CCZ-equivalence, it is evident that EA-equivalence leaves the set Π_F invariant as well. Under EA-equivalence, however, a stronger invariance holds.

Proposition 4. For any fixed $\beta \in \mathbb{F}_{2^n}$, if F' and F are EA-equivalent APN functions via $F' = A_1 \circ F \circ A_2 + A$, where A_1, A_2 and A are affine and A_1, A_2 are bijective, we have

$$(\forall t \in \mathbb{F}_{2^n})(|\Pi_{F'}^\beta(t)| = |\Pi_F^{A_2(\beta)}(A_1^{-1}(t + A(\beta)))|).$$

Consequently, $\Pi_{F'}^\beta = \Pi_F^{A_2(\beta)}$.

Proof. We have, thanks to F and F' being APN and their derivatives being 2-to-1 functions,

$$\begin{aligned}
&2|\Pi^{\beta}_{F'}(t)| = |\{(a,x) \in \mathbb{F}_{2^n}^2 : F'(x) + F'(a+x) + F'(a+\beta) = t\}| = \\
&|\{(a,x) : A_1(F(A_2(x))) + A_1(F(A_2(a+x))) + \\
&A_1(F(A_2(a+\beta))) + A(x) + A(a+x) + A(a+\beta) = t\}| = \\
&|\{(a,x) : A_1(F(A_2(x)) + F(A_2(a)) + F(A_2(a+x+\beta))) = t + A(\beta)\}| = \\
&|\{(a,x) : A_1(F(x) + F(a) + F(a+x+A_2(\beta))) = t + A(\beta)\}| = \\
&|\{(a,x) : F(x) + F(a) + F(a+x+A_2(\beta)) = A_1^{-1}(t + A(\beta))\}| = \\
&2|\Pi_F^{A_2(\beta)}(A_1^{-1}(t + A(\beta)))|.
\end{aligned} \tag{8}$$

In the second step we use that for any affine function A we have $A(x+y+z) = A(x) + A(y) + A(z)$ for any x, y, z, and also count through $(x, a+x)$ instead of (x, a). In the third step we use the fact that A_2 is a permutation and count through all pairs $(A_2(a), A_2(x))$ instead of (a, x); then $A_2(x)$ becomes x, $A_2(a)$ becomes a and $A_2(x + a + \beta) = A_2(x) + A_2(a) + A_2(\beta)$ becomes $x + a + A_2(\beta)$.

Then clearly

$$\begin{aligned}
\Pi^{\beta}_{F'} &= \{|\Pi^{\beta}_{F'}(t)| : t \in \mathbb{F}_{2^n}\} = \{|\Pi_F^{A_2(\beta)}(A_1^{-1}(t + A(\beta)))| : t \in \mathbb{F}_{2^n}\} \\
&= \{|\Pi_F^{A_2(\beta)}(t)| : t \in \mathbb{F}_{2^n}\} = \Pi_F^{A_2(\beta)},
\end{aligned} \tag{9}$$

thereby concluding the proof. □

D. The case of quadratic functions

For a quadratic function F, the set Π^{β}_F does not depend on the choice of β, which greatly reduces the amount of computation needed to calculate m_F.

Proposition 5. Let F be a quadratic (n,n)-function. Then $\Pi^{\beta}_F = \Pi^{\beta'}_F$ for any $\beta, \beta' \in \mathbb{F}_{2^n}$.

Proof. Since F is quadratic, its derivatives D_aF for any $a \neq 0$ are affine functions, i.e. they satisfy

$$D_aF(x) + D_aF(y) = D_aF(x+y) + D_aF(0)$$

for any $x, y \in \mathbb{F}_{2^n}$. We thus have

$$\begin{aligned}
D^{\beta}_aF(x) + D^0_aF(x+\beta) = D_aF(x) + D_aF(x+\beta) + F(a+\beta) + F(a) = \\
D_aF(\beta) + D_aF(0) + F(a+\beta) + F(a) = \\
F(\beta) + F(a+\beta) + F(0) + F(a) + F(a+\beta) + F(a) = F(\beta) + F(0)
\end{aligned} \tag{10}$$

so that we have

$$D^{\beta}_aF(x) = D^0_aF(x+\beta) + s$$

for some constant s which depends only on F and β.

We have then

$$|\Pi^{\beta}_F(t)| = |\Pi^0_F(t+s)|$$

so that, indeed,

$$\Pi^{\beta}_F = \{|\Pi^{\beta}_F(t)| : t \in \mathbb{F}_{2^n}\} = \{|\Pi^0_F(t+s)| : t \in \mathbb{F}_{2^n}\} = \Pi^0_F$$

as claimed. □

E. Examples and computation results

In some cases, the value m_F can be computed mathematically. As an example, we consider the function $F(x) = x^3$ over the finite field $\mathbb{F}_{2^n}$. We derive an exact formula for the size of $\Pi_F^\beta(b)$, which allows us to express Π_F^β and, consequently, m_F as a function of the dimension n. From this we can then immediately derive a lower bound on the distance between x^3 and the closest APN function. Note that since x^3 is quadratic, by Proposition 5 we have that $m_F = \min \Pi_F^\beta$ for an arbitrary $\beta \in \mathbb{F}_{2^n}$.

Proposition 6. Let $F(x) = x^3$ be over $\mathbb{F}_{2^n}$ and let $b, \beta \in \mathbb{F}_{2^n}$ be arbitrary. Then

$$|\Pi_F^\beta(b)| = \begin{cases} 2^n - 1 & b = \beta^3; \\ 2^{n-1} - 1 & b \neq \beta^3, n \text{ odd}; \\ 2^{n-1} + 2^{n/2} - 1 & b \neq \beta^3, b + \beta^3 \text{ is a cube}, n \text{ even}, n/2 \text{ odd}; \\ 2^{n-1} - 2^{n/2-1} - 1 & b \neq \beta^3, b + \beta^3 \text{ is not a cube}, n \text{ even}, n/2 \text{ odd}; \\ 2^{n-1} - 2^{n/2} - 1 & b \neq \beta^3, b + \beta^3 \text{ is a cube}, n \text{ even}, n/2 \text{ even}; \\ 2^{n-1} + 2^{n/2-1} - 1 & b \neq \beta^3, b + \beta^3 \text{ is not a cube}, n \text{ even}, n/2 \text{ even}. \end{cases} \tag{11}$$

The value $\min_{b \in \mathbb{F}_{2^n}} |\Pi_F^\beta(b)|$ is then equal to

$$m_F = \min \Pi_F^\beta = \begin{cases} 2^{n-1} - 1 & n \text{ is odd}; \\ 2^{n-1} - 2^{n/2-1} - 1 & n \text{ is even}, n/2 \text{ is odd}; \\ 2^{n-1} - 2^{n/2} - 1 & n \text{ is even}, n/2 \text{ is even}; \end{cases} \tag{12}$$

and the lower bound on the distance to the closest APN function G can be explicitly written as

$$d(F, G) \geq \begin{cases} \frac{2^{n-1}+2}{3} & n \text{ is odd}; \\ \frac{2^{n-1}-2^{n/2-1}+2}{3} & n \text{ is even}, n/2 \text{ is odd}; \\ \frac{2^{n-1}-2^{n/2}+2}{3} & n \text{ is even}, n/2 \text{ is even}. \end{cases} \tag{13}$$

Proof. The shifted derivative $D_a^\beta F$ of the Gold function $F(x) = x^3$ takes the form

$$D_a^\beta F(x) = x^3 + (x + a)^3 + (a + \beta)^3 = a^2(x + \beta) + a(x + \beta)^2 + \beta^3$$

for any $a, \beta \in \mathbb{F}_{2^n}$.

For convenience, we introduce the "equality indicator" $I(A, B)$, where A and B are some arbitrary expressions, defined as

$$I(A, B) = \begin{cases} 1 & A = B \\ 0 & A \neq B. \end{cases}$$

Recall that the value of $|\Pi_F^\beta(b)|$ is the number of derivative directions $a \in \mathbb{F}_{2^n}$ for which $D_a^\beta F$ maps to b. Since F is APN, $|\Pi_F^\beta(b)|$ can be expressed as

$$|\Pi_F^\beta(b)| = \frac{1}{2}|\{(a, x) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} : a^2(x + \beta) + a(x + \beta)^2 + \beta^3 = b\}| + I(b, \beta^3) = \frac{1}{2}|\{(a, x) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} : a^2 x + a x^2 = b + \beta^3\}| + I(b, \beta^3) \tag{14}$$

by substituting $x + \beta$ for x.

Note that for $a = 0$, (14) becomes $b = \beta^3$, so that the number of solutions x is $2^n I(\beta, b^3)$; however, all of these solutions correspond to the same derivative direction $a = 0$. For any fixed $a \neq 0$, we can divide both sides of the equation

$$a^2(x+\beta) + a(x+\beta)^2 = b + \beta^3$$

by a^3 and substitute $ax + \beta$ for x in order to obtain

$$x^2 + x = \frac{b+\beta^3}{a^3}. \tag{15}$$

Since $x^2 + x$ is linear with roots 0 and 1, it is a 2-to-1 mapping, and its image set over $\mathbb{F}_{2^n}$ is precisely the set of all elements with zero trace. Therefore, for a fixed $a \neq 0$, equation (15) has two solutions if $\mathrm{Tr}_n\left(\frac{b+\beta^3}{a^3}\right) = 0$, and no solutions otherwise. Consequently, if we define the function $h : \mathbb{F}_{2^n} \to \mathbb{F}_2$ as

$$h(a) = \begin{cases} \mathrm{Tr}_n\left(\frac{b+\beta^3}{a^3}\right) + 1 & a \neq 0 \\ 0 & a = 0, \end{cases}$$

we can express $|\Pi_F^\beta(b)|$ as

$$|\Pi_F^\beta(b)| = I(b, \beta^3) + \mathrm{wt}(h) \tag{16}$$

where $\mathrm{wt}(h)$ is the Hamming weight of h, i.e. the number of elements $a \in \mathbb{F}_{2^n}$ for which $h(a)$ is non-zero.

The weight of the Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined as $f(a) = \mathrm{Tr}_n(\lambda a^3)$ for some given constant $\lambda \in \mathbb{F}_{2^n}$ is known from [13]. More precisely, $\mathrm{wt}(f)$ takes the following values:

$$\mathrm{wt}(f) = \begin{cases} 0 & \lambda = 0; \\ 2^{n-1} & n \text{ odd }, \lambda \neq 0; \\ 2^{n-1} - 2^{n/2} & n \text{ even}, n/2 \text{ odd}, \lambda \text{ is a cube}, \lambda \neq 0; \\ 2^{n-1} + 2^{n/2-1} & n \text{ even}, n/2 \text{ odd}, \lambda \text{ is not a cube}, \lambda \neq 0; \\ 2^{n-1} + 2^{n/2} & n \text{ even}, n/2 \text{ even}, \lambda \text{ is a cube}, \lambda \neq 0; \\ 2^{n-1} - 2^{n/2-1} & n \text{ even}, n/2 \text{ even}, \lambda \text{ is not a cube}, \lambda \neq 0. \end{cases} \tag{17}$$

Note that in the case of $a \neq 0$ we can express the weight of h as

$$wt(h) = 2^n - wt(f) - 1 \tag{18}$$

for $f(a) = \mathrm{Tr}_n(\lambda a^3)$ with $\lambda = (b + \beta^3)$. □

From Proposition 6 we can easily see that the distance $d(x^3, G)$ tends to infinity with n. Observe that the value Π_F^β does not actually depend on the shift β; this is true for all quadratic functions as per Proposition 5.

Table I gives the values of m_F (for $F(x) = x^3$) and the lower bound on the distance between x^3 and the nearest APN function for all dimensions n in the range $1 \leq n \leq 20$. Note that for $1 \leq n \leq 4$ the bound is tight as witnessed by:

- $u_1 = 0$, $v_1 = 1$ for $n = 1$;
- $u_1 = 0$, $v_1 = \alpha$ for $n = 2$, where α is a primitive element of $\mathbb{F}_{2^2}$;

- $u_1 = 0$, $u_2 = 1$, $v_1 = 1$, $v_2 = \alpha$ for $n = 3$, where α is a primitive element of $\mathbb{F}_{2^3}$;
- $u_1 = 0$, $u_2 = 1$, $v_1 = 1$, $v_2 = 1$ for $n = 4$.

However, as soon as $n \geq 5$, the bound is no longer tight in general. Indeed, in the case of $n = 5$, we have verified that the smallest distance to an APN function is equal to 8, which shows that the bound is not tight anymore. It is worth noting, furthermore, that in this case all possible APN functions at distance 8 from x^3 were obtained by shifting 8 points from $\mathbb{F}_{2^n}$ by the same value $v \in \mathbb{F}_{2^n}$. Whether the bound is tight for some $n > 5$ remains an open question.

TABLE I
VALUES OF m_F AND LOWER BOUNDS ON $d(F, G)$ FOR ANY G APN FOR $F(x) = x^3$ OVER $\mathbb{F}_{2^n}$

Dimension	m_{x^3}	Lower bound on minimum distance
1	0	1
2	0	1
3	3	2
4	3	2
5	15	6
6	27	10
7	63	22
8	111	38
9	255	86
10	495	166
11	1023	342
12	1983	662
13	4095	1366
14	8127	2710
15	16383	5462
16	32511	10838
17	65535	21846
18	130815	43606
19	262143	87382
20	523263	174422

By Proposition 3, we know that the value m_F for some given APN function F and the lower bound K on the distance to the closest APN function derived from it are valid not only for F itself, but for all functions belonging to its CCZ-equivalence class. Since all APN functions of dimensions four and five have been classified up to CCZ-equivalence [3], Corollary 2 can now be used to obtain a lower bound on the Hamming distance between any two APN functions over $\mathbb{F}_{2^n}$ with $n \in \{4, 5\}$ by examining a single representative from each. For higher dimensions, we can compute the lower bound for the known CCZ-classes.

Table II gives the values of m_F for representatives from all switching classes [16] over $\mathbb{F}_{2^n}$ with $n \in \{4, 5, 6, 7, 8\}$. In the case of $n \in \{4, 5\}$ the selected functions encompass representatives from all CCZ-equivalence classes of the corresponding dimension. In the case of $n \in \{6, 8\}$, the functions are given and indexed according to Table 5 from [16]. Note that for $n = 7$, we obtain the same bound for all functions listed in [16] except for the inverse function. Since APN functions in dimensions $n \leq 5$ have been completely classified up to CCZ-equivalence [3], this means that for $n \leq 5$ we now have a lower bound on the distance to the closest APN function for all APN functions over $\mathbb{F}_{2^n}$.

In addition, we compute the values of Π_F and m_F for new 471, resp. 8157 APN functions over $\mathbb{F}_{2^7}$, resp. $\mathbb{F}_{2^8}$ listed in [23]. In the case of $n = 7$, we obtain $m_F = 63$ for all functions F giving a lower bound of 22 on the minimum distance to the closest

APN function. In the case of $n = 8$, m_F takes values $69, 75, 81, 87, 93, 99, 105$, so that the lower bound on the Hamming distance is always at least 24. We thus have a lower bound on the distance to the closest APN function for all known APN functions in dimensions $n = 7$ and $n = 8$. The multiset Π_F takes 6665 distinct values for these 8157 functions. A detailed summary of these computational results can be found online at *https://boolean.h.uib.no/mediawiki/*.

The next-to-last column of the table gives the minimum distance from a given function F to the nearest APN function; this can be computed simply as $\lceil m_F/3 \rceil + 1$ but is explicitly given here for convenience. The last column gives the minimum distance to the closest APN function that can be obtained from F by shifting some number of points by the same shift, as described in Section V. These values can be computed efficiently and effectively provide an upper bound on the minimum distance to the closest APN function.

For the case of $n = 5$, we use the filtering methods described above to compute the exact minimum distance to the closest APN function for a representative from each EA-equivalence class; APN functions have been completely classified in this dimension up to EA-equivalence [3]. This shows, in particular, that the single shift distance can, in general, be larger than the minimum distance to an APN function, and that this minimum distance is not preserved under CCZ-equivalence. The results are given in Table III. In the column labeled "Number of shifts", we given the number of distinct shifts that lead to an APN function; e.g. for BCP-2, either all points from U must be assigned the same shift, or they should be divided into four pairs, with each pair of points shifted by the same value. The last column of Table III gives the CCZ-class to which the function obtained by shifting points from F belongs. The functions labeled "BCP-1" and "BCP-2" are constructed in [8], and constitute the earliest example of an APN function EA-inequivalent to a power function.

V. Single shift

A significantly simplified construction involves shifting all the points $u_1, u_2, \ldots, u_K$ by the same value $v \in \mathbb{F}_{2^n}^*$. In this case, characterizing the APN-ness of

$$G(x) = F(x) + v\left(\sum_{i\in[K]} 1_{u_i}(x)\right)$$

becomes easier regardless of whether F is assumed to be APN or not.

For a given triple $(a, x, y) \in \mathbb{F}_{2^n}^3$, let us denote by $N_{a,x,y}$ the parity of the number of elements from $\{x, y, a + x, a + y\}$ that are in U, i.e.

$$N_{a,x,y} = |\{x, y, a + x, a + y\} \cap U| \mod 2.$$

Observe that a differential equation of the form $D_aG(x) = b$ for given $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$ can have more than two solutions if and only if

$$D_aF(x) + D_aF(y) = vN_{a,x,y}$$

for $x, y \in \mathbb{F}_{2^n}$ with $x + y \neq a$.

Given some initial function F over $\mathbb{F}_{2^n}$, the following procedure can then be used to find all APN functions G that can be obtained from F by shifting some set of points U by a given shift $v \in \mathbb{F}_{2^n}^*$:

TABLE II
VALUES OF m_F, LOWER BOUNDS ON $d(F, G)$ AND MINIMUM SINGLE SHIFT DISTANCE FOR ANY $G \neq F$ APN FOR $F(x)$ FROM [16]

Dimension	F	m_F	Lower bound on minimum distance	Minimum single-shift distance
4	x^3	3	2	2
5	x^3	15	6	8
5	x^5	15	6	8
5	x^{15}	9	4	10
6	1.1	27	10	16
6	1.2	27	10	16
6	2.1	15	6	16
6	2.2	27	10	16
6	2.3	27	10	16
6	2.4	15	6	8
6	2.5	15	6	16
6	2.6	15	6	8
6	2.7	15	6	8
6	2.8	15	6	8
6	2.9	21	8	16
6	2.10	21	8	8
6	2.11	15	6	16
6	2.12	15	6	8
7	7.1	54	19	?
7	all others	63	22	?
8	1.1	111	38	?
8	1.2	111	38	?
8	1.3	111	38	?
8	1.4	111	38	?
8	1.5	111	38	?
8	1.6	111	38	?
8	1.7	111	38	?
8	1.8	111	38	?
8	1.9	111	38	?
8	1.10	111	38	?
8	1.11	111	38	?
8	1.12	111	38	?
8	1.13	111	38	?
8	1.14	99	34	?
8	1.15	111	38	?
8	1.16	111	38	?
8	1.17	111	38	?
8	2.1	111	38	?
8	3.1	111	38	?
8	4.1	99	34	?
8	5.1	105	36	?
8	6.1	105	36	?
8	7.1	111	38	?

TABLE III
DISTANCE BETWEEN APN EA-REPRESENTATIVES FROM $\mathbb{F}_{2^5}$ AND CLOSEST APN FUNCTION

F	Lower bound	Actual distance	Single-shift distance	Number of shifts	CCZ-class
x^3	6	8	8	1	x^5
x^5	6	8	8	1	x^3
BCP-2	6	8	8	1,4	x^3
BCP-1	6	8	8	1,4	x^5
x^7	6	10	12	10	x^7
x^{11}	6	10	12	10	x^{11}
x^{15}	4	10	10	10	x^{15}

1) assign a Boolean variable $u_x \in \mathbb{F}_2$ to every field element $x \in \mathbb{F}_{2^n}$; the value of u_x will indicate whether x is in U or not;
2) find all tuples $(x, y, a) \in \mathbb{F}_{2^n}^3$ for which $D_aF(x) + D_aF(y) = v$ with $a \neq 0, x \neq y, a + y$;
3) for every such tuple, consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 0$;
4) find also all tuples $(x, y, a) \in \mathbb{F}_{2^n}^3$ for which $D_aF(x) + D_aF(y) = 0$ with $a \neq 0, x \neq y, a + y$;
5) for every such tuple, consider the equation $u_x + u_y + u_{a+x} + u_{a+y} = 1$;
6) solve the system of all such equations; this can be done by e.g. constructing an $e \times (2^n)$ matrix over $\mathbb{F}_2$, where e is the number of tuples of both types considered above;
7) the solutions to this system now correspond to precisely those sets $U \subseteq \mathbb{F}_{2^n}$ for which G is APN.

Note that in the case that F is APN, no equations of the type $D_aF(x) + D_aF(y) = 0$ exist for $x + y \neq a$ so that steps four and five above can be skipped.

This method is quite useful in practice, as it can be applied rather efficiently (the main part of the computations consists of finding all tuples (x, y, a) satisfying one of the conditions given above) and since it can be applied to an arbitrary function F (not only APN). Note that the same method can be obtained from Theorem 9 in [16] for the case that F is APN, where it is presented as a special case of the so-called "switching construction". A construction in which a Boolean function is added to an (n, n)-function is also studied in [7].

VI. Conclusion

We examined a construction in which a given vectorial Boolean function F is modified at K different points in order to obtain a new function G. We introduced a new CCZ-invariant for APN functions Π_F which to the best of our knowledge is the first such new invariant for the last ten years. We computed the values of Π_F for all known APN functions over $\mathbb{F}_{2^n}$ for $n \leq 8$. We obtained sufficient and necessary conditions for G to be APN, from which we derived an efficient procedure for searching for APN functions at a given distance from F as well as a lower bound on the distance to the closest APN function in terms of Π_F and m_F. Based on this, we computed a lower bound on the Hamming distance to the closest APN function for all APN functions over $\mathbb{F}_{2^n}$ for $n \leq 5$, and for all known APN functions over $\mathbb{F}_{2^n}$ for $n \leq 8$. We also gave a formula expressing this lower bound for the Gold function x^3 over $\mathbb{F}_{2^n}$ for any dimension n. An additional method for characterizing the APN-ness of G was given for the special case when all the shifts $v_1, v_2, \ldots, v_K$ are identical.

There is a lot of room for future work, and a number of questions and research directions remain open. The methods used here for the characterizations of APN functions may be applied to other classes such as differentially 4-uniform functions. A theoretical lower bound on the value m_F would be valuable, as well as additional results related to its computation. Finding relations between m_F and other properties of F may be very important, and applying the filtering procedure in practice may lead to new examples of APN functions.

ACKNOWLEDGEMENTS

The research presented in this paper was supported by the Trond Mohn Foundation, and by the Research Council of Norway under contract 247742/O70.

REFERENCES

[1] Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. On Almost Perfect Nonlinear Functions Over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

[2] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 4(1):3–72, Jan 1991.

[3] Marcus Brinkmann and Gregor Leander. On the Classification of APN Functions up to Dimension Five. *Designs, Codes and Cryptography*, 49:273–288, 2008.

[4] Lilya Budaghyan. *The Equivalence of Almost Bent and Almost Perfect Nonlinear Functions and Their Generalizations*. PhD thesis, Otto-von-Guericke-University Magdeburg, 2005.

[5] Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Nikolay Kaleyski. Changing Points in APN Functions. The 3rd International Workshop on Boolean Functions and their Applications (BFA), June 17-22, Loen, Norway.

[6] Lilya Budaghyan, Claude Carlet, Tor Helleseth, Nian Li, and Bo Sun. On Upper Bounds for Algebraic Degrees of APN Functions. *IEEE Transactions on Information Theory*, 64(6):4399–4411, 2018.

[7] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing New APN Functions from Known Ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[8] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[9] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Binary m-sequences with three-valued crosscorrelation: a proof of welch's conjecture. *IEEE Transactions on Information Theory*, 46(1):4–8, 2000.

[10] Claude Carlet. Vectorial Boolean Functions for Cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

[11] Claude Carlet. Boolean and Vectorial Plateaued Functions and APN Functions. *IEEE Transactions on Information Theory*, 61(11):6272–6289, 2015.

[12] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[13] Leonard Carlitz. Explicit Evaluation of Certain Exponential Sums. *Mathematica Scandinavica*, 44:5–16, 1979.

[14] Florent Chabaud and Serge Vaudenay. Links between Differential and Linear Cryptanalysis. In *Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT 94*, volume 950, pages 356–365, 1994.

[15] Pascale Charpin, Sihem Mesnager, and Sumanta Sarkar. Involutions over the Galois field $\mathbb{F}_{2^n}$. *IEEE Transactions on Information Theory*, 62(4):2266–2276, 2016.

[16] Yves Edel and Alexander Pott. A New Almost Perfect Nonlinear Function which is not Quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.

[17] Nikolay S. Kaleyski. Changing APN Functions at Two Points. *Cryptography and Communications*, Apr 2019.

[18] Yongqiang Li, Mingsheng Wang, and Yuyin Yu. Constructing Differentially 4-uniform Permutations over $GF(2^{2k})$ from the Inverse Function Revisited. *IACR Cryptology ePrint Archive*, 2013:731, 2013.

[19] Kaisa Nyberg. Perfect nonlinear s-boxes. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 378–386, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[20] Kaisa Nyberg. Differentially Uniform Mappings for Cryptography. *Lecture Notes in Computer Science*, 765:55–64, 1994.

[21] Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In *International Workshop on Fast Software Encryption*, pages 111–130, 1994.

[22] Lawrence C. Washington and Wade Trappe. *Introduction to Cryptography with Coding Theory*. Prentice Hall, 2002.

[23] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A Matrix Approach for Constructing Quadratic APN Functions.

[24] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. Constructing Differentially 4 Uniform Permutations from Known Ones. *Chinese Journal of Electronics*, 22(3):495–499, 2013.

Paper III

Classification of quadratic APN functions with coefficients in GF(2) for dimensions up to 9

Yuyin Yu, Nikolay S. Kaleyski, Lilya Budaghyan, Yongqiang Li
Finite Fields and Their Applications, **vol. 68, 101733** (2020)

Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9

Yuyin Yu[1], Nikolay Kaleyski[2], Lilya Budaghyan[2], and Yongqiang Li[3]

[1]*College of Mathematics and Information Science, Guangzhou University, Guangzhou*
[2]*Department of informatics, University of Bergen*
[3]*State Key Laboratory of Information Security,Institute of Information Engineering, Chinese Academy of Sciences*

Abstract

Almost perfect nonlinear (APN) and almost bent (AB) functions are integral components of modern block ciphers and play a fundamental role in symmetric cryptography. In this paper, we describe a procedure for searching for quadratic APN functions with coefficients in $\mathbb{F}_2$ over the finite field $\mathbb{F}_{2^n}$ and apply this procedure to classify all such functions over $\mathbb{F}_{2^n}$ with $n \leq 9$. We discover two new APN functions (which are also AB) over $\mathbb{F}_{2^9}$ that are CCZ-inequivalent to any known APN function over this field. We also verify that there are no quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ with $6 \leq n \leq 8$ other than the currently known ones.

I. Introduction

A vectorial Boolean (n, m)-function is a function between the vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ over the finite field $\mathbb{F}_2 = \{0, 1\}$ for some two positive integers m, n. Vectorial Boolean functions play a crucial role in the design of modern block ciphers (where they are referred to as "S-boxes" or "substitution boxes"), in which they typically represent the only nonlinear part of the encryption. For this reason, the resistance of a block cipher to cryptanalytic attacks directly depends on the properties of its substitution boxes. Vectorial Boolean (n, n)-functions are of particular importance in cryptography since one typically wishes to substitute a sequence of bits for another sequence of the same length. In this case, the vector space $\mathbb{F}_2^n$ is usually identified with the finite field $\mathbb{F}_{2^n}$, and (n, n)-functions are expressed as polynomials over $\mathbb{F}_{2^n}$.

Among the most powerful cryptanalytic attacks known to date are the so-called "differential cryptanalysis" introduced by Biham and Shamir [1], and the "linear cryptanalysis" introduced by Matsui [26]. Almost perfect nonlinear (APN) functions were introduced by Nyberg [27] as the class of (n, n)-functions offering optimal resistance to differential cryptanalysis, while almost bent (AB) functions are the ones that are optimal against linear cryptanalysis [22]. Finding new examples and constructions of APN and AB functions is very important not only for the purpose of constructing new block ciphers in cryptography, but also for other areas of computer science and discrete mathematics (such as combinatorics, sequence design, coding theory, design theory) in which some APN functions correspond to optimal objects. Furthermore, finding new APN and AB functions is a difficult task, especially for large dimensions n: indeed, to date only six infinite monomial APN families and twelve infinite polynomial APN families have been discovered[1], despite ongoing research on the topic since the early 90's. Among these, there are four infinite families of AB monomials and eight infinite families of AB polynomials.

[1]Tables of the known infinite monomial and polynomial families can be found at https://boolean.h.uib.no/mediawiki/

The case of quadratic APN functions is more tractable than the general one, which is evinced by the fact that all the infinite polynomial families constructed so far are quadratic, and only one known sporadic example of a non-quadratic (up to CCZ-equivalence) APN function (which is defined over $\mathbb{F}_{2^6}$) is known [24]. Nevertheless, quadratic APN functions are an important ongoing direction of research: in 2010, Dillon et al. discovered an APN permutation in dimension $n = 6$, thereby disproving the conjecture that APN functions over fields of even dimension could never be bijective [5]. Despite Dillon's permutation not being a quadratic APN function per se, it was constructed by traversing the CCZ-equivalence class of a quadratic function. The question of the existence of other APN permutations for even n remains open, and investigating new instances of quadratic APN functions is a promising way to approach it.

A lot of research has been done on the topic of APN functions in recent years. An infinite construction of APN binomials inequivalent to power functions is given in [13], disproving the long-standing conjecture that all infinite APN families must be monomials. Further infinite constructions of APN and AB functions are proposed in [2], [8], [9], [10], [11], [12], [13], [14], [15], [30], [33]. Previously, a classification of all APN functions over $\mathbb{F}_{2^n}$ for n up to 5 was given in [3], with classification for dimensions n higher than 5 remaining incomplete at the time of writing. In the case of $n = 6$, classification is complete for the particular cases of quadratic and cubic functions: in [4], 13 CCZ-inequivalent quadratic functions over $\mathbb{F}_{2^6}$ are listed, and it is shown that these encompass all quadratic CCZ-classes over $\mathbb{F}_{2^6}$ in [23]; as for the case of cubic APN functions, their classification is given in [25]. Furthermore, a study of the EA-equivalence classes corresponding to all known APN functions over $\mathbb{F}_{2^6}$ is presented in [17], [18]. More background on APN functions and their construction can be found e.g. in [7] or [20].

Using a matrix construction, a large number of CCZ-inequivalent APN functions were found over $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ [32], bringing the total number of known APN functions over these fields to 490 and 8180, respectively. To the best of our knowledge, no systematic search of this kind has been performed over $\mathbb{F}_{2^n}$ for any dimension $n \geq 9$. The main reason for this is that the complexity of a computer search (which increases exponentially with the dimension n) becomes too demanding over dimensions of this magnitude.

Results similar to those in [32] have been independently obtained in [31], wherein 285 and 10 previously unknown quadratic APN functions are obtained over $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$, respectively. Another similar approach based on the concept of antidifferentiation is developed in and [28] and [29].

In this paper, we focus on the particular case of quadratic APN functions over $\mathbb{F}_{2^n}$ with $n \leq 9$ and with coefficients in $\mathbb{F}_2$. We employ a specialization of the matrix method presented in [32] to conduct our search, and obtain a complete classification (up to CCZ-equivalence) of these functions over $\mathbb{F}_{2^9}$. In particular, we discover two instances of APN functions over $\mathbb{F}_{2^9}$ that are inequivalent to any known APN function over this field. For dimensions n with $6 \leq n \leq 8$, we show that there are no quadratic APN functions with coefficients in $\mathbb{F}_2$ other than the already known ones.

In our classification, we list a shortest possible representative from each discovered CCZ-equivalence class. In dimensions n up to 6, these shortest representatives are all

monomials. In dimensions $n \in \{7, 8\}$, the longest representative has 6 terms, while in dimension $n = 9$, the longest representative has 9 terms. This raises the question of whether any quadratic APN function over $\mathbb{F}_{2^n}$ represented by a polynomial with coefficients in $\mathbb{F}_2$ is CCZ-equivalent to a function that can be represented by a polynomial with coefficients in $\mathbb{F}_2$ with at most n terms.

Furthermore, although all of the functions that we find over $\mathbb{F}_{2^8}$ are equivalent to representatives from [24], we find shorter representatives for two of these functions, viz. $x^3 + x^6 + x^{72}$ for $x^3 + \mathrm{Tr}(x^9)$ and $x^3 + x^6 + x^{144}$ for $x^9 + \mathrm{Tr}(x^3)$. Thus, to the best of our knowledge, our classification lists the shortest known representatives for these CCZ-equivalence classes.

II. Preliminaries

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, by $\mathbb{F}_{2^n}^\star$ its multiplicative group, and by $\mathbb{F}_{2^n}[x]$ the univariate polynomial ring over $\mathbb{F}_{2^n}$ in indeterminate x. The trace function $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ for $x \in \mathbb{F}_{2^n}$. By $\mathbb{F}_{2^n}^{m\times k}$, we denote the set of m-by-k matrices with entries in $\mathbb{F}_{2^n}$, and if $M \in \mathbb{F}_{2^n}^{m\times k}$, we denote by $M[i, j]$ the entry in the i-th row and j-th column of M, for $0 \le i \le m-1$, $0 \le j \le k-1$. By Submatrix(M, i, j, p, q), we will denote the $p \times q$ submatrix of M rooted at (i, j), for $0 \le i \le m-1$, $0 \le j \le k-1$, $1 \le p \le m-i$, $1 \le q \le k-1$. Note that we index matrix rows and columns from zero.

We will use the following conventions and notation throughout the paper:

(i) When working over $\mathbb{F}_{2^n}$, integers indexing i.a. basis elements and matrix rows and columns will be considered modulo n. For instance, a normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ satisfies $\alpha_{i+1} = \alpha_i^2$ for $0 \le i \le n-1$; this means that $\alpha_{i+1} = \alpha_i^2$ for $0 \le i \le n-2$, and $\alpha_0 = \alpha_{n-1}^2$.

(ii) Suppose $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, so that $\alpha_{i+1} = \alpha_i^2$ for $0 \le i \le n-1$, and suppose $\{\theta_0, \theta_1, \ldots, \theta_{n-1}\}$ is its dual basis, i.e. $\mathrm{Tr}(\alpha_i\theta_j) = 0$ for $i \ne j$ and $\mathrm{Tr}(\alpha_i\theta_i) = 1$ for $0 \le i, j \le n-1$. Note that $\{\theta_0, \theta_1, \ldots, \theta_{n-1}\}$ is also a normal basis, so that without loss of generality, we can assume $\theta_{i+1} = \theta_i^2$ for $0 \le i \le n-1$.
Let $M_\alpha \in \mathbb{F}_{2^n}^{n\times n}$ and $M_\theta \in \mathbb{F}_{2^n}^{n\times n}$ be such that

$$M_\alpha[i, u] = \alpha_u^{2^i} \text{ and } M_\theta[i, u] = \theta_u^{2^i} \tag{1}$$

for $0 \le u, i \le n-1$. Then $M_\alpha^t M_\theta[u, j] = \mathrm{Tr}(\alpha_u\theta_j)$ for $0 \le u, j \le n-1$, so that $M_\alpha^t M_\theta = I_n$, where I_n is the identity matrix of order n. Thus $M_\theta^{-1} = M_\alpha^t$, where M_α^t is the transpose of M_α.

(iii) Let $B \in \mathbb{F}_{2^n}^m$ be a vector $B = (\eta_0, \eta_1, \cdots \eta_{m-1})$ where $\eta_i \in \mathbb{F}_{2^n}$ for $0 \le i \le m-1$. Then $\mathrm{Span}(B) = \mathrm{Span}(\eta_0, \eta_1, \cdots, \eta_{m-1})$ is the subspace spanned by $\{\eta_0, \eta_1, \cdots, \eta_{m-1}\}$ over $\mathbb{F}_2$. The dimension of this subspace is denoted by $\mathrm{Rank}(B) = \mathrm{Rank}(\eta_0, \eta_1, \cdots, \eta_{m-1})$, and is referred to as the rank of B over $\mathbb{F}_2$. If $\eta_i = \sum_{j=0}^{n-1} \lambda_{i,j}\alpha_j$ for $0 \le j \le m-1$, with $\lambda_{i,j} \in \mathbb{F}_2$ for $0 \le i, j \le n-1$, and we define an m-by-n matrix $\Lambda \in \mathbb{F}_2^{m\times n}$ by $\Lambda[i, j] = \lambda_{i,j}$, then the rank of B is equal to the rank of Λ.

An (n, n)-function, or vectorial Boolean function, is any mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ from the field with 2^n elements to itself. Any (n, n)-function can be represented as a polynomial $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ with $a_i \in \mathbb{F}_{2^n}$; this representation is referred

to as the univariate representation of F, and is unique. The binary weight $wt_2(i)$ of a positive integer i is the number of ones in its binary notation; equivalently, if we write i as a sum of powers of two, so that $i = \sum_{j=0}^{k} b_j 2^j$ for $b_j \in \{0, 1\}$, then its binary weight is $wt_2(x) = \sum_{i=0}^{k} b_j$, with the sum taken over the integers. The largest binary weight of an exponent i with non-zero coefficient a_i in the univariate representation of an (n, n)-function F is called the algebraic degree of F and is denoted by $\deg(F)$. A function of algebraic degree 1, resp. 2, resp. 3 is called affine, resp. quadratic, resp. cubic. An affine F satisfying $F(0) = 0$ is called linear.

In the following, we concentrate on the case of homogeneous quadratic functions, which can be written as

$$F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$$

for $a_{i,j} \in \mathbb{F}_{2^n}$, i.e. quadratic functions with no linear terms in their univariate representation.

Definition 1. A mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **differentially $\delta(F)$- uniform** if

$$\delta(F) = \max_{a \in \mathbb{F}_{2^n}^{\star}, b \in \mathbb{F}_{2^n}} \#\Delta_F(a, b),$$

where $\Delta_F(a, b) = \{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}$, and $\#\Delta_F(a, b)$ is the cardinality of $\Delta_F(a, b)$. If $\delta(F) = 2$, F is called **almost perfect nonlinear (APN)**.

Definition 2. Let F and F' be two functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We say that F and F' are **EA-equivalent** (Extended affine equivalent) if we can write F' as

$$F'(x) = A_1(F(A_2(x))) + A_3(x),$$

where A_1 and A_2 are affine permutations of $\mathbb{F}_{2^n}$, and A_3 is an affine function on $\mathbb{F}_{2^n}$.

We say that F and F' are **CCZ-equivalent** (Carlet-Charpin-Zinoviev equivalent) [21], if there exists an affine permutation which maps G_F onto $G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F, and $G_{F'}$ is the graph of F'.

EA-equivalence is a special case of CCZ-equivalence, and the latter, which also includes taking inverses of permutations as a particular case, is known to be strictly more general that the combination of both of the aforementioned transformations [6], [8], [19]. An important property of CCZ-equivalence is that it leaves the differential uniformity $\delta(F)$ invariant, i.e. if two (n, n)-functions F and F' are CCZ-equivalent, then $\delta(F) = \delta(F')$. For this reason, APN functions are typically classified up to CCZ-equivalence, and this makes the classification process somewhat easier despite the large amount of (n, n)-functions.

Computationally testing whether two (n, n)-functions are CCZ-equivalent is typically done by associating a linear code to each function and then testing whether the resulting two codes are isomorphic [4]. To the best of our knowledge, this test is reliable for finite fields $\mathbb{F}_{2^n}$ with $n \le 9$, but sometimes fails for higher values of n due to a lack of computational resources. The Γ-rank, Δ-rank, and the order of the multiplier group are CCZ-invariants introduced in[24]. In our search, we use the code isomorphism test to partition the APN functions that we find into CCZ-equivalence

classes, and use the Γ-ranks of the two new functions that we find as proof that they lie outside the bounds of all previously known APN functions over $\mathbb{F}_{2^9}$.

We recall a couple of useful notions from [32].

Definition 3. Let $H \in \mathbb{F}_{2^n}^{m\times k}$ $(m, k \leq n)$. We say that H is **proper** if every nonzero linear combination over $\mathbb{F}_2$ of the m rows of H has rank at least $k-1$.

Definition 4. Let H be an $n \times n$ matrix defined on $\mathbb{F}_{2^n}$. Then H is called a **QAM** (quadratic APN matrix) if:
i) H is symmetric and the elements in its main diagonal are all zeros;
ii) H is proper, i.e. every nonzero linear combination of the n rows (or, equivalently, columns, due to H being symmetric) of H has rank $n-1$.

III. Construction of quadratic APN functions

A. Correspondence between quadratic functions with coefficients in $\mathbb{F}_2$ and a class of matrices

As shown in [32], there is a one-to-one correspondence between quadratic APN functions and QAM's. The precise statement is given in Theorem 1 below.

Theorem 1. [32] Let $F(x) = \sum_{0\leq t<i\leq n-1} c_{i,t}x^{2^i+2^t} \in \mathbb{F}_{2^n}[x]$ be a homogeneous quadratic (n, n)-function and let $C_F \in \mathbb{F}_{2^n}^{n\times n}$ be defined by $C_F[i, t] = C_F[t, i] = c_{i,t}$, $C_F[i, i] = 0$ for $0 \leq i < t \leq n-1$. Let $H = M_\alpha^t H M_\alpha$ where M_α is as defined in (1). Then $\delta(F) = 2^k$ if and only if any non-zero linear combination over $\mathbb{F}_2$ of the n rows of H has rank at least $n-k$. In particular, F is APN if and only if H is a QAM.

The following theorem addresses the specific case when all coefficients of the function are in $\mathbb{F}_2$.

Theorem 2. Let $F(x) = \sum_{0\leq t<i\leq n-1} c_{i,t}x^{2^i+2^t}$ be a quadratic homogeneous (n, n)-function. Define an $n \times n$ matrix C_F by $C_F[t, i] = C_F[i, t] = c_{i,t}$ for $0 \leq t < i \leq n-1$ and $C_F[i, i] = 0$ for $0 \leq i \leq n-1$. Finally, take

$$H = M_\alpha^t C_F M_\alpha.$$

Then

$$H[u+1, v+1] = H[u, v]^2 \tag{2}$$

(with the indices taken modulo n) for $0 \leq v, u \leq n-1$ if and only if $c_{i,t} \in \mathbb{F}_2$ for $0 \leq t < i \leq n-1$.

Proof. ($\Leftarrow$) Suppose $c_{i,t} \in \mathbb{F}_2$ for $0 \leq t < i \leq n-1$. From $H = M_\alpha^t C_F M_\alpha$ we have, for all $0 \leq v, u \leq n-1$,

$$H[u, v] = \sum_{0\leq t<i\leq n-1} c_{it}(\alpha_u^{2^i}\alpha_v^{2^t} + \alpha_u^{2^t}\alpha_v^{2^i}).$$

It is easy to see that $H[u+1, v+1] = H[u, v]^2$ for $0 \leq v, u \leq n-1$, since $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is a normal basis such that $\alpha_{i+1} = \alpha_i^2$ for $0 \leq i \leq n-1$. Note that in the case $i = n-1$, this means that $\alpha_{n-1}^2 = \alpha_0$.

($\Rightarrow$) Suppose now that H satisfies (2). From $H = M_\alpha^t C_F M_\alpha$, we have $C_F = (M_\alpha^t)^{-1} H M_\alpha^{-1} = M_\theta H M_\theta^t$, which means that, for all $0 \leq v, u \leq n-1$,

$$c_{i,t} = C_F[i,t] = \sum_{0 \leq u,v \leq n-1} (\theta_u^{2^i} \theta_v^{2^t}) H[u,v].$$

Since $\theta_{i+1} = \theta_i^2$ for $0 \leq i \leq n-1$, if $H[u+1, v+1] = H[u,v]^2$ for $0 \leq v, u \leq n-1$, we have

$$c_{i,t} = \sum_{0 \leq k \leq n-1} Tr(\theta_0^{2^i} \theta_{0+k}^{2^t} H[0, 0+k]),$$

which clearly belongs to $\mathbb{F}_2$. □

By Theorem 2, any matrix H representing a quadratic APN function with coefficients in $\mathbb{F}_2$ satisfies (2); this significantly reduces the search space, and allows an exhaustive search to be performed in practice for higher dimensions.

B. Conditions on QAM's

In the following subsection, we describe how we conduct an exhaustive search over all $n \times n$ QAM's corresponding to (n,n)-functions represented by univariate polynomials with coefficients in $\mathbb{F}_2$. The condition $H[u+1, v+1] = H[u,v]^2$ greatly reduces the search space, and, in fact, implies that the values of only $\lfloor n/2 \rfloor$ entries of the matrix have to be guessed before the values of the remaining entries can be uniquely reconstructed. Depending on the parity of n, the situation is slightly different, and so, in the following we look at two concrete examples, one for $n = 5$, and one for $n = 6$.

Example 1. In the case of $n = 5$, suppose that H is a symmetric 5×5 matrix with zero diagonal and such that $H[u+1, v+1] = H[u,v]^2$ for all $0 \leq u, v \leq 4$. If we denote the entries of this matrix at $H[0,1]$ and $H[0,2]$ by a and b, respectively, we can readily see that H must take the form

$$H = \begin{pmatrix} 0 & a & b & b^8 & a^{16} \\ a & 0 & a^2 & b^2 & b^{16} \\ b & a^2 & 0 & a^4 & b^4 \\ b^8 & b^2 & a^4 & 0 & a^8 \\ a^{16} & b^{16} & b^4 & a^8 & 0 \end{pmatrix}.$$

Thus, knowing the values of only two entries of the matrix completely determines the rest. For comparison, without the condition $H[u+1, v+1] = H[u,v]^2$, we would have to guess $1+2+3+4 = 10$ entries of the matrix.

In the case of $n = 6$, we once again label the entries of a 6×6 matrix H at $H[0,1]$, $H[0,2]$, and $H[0,3]$ by a, b, and c, respectively. The matrix then takes the form

$$H = \begin{pmatrix} 0 & a & b & c & b^{16} & a^{32} \\ a & 0 & a^2 & b^2 & c^2 & b^{32} \\ b & a^2 & 0 & a^4 & b^4 & c^4 \\ c^8 & b^2 & a^4 & 0 & a^8 & b^8 \\ b^{16} & c^{16} & b^4 & a^8 & 0 & a^{16} \\ a^{32} & b^{32} & c^{32} & b^8 & a^{16} & 0 \end{pmatrix}.$$

Since H must be symmetric, from $H[0,3] = c$ and $H[3,0] = c^8$ we get an additional condition on the value of c, namely $c^8 = c$, i.e. $c \in \mathbb{F}_{2^3}$. In this case, only 3 entries of H need to be guessed before the entire matrix can be reconstructed. For comparison, omitting the condition $H[u+1, v+1] = H[u,v]^2$ would require us to guess $1+2+3+4+5 = 15$ entries of the matrix.

The above principles can be generalized as follows.

Proposition 1. Let n be a positive integer and H be a symmetric $n \times n$ matrix over $\mathbb{F}_{2^n}$ with zeros on its main diagonal such that $H[u+1, v+1] = H[u,v]^2$ for all $0 \leq u, v \leq n-1$, with the indices being taken modulo n. Then:

1) $H[i,j] = H[0, j-i]^{2^i}$ for any $0 \leq i, j \leq n-1$;
2) $H[0,j] = H[0,-j]^{2^j}$ for any $0 \leq j \leq n-1$;
3) if n is even, then $H[0, n/2] \in \mathbb{F}_{2^{n/2}}$.

Consequently, the entries of H at $H[0,j]$ for $1 \leq j \leq \lfloor n/2 \rfloor$ uniquely determine the values of all entries of H.

Proof. The first point follows from (2) by induction on i. For the second point, we have

$$H[0, n-j+1] = H[n-j+1, 0] = H[0, j-n-1]^{2^{n-j+1}} = H[0, j-1]^{2^{n-j+1}}$$

using the symmetry of H and the first point. The third point then follows from the second one by taking $j = n/2$. □

In general (that is, without the condition from Theorem 2), a symmetric $n \times n$ matrix with zeros on the main diagonal is determined by $1 + 2 + \cdots + (n-1) = n(n-1)/2$ entries. By restricting ourselves to matrices satisfying (2), the number of entries drops to $\lfloor n/2 \rfloor$ as pointed out in Proposition 1, which decreases the number of guesses from quadratic to linear in the dimension n.

The following proposition allows us to further reduce the search complexity by discarding QAM's which a priori correspond to equivalent functions. Proposition 2 follows from Theorem 3 of [32], which asserts that if $H \in \mathbb{F}_{2^n}^{n \times n}$ is a symmetric matrix, and $H' \in \mathbb{F}_{2^n}^{n \times n}$ is defined by applying a linear permutation $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ to all elements of H, then the quadratic functions defined by H and H' are EA-equivalent. As the mapping $x \mapsto x^2$ is a linear permutation on account of $\gcd(2, 2^n - 1) = 1$, the proposition is an immediate consequence of this theorem. The restriction to linear permutations of the form $x \mapsto x^{2^k}$ comes from the fact that the property (2) remains invariant under such permutations.

Proposition 2. Suppose $F_1 \in \mathbb{F}_{2^n}[x]$ is a homogeneous quadratic APN function with coefficients in $\mathbb{F}_2$, and H is its corresponding QAM. Let H' be the matrix defined by $H'[i,j] = H[i,j]^2$ for $0 \leq i, j < n$. Then H' is also a QAM, and its corresponding function $F_2 \in \mathbb{F}_2[x]$ is EA-equivalent to F_1.

Following the statement of Proposition 2, recall that we will two elements $a, b \in \mathbb{F}_{2^n}$ *conjugates* if there is a non-negative integer k such that $a = b^{2^k}$. The relation "conjugate to" is an equivalence relation which induces a partition of $\mathbb{F}_{2^n}$ into conjugacy classes.

To summarize, by Proposition 2, only a single representative from each conjugacy class has to be considered for the first entry that we guess, which further reduces the number of possibilities that have to be considered. Furthermore, in the case of even n, the set of possible values for the last entry that we guess can be restricted to the subfield $\mathbb{F}_{2^{n/2}}$.

The results from Theorems 1, 2 and Proposition 2 are combined into an efficient procedure for searching for quadratic APN functions over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^n}$ in Algorithm 1.

C. The algorithm

The algorithm is essentially an exhaustive search which traverses all possible $n \times n$ QAM's by starting with the $n \times n$ zero matrix and iteratively assigning concrete values to its entries. Condition (2) greatly reduces the search space.

The *Search(j, H)* procedure implements the basic logic of the exhaustive search. An invocation of *Search(j, H)* attempts to assign a value to the entry of the matrix in the first row and j-th column, i.e. $H[0, j]$. In order to achieve this, it first invokes the *GetPossibleValues(j, H)* function which returns a list W of all possible values that $H[0, j]$ can take; using Proposition 2, a number of impossible values are filtered out by *GetPossibleValues*, which further reduces the complexity of the search. For all possible values $w \in W$, the *Search* procedure attempts to assign w to $H[0, j]$. This is performed by calling the *Assign(j, H, w)* procedure, which assigns w to $H[0, j]$ and derives the values of all other entries of the matrix that follow from $H[0, j]$ by symmetry and by (2). If $j = \lfloor n/2 \rfloor$ and a value w is assigned to $H[0, j]$, then all entries in the matrix are already known, and it remains to check whether the obtained matrix is a QAM. If $j < m$, then *Search($j + 1, H$)* is called recursively to assign a value to the next variable.

The *GetPossibleValues(j, H)* function distinguishes between two cases. Since a QAM must contain zeros on the main diagonal, $H[0, 1]$ is the first variable to be assigned a value. By Proposition 2, it suffices to consider a single representative from every conjugacy class in $\mathbb{F}_{2^n}$; this is precisely what the function *GetConjugacyClass-Representatives(n)* returns.

When $j > 2$, we can no longer restrict ourselves to a single representative from each conjugacy class, but can reduce the range of possible values for $H[0, j]$ in other ways. Recall that by the definition of a QAM, every nonzero linear combination of rows must have rank $n - 1$. Since every row contains a zero element on the main diagonal, this is equivalent to saying that the elements of each row that do not lie on the main diagonal must be linearly independent. For this reason, the subspace S spanned by the entries in the first row that have already been assigned is removed from the list E of possible values. After S is computed, its size is used to test whether the known elements on the first row are linearly independent; note that while the element at $H[0, j]$ is always selected so that it is linearly independent on the previously assigned elements, the same is not necessarily true for the value of $H[0, -j]$ derived by Proposition 1, and this necessitates the test for linear independence. If the test fails, *GetPossibleValues* returns an empty set for the possible values of $H[0, j]$, which immediately forces the search procedure to backtrack to $H[0, j - 1]$. By Corollary 2 of [32], every submatrix of a QAM must be proper. This condition is also exploited

by *GetPossibleValues* in order to reduce the set E of possible values; once all entries $H[0,j]$ for $1 \leq j \leq j-1$ are known, the submatrix of H consisting of the first j rows and $j+1$ columns is fully determined. All values of $H[0,j]$ for which this submatrix is not proper are removed from E.

The entire search procedure begins by initializing H to an $n \times n$ zero matrix and invoking *Search(*$1, H$*)* to assign a value to the first variable.

As observed in Subsection III-B, the cases for an even and for an odd dimension n are slightly different. The only major difference is that the values of one of the entires of the matrix can be restricted to the subfield $\mathbb{F}_{2^{n/2}}$ when n is even. When implementing the search in practice, the distinction between the odd and even case manifests in the indexing of the variables. Algorithm 1 provides an explicit description of the search procedure in the case of odd n; this is motivated by the fact that our experiments for $n = 9$ constitute the main point of interest in our experimental output, as, to the best of our knowledge, no search of this type has been performed for dimensions greater than 8. The algorithm in the case of an even n is principally the same, keeping in mind that the value of $H[0, n/2]$ can be restricted to $\mathbb{F}_{2^{n/2}}$.

D. Summary of experimental results

Running the search for $n = 9$ on a server operating with an Intel Xeon E5 CPU at 3.5G GHz took approximately 33 days and produced a list of 21504 functions. Partitioning them into CCZ-equivalence classes by the code isomorphism test was performed by running several parallel processes on a server with an Intel Xeon E5 CPU at 2.60 GHz, and around 15-16 months. The result are the 8 CCZ-inequivalent representatives given in Table I. Computing the Γ-rank of one representative on the same server takes around an hour, while computing the Δ-rank takes approximately 3 days.

The running time for lower dimensions are negligible, and the computations were performed on a personal computer running an Intel m5-6Y54 CPU at 1.5 GHz. For $n = 8$, performing the exhaustive search took around 3 hours and produced 7616 functions, which were partitioned into CCZ-classes in 8 hours. For $n = 7$, 4410 functions were found in 2 minutes, and partitioned into CCZ-classes within 12 hours. For $4 \leq n \leq 6$, both performing the search and partitioning the resulting functions into CCZ-equivalence classes takes less than a second; the number of functions found was 4 for $n = 4$, 72 for $n = 5$, and 32 for $n = 6$.

Table I lists representatives from all CCZ-equivalence classes found by our method. Note that the search is complete, i.e. the CCZ-equivalence classes containing these representatives cover all possible homogeneous quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ with $4 \leq n \leq 9$. For each representative, we have also computed its Γ-rank, Δ-rank, and the order $|\mathcal{M}(G_F)|$ of its multiplier group [24].

In dimensions $n \leq 6$, we only find power functions as expected. In dimension $n = 7$, besides three power functions, we find 12 polynomials, among which are two binomials, six quadrinomials, four pentanomials, and one hexanomial. In dimension $n = 8$, we find two power functions and 5 polynomials, which consist of two trinomials, two pentanomials, and one hexanomial. In dimension $n = 9$, we find three power functions, along with 5 polynomials: two of them have 7 terms, one has 8 terms, and

Algorithm 1: A procedure for searching for QAM's corresponding to APN functions with coefficients in $\mathbb{F}_2$

Input: An integer $n = 2m + 1$
Output: A list of APN functions over $\mathbb{F}_{2^n}$ represented by univariate polynomials with coefficients in $\mathbb{F}_2$

```
procedure Search(n);
H ← an n × n zero matrix;
Search(1, H);
end procedure;

procedure Search(j, H);
W ← GetPossibleValues(j, H);
for w ∈ W do
    Assign(j, H, w);
    if j = m then
        if H is a QAM then
            output the polynomial corresponding to H;
    else
        Search(j + 1, H);
end procedure;

procedure Assign(j, H, w);
H[0, j] ← w;
H[j, 0] ← w;
for t ∈ 1, ··· , n − 1 do
    //Note that all indices are modulo n
    H[t, j + t] ← H[t − 1, j + t − 1]^2;
    H[j + t, t] ← H[t, j + t];
end procedure;

function GetPossibleValues(j, H);
if j = 1 then
    return GetConjugacyClassRepresentatives(n);
else
    S ← Span({H[0, i], H[0, n − i] : i ∈ 1, 2, ··· , j − 1});
    if #S < 2^(2j−2) then
        return ∅;
    E ← F*_{2^n} \ S;
    for e ∈ E do
        H[0, j] ← e;
        A ← Submatrix(H, 0, 0, j, j + 1);
        if A is not proper then
            E ← E \ {e};
    return E;
end function;
```

two have 9 terms. All the representatives given in the tables are in shortest possible presentation.

In the case of dimension $n \leq 8$, all of the representatives that we have discovered are identical or equivalent to switching class representatives from [24]. Despite this, in dimension $n = 8$, we discover very "short" and previously undocumented representatives (namely, trinomials) for two of the switching classes from [24]: $x^3+x^6+x^{72}$ is CCZ-equivalent to $x^3 + \mathrm{Tr}(x^9)$, and $x^3 + x^6 + x^{144}$ is CCZ-equivalent to $x^9 + \mathrm{Tr}(x^3)$. Both of these trinomials consist of monomials from the cyclotomic cosets of x^3 and x^9, and despite their nearly identical structure, they belong to distinct CCZ-equivalence classes. Note that the $x^3 + \mathrm{Tr}(x^9)$ belongs to the infinite family of APN functions from [14], while the second has not be generalized into any infinite family so far.

Furthermore, in dimension $n = 9$, we discover two representatives, viz.

$$s_1(x) = x^{136} + x^{132} + x^{96} + x^{80} + x^{36} + x^{34} + x^{18} + x^{17} + x^{12}$$

and

$$s_2(x) = x^{288} + x^{272} + x^{264} + x^{160} + x^{144} + x^{130} + x^{48} + x^{34}$$

which are CCZ-inequivalent to any currently known APN function over $\mathbb{F}_{2^9}$. We have verified this inequivalence in two ways: by means of the code isomorphism test, and, in addition, by computing their Γ-ranks, which turn out to be 48856 AND 48858, respectively.

We have computationally checked that these newly found functions are not CCZ-equivalent to a permutation, which took us about 40 hours computation. Thus, no quadratic APN function with coefficients in $\mathbb{F}_2$ can be CCZ-equivalent to a permutation over $\mathbb{F}_{2^n}$ with $n \leq 9$, except for the Gold APN monomials in the case of odd n.

Based on the computational results for dimensions $n \leq 9$, we can observe that any quadratic APN function F_1 with coefficients in $\mathbb{F}_2$ appears to be CCZ-equivalent to a quadratic APN function F_2 with at most n non-zero coefficients in $\mathbb{F}_{2^n}$. It would be interesting to establish whether this is true in general; if so, it would indicate the existence of a simple polynomial form for functions of this type, which would significantly simplify the complexity of searching for them.

This is closely related to the problem of finding the "simplest" possible polynomial representation for a given (n, n)-function F. A simple representation not only results in a polynomial representation that can be evaluated more efficiently in practice, but facilitates the mathematical analysis of the function in question and its properties.

Problem 1. Given an (n, n)-function F, find a function G, such that G is CCZ-equivalent to F and its univariate representation has the least possible number of non-zero coefficients.

n	ID	Functions	Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F)\rvert$
4	4.1	x^3	100	20	5760
5	5.1	x^3	330	42	4960
	5.2	x^5	330	42	4960
6	6.1	x^3	1102	94	24192
7	7.1	x^3	3610	198	113792
	7.2	x^5	3708	198	113792
	7.3	x^9	3610	198	113792
	7.4	$x^3+x^5+x^6+x^{12}+x^{33}+x^{34}$	4050	210	896
	7.5	$x^3+x^5+x^{10}+x^{33}+x^{34}$	4040	212	896
	7.6	$x^3+x^6+x^{20}$	4038	212	896
	7.7	$x^3+x^6+x^{34}+x^{40}+x^{72}$	4048	212	896
	7.8	$x^3+x^9+x^{10}+x^{66}+x^{80}$	4026	212	896
	7.9	$x^3+x^9+x^{18}+x^{66}$	4044	212	896
	7.10	$x^3+x^{12}+x^{17}+x^{33}$	4048	210	896
	7.11	$x^3+x^{12}+x^{40}+x^{72}$	4048	210	896
	7.12	$x^3+x^{17}+x^{20}+x^{34}+x^{66}$	4040	210	896
	7.13	$x^3+x^{17}+x^{33}+x^{34}$	4040	212	896
	7.14	$x^3+x^{20}+x^{34}+x^{66}$	4048	210	896
	7.15	$x^5+x^{18}+x^{34}$	4034	210	896
8	8.1	x^3	11818	420	522240
	8.2	x^9	12370	420	522240
	8.3	$x^3+x^5+x^{18}+x^{40}+x^{66}$	14044	446	2048
	8.4	$x^3+x^6+x^{72}$	13800	432	6144
	8.5	$x^3+x^6+x^{68}+x^{80}+x^{132}+x^{160}$	14040	454	2048
	8.6	$x^3+x^6+x^{144}$	13804	434	6144
	8.7	$x^3+x^{12}+x^{40}+x^{66}+x^{130}$	14046	438	2048
9	9.1	x^3	38470	872	2354688
	9.2	x^5	41494	872	2354688
	9.3	x^{17}	38470	872	2354688
	9.4	$x^{136}+x^{132}+x^{96}+x^{80}+x^{36}+x^{34}+x^{18}+x^{17}+x^{12}$	48856	940	4608
	9.5	$x^{144}+x^{130}+x^{72}+x^{65}+x^{18}+x^9+x^3$	48428	930	4608
	9.6	$x^{257}+x^{144}+x^{130}+x^{72}+x^{65}+x^{18}+x^9$	48460	944	4608
	9.7	$x^{264}+x^{160}+x^{144}+x^{132}+x^{80}+x^{72}+x^{66}+x^{40}+x^{17}$	47890	920	4608
	9.8	$x^{288}+x^{272}+x^{264}+x^{160}+x^{144}+x^{130}+x^{48}+x^{34}$	48858	940	4608

TABLE I: List of representatives from all CCZ-equivalence classes of quadratic APN functions over $\mathbb{F}_{2^n}$ represented by polynomials with coefficients in $\mathbb{F}_2$, for $4 \leq n \leq 9$

IV. Conclusion

We have described a procedure for searching for quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ by constructing matrices of a particular type, and have used this procedure to classify all such functions over the finite fields $\mathbb{F}_{2^n}$ with $n \leq 9$. We have discovered two previously unknown APN functions over $\mathbb{F}_{2^9}$, and a representation of two of the switching class representatives over $\mathbb{F}_{2^8}$ in the form of trinomials, which is simpler than their currently known representations. In the case of $6 \leq n \leq 8$, we have experimentally verified that there are no quadratic APN functions with coefficients in $\mathbb{F}_2$ other than the previously known ones.

V. Acknowledgements

The research of the second and the third authors is supported by the "Optimal Boolean functions" grant of the Trond Mohn foundation. Yuyin Yu is supported by

the NSF of China (Grant No. 61502113), and the Guangdong Provincial NSF (Grant No. 2015A030310174). Yongqiang Li is supported by the NSF of China (Grant No. 61772517).

REFERENCES

[1] Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems., Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.
[2] Bracken C, Byrne E, Markin N, McGuire G.: A few more quadratic APN functions, Cryptogr. Commun., vol. 3, no. 3, pp. 43-53, 2011.
[3] Brinkmann M., Leander G.: On the classification of APN functions up to dimension five, Designs, Codes and Cryptography,vol. 49, no.1-3, pp. 273 - 288, 2008.
[4] Browning K., Dillon J F., McQuistan M.: APN polynomials and related codes, Special volume of Journal of Combinatorics, Information and System Sciences, honoring the 75-th birthday of Prof. D.K.Ray-Chaudhuri, vol. 34, no. 1-4, pp. 135-159, 2009.
[5] Browning K, Dillon J. F., McQuistan M., Wolfe A. J.: An APN permutation in dimension six, Contemporary Mathematics, vol. 58, pp. 33-42, 2010.
[6] L. Budaghyan.: The Simplest Method for Constructing APN Polynomials EA-Inequivalent to Power Functions. Proceedings of the International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, Lecture Notes in Computer Science 4547, pp. 177-188, Madrid, Spain, June 2007.
[7] Budaghyan L.: Construction and Analysis of Cryptographic Functions. Springer Verlag, 2014.
[8] Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials, IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 1141-1152, 2006.
[9] Budaghyan L., Carlet C.: Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2354-2357, 2008.
[10] Budaghyan L., Calderini C., Carlet C., Coulter R., Villa I.: Constructing APN functions through isotopic shifts, https://eprint.iacr.org/2018/769.
[11] Budaghyan L., Carlet C., Felke P., Leander G.: An infinite class of quadratic APN functions which are not equivalent to power mappings, IEEE International Symposium on Information Theory, pp. 2637-2641, 2006.
[12] Budaghyan L., Helleseth T., Kaleyski N.: A new family of APN quadrinomials, Cryptology ePrint Archive, Report 2019/994, 2019.
[13] Budaghyan L., Carlet C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions, IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4218-4229, 2008.
[14] Budaghyan L., Carlet C., G. Leander, Constructing new APN functions from known ones, Finite Fields and Their Appl., vol. 15, no. 2, pp. 150-159, 2009.
[15] Budaghyan L., Carlet C., Leander G.: On a construction of quadratic APN functions, 2009 IEEE Information Theory Workshop, 2009.
[16] Budaghyan L, Helleseth T, Li N, Sun B. Some results on the known classes of quadratic APN functions. In International Conference on Codes, Cryptology, and Information Security 2017 Apr 10 (pp. 3-16). Springer, Cham.
[17] Budaghyan L., Calderini M., Villa I.: On equivalence between known families of quadratic APN functions, https://eprint.iacr.org/2019/793.
[18] Calderini M. On the EA-classes of known APN functions in small dimensions, https://eprint.iacr.org/2019/369.
[19] Canteaut A., Perrin L.: On CCZ-equivalence, extended-affine equivalence, and function twisting. Finite Fields and Their Applications, vol. 56, pp.209-246, 2019.
[20] Carlet C.: Vectorial Boolean functions for cryptography. Boolean models and methods in mathematics, computer science, and engineering, Encyclopedia of Mathematics and its Applications, vol. 134, pp. 398-469, 2010.
[21] Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography, 15(2):125-156, 1998.
[22] Chabaud F, Vaudenay S. Links between differential and linear cryptanalysis. InWorkshop on the Theory and Application of of Cryptographic Techniques 1994 May 9 (pp. 356-365). Springer, Berlin, Heidelberg.
[23] Edel Y.: Quadratic APN functions as subspaces of alternating bilinear forms. Proceedings of the Contact Forum Coding Theory and Cryptography III, Belgium 2011 (Vol. 2009, pp. 11-24).
[24] Yves Edel, Alexander Pott. A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications, 2009, 3 (1) : 59-81
[25] Langevin P.: Classification of APN cubics in dimension 6 over GF(2). http://langevin.univ-tln.fr/project/apn-6/apn-6.html.
[26] Matsui, M.: Linear cryptanalysis method for DES cipher. Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Springer, Berlin, Heidelberg, 1993.
[27] Nyberg, K.: Differentially uniform mappings for cryptography. Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Springer, Berlin, Heidelberg, 1993.
[28] Sălăgean, A.: Discrete antiderivatives for functions over $\mathbb{F}_p^n$. Designs, Codes and Cryptography 88.3 (2020): 471-486.
[29] Suder, V. Antiderivative functions over $\mathbb{F}_{2^n}$. Designs, Codes and Cryptography 82.1-2 (2017): 435-447.

[30] Taniguchi H.: On some quadratic APN functions, Designs, Codes and Cryptography, vol. 87, no. 9, pp 1973–1983, 2019.
[31] Weng, G., Yin T., and Guang G. On quadratic almost perfect nonlinear functions and their related algebraic object. Workshop on Coding and Cryptography, WCC. 2013.
[32] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions.Designs, Codes and Cryptography, vol. 73, no. 2, pp. 587-600, 2014.
[33] Zhou Y., Pott A.: A new family of semifields with 2 parameters. Advances in Mathematics, vol. 234, pp. 43-60, 2013.

Paper IV

A new family of APN quadrinomials

Lilya Budaghyan, Nikolay S. Kaleyski, Tor Helleseth
IEEE Transactions on Information Theory, **vol. 66, no. 11** (2020)

A new family of APN quadrinomials

Lilya Budaghyan[1], Tor Helleseth[1], and Nikolay Kaleyski[1]

[1]*Department of Informatics, University of Bergen*

Abstract

The binomial $B(x) = x^3 + \beta x^{36}$ (where β is primitive in $\mathbb{F}_{2^2}$) over $\mathbb{F}_{2^{10}}$ is the first known example of an Almost Perfect Nonlinear (APN) function that is not CCZ-equivalent to a power function, and has remained unclassified into any infinite family of APN functions since its discovery in 2006. We generalize this binomial to an infinite family of APN quadrinomials of the form $x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$ from which $B(x)$ can be obtained by setting $a = \beta$, $b = c = 0$, $i = 3$, $k = 2$. We show that for any dimension $n = 2m$ with m odd and $3 \nmid m$, setting $(a, b, c) = (\beta, \beta^2, 1)$ and $i = m-2$ or $i = (m-2)^{-1} \mod n$ yields an APN function, and verify that for $n = 10$ the quadrinomials obtained in this way for $i = m - 2$ and $i = (m-2)^{-1} \mod n$ are CCZ-inequivalent to each other, to $B(x)$, and to any other known APN function over $\mathbb{F}_{2^{10}}$.

I. Introduction

Vectorial Boolean functions, or (n, m)-functions, are mappings between the vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ for some positive integers n and m, where $\mathbb{F}_2$ is the finite field with two elements. Any such mapping can be understood as a transformation substituting a sequence of n bits (zeros and ones) with a sequence of m bits according to a given prescription, and for this reason (n, m)-functions naturally appear in different areas of computer science and engineering. In particular, (n, m)-functions are of critical importance in the field of cryptography: virtually all modern block ciphers incorporate an (n, m)-function (usually referred to as an "S-box" or "substitution box" in this context) as their only nonlinear component, and as such the security of the encryption directly depends on the properties of the (n, m)-function. Researchers have defined various properties which measure the resistance of an (n, m)-function to different kinds of cryptanalysis, including nonlinearity, differential uniformity, boomerang uniformity, algebraic degree, and so forth. The lower the differential uniformity of a function, in particular, the better its security against differential cryptanalysis [3], which is one of the most efficient attacks that can be employed against block ciphers. When $n = m$, which is the main case of our interest, the differential uniformity of any (n, n)-function is at least 2, and the (n, n)-functions meeting this bound are called almost perfect nonlinear (APN). Discovering new examples and constructions of APN functions is thus a matter of significant practical importance since they enable the design of new block ciphers. APN functions are interesting from a theoretical point of view as well, as they correspond to optimal objects within other areas of mathematics and computer science, e.g. coding theory, combinatorics, and projective geometry.

Finding new constructions of APN functions is difficult. APN functions have been known and studied since the early 90's [22] but, to date, only six infinite families of

This paper was presented in part at the Fourth International Workshop on Boolean Functions and their Applications (BFA-2019) which took place in Florence, Italy on June 16-21, 2019

TABLE I
KNOWN INFINITE FAMILIES OF APN POWER FUNCTIONS OVER $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	2^i+1	$\gcd(i,n) = 1$	2	[18], [22]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n) = 1$	$i+1$	[19], [20]
Welch	2^t+3	$n = 2t+1$	3	[13]
Niho	$2^t+2^{t/2}-1$, t even $2^t+2^{(3t+1)/2}-1$, t odd	$n = 2t+1$	$(t+2)/2$ $t+1$	[12]
Inverse	$2^{2t}-1$	$n = 2t+1$	$n-1$	[2], [22]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n = 5i$	$i+3$	[14]

TABLE II
KNOWN INFINITE FAMILIES OF QUADRATIC APN POLYNOMIALS OVER $\mathbb{F}_{2^n}$

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk, \gcd(k,3) = \gcd(s,3k) = 1, p \in \{3,4\}, i = sk \bmod p, m = p-i, n \geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[9]
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q = 2^m, n = 2m$, $gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[8]
F4	$x^3+a^{-1}\mathrm{Tr}_1^n(a^3x^9)$	$a \neq 0$	[10]
F5	$x^3+a^{-1}\mathrm{Tr}_3^n(a^3x^9+a^6x^{18})$	$3 \vert n$, $a \neq 0$	[11]
F6	$x^3+a^{-1}\mathrm{Tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3 \vert n$, $a \neq 0$	[11]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k,3) = \gcd(s,3k) = 1, v, w \in \mathbb{F}_{2^k}, vw \neq 1, 3 \vert (k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[5]
F10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n = 2m, m \geqslant 2$ even, $\gcd(k,m) = 1$ and $i \geqslant 2$ even, u primitive in $\mathbb{F}_{2^n}^*, u' \in \mathbb{F}_{2^m}$ not a cube	[26]
F11	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n = 3m, m$ odd, $L(x) = ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [7]	[7]
F12	$u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q = 2^m, n = 2m, \gcd(i,m) = 1$, $x^{2^i+1}+ax+b$ has no roots in $\mathbb{F}_{2^m}$	[23]
F13	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m$, $a, b, c \in \mathbb{F}_4$ satisfying the conditions of Corollary 1	new

APN monomials and 11 infinite families of APN polynomials are known. Together, these cover only a miniscule fraction of all APN functions: for instance, more than 8000 CCZ-inequivalent APN functions have been constructed over $\mathbb{F}_2^8$ [25], yet none of them have been classified into general constructions yet. Finding new examples of infinite families is an area of intense ongoing research. Tables I and II list all currently known infinite families of APN functions.

When $n = m$, it is convenient to identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and to consider mappings from $\mathbb{F}_{2^n}$ (instead of $\mathbb{F}_2^n$) to itself. The binomials $B'(x) = x^3+\alpha^{36}x^{36}$ and $B(x) = x^3+\alpha^{341}x^{36}$ (where α is a primitive element of $\mathbb{F}_{2^{10}}$) are known to be APN over $\mathbb{F}_{2^{10}}$ [16] and are remarkable as the first examples of APN functions

that are CCZ-inequivalent to power functions. Since their discovery in 2006, a lot of work has been done on the construction of polynomial APN functions [4], [5], [7]–[11], [26] but the binomials $B(x)$ and $B'(x)$ have not been classified into any infinite family or construction to date. It is worth noting that the binomial x^3+wx^{258} over $\mathbb{F}_{2^{12}}$ (where $w \in \mathbb{F}_{2^{12}}$ has order 273 or 585) was also a sporadic, i.e., not belonging to any infinite family, APN polynomial, until it was classified into two infinite families, one for dimensions n that are multiples of 3, and one for dimensions n that are multiples of 4 [9].

Attempts to generalize $B(x)$ and $B'(x)$ to an infinite family have, to the best of our knowledge, so far only considered binomials of a similar form in higher dimensions [10], which has not resulted in any success thus far. In our work, we take a different approach, which involves expanding $B(x)$ and $B'(x)$ into APN polynomials with more than two terms, and then generalizing these polynomials to higher dimensions. Based on our experiments, we arrive at a family of quadrinomials of the form

$$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$$

in which $B(x)$ corresponds to the coefficients$(a, b, c) = (\beta, 0, 0)$ and the exponents $i = 3$, $k = 2$. We show that the coefficients $(a, b, c) = (\beta, \beta^2, 1)$, where β is primitive in $\mathbb{F}_{2^2}$, and exponents $i = m-2$, $i = (m-2)^{-1} \mod n$, $i = m$ or $i = n-1$ in the case of even k, or $i = m+2$, $i = (m+2)^{-1} \mod n$, or $i = n-1$ in the case of odd k, where $n = 2m$ and m is odd with $3 \nmid m$, give rise to APN functions. Furthermore, in the case of $n = 10$, we show that for $i = m-2$ and $i = (m-2)^{-1}$, these APN functions are CCZ-inequivalent to each other or to any other known APN function over $\mathbb{F}_{2^{10}}$, including $B(x)$ and $B'(x)$. For $i = m$ and $i = n-1$ the functions are equivalent to representatives from the known families.

The condition $3 \nmid m$ is needed since β is a cube in $\mathbb{F}_{2^n}$ if and only if $3 \mid m$. Indeed, β is a cube in $\mathbb{F}_{2^n}$ if and only if $\beta^{(2^n-1)/d} = 1$, where $d = \gcd(2^n-1, 3)$; see e.g. [21]. For even n, $\gcd(2^n-1, 3) = 3$. The rest follows by observing that for $n = 2m$, $(2^n-1)/3 \equiv 0 \pmod{2^n-1}$ if and only if $3 \mid m$, and since $\beta^3 = 1$.

II. Preliminaries

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, and by $\mathbb{F}_{2^n}^*$ the set of its non-zero elements, i.e., its multiplicative group. For $m \mid n$, we denote by $\mathrm{Tr}_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, resp. $\mathrm{N}_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ the trace function $\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}$, resp. the *norm function* $\mathrm{N}_m^n(x) = \prod_{i=0}^{n/m-1} x^{2^{mi}}$ from $\mathbb{F}_{2^n}$ into its subfield $\mathbb{F}_{2^m}$. We will only work with fields of even dimension $n = 2k$; given some element $x \in \mathbb{F}_{2^n}$, we denote $\overline{x} = x^{2^k}$, and refer to $\overline{x}$ as the *conjugate* of x.

An (n, n)-function is any mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Any such function can be expressed as a polynomial of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, for $a_i \in \mathbb{F}_{2^n}$. This is the *univariate representation* of F, and it is unique. The *algebraic degree* of F, denoted $\deg(F)$, is the largest binary weight of an exponent i with $a_i \neq 0$ in the univariate representation, where the *binary weight* of an integer is the number of ones in its binary notation, i.e., the minimum number of distinct powers of two that sum up to it. Functions of algebraic degree 1, 2, and 3 are called *affine*, *quadratic*, and *cubic*, respectively. An affine function F satisfying $F(0) = 0$ is called *linear*.

Given an (n,n)-function F, we denote by $\Delta_F(a,b)$ the number of solutions x to the equation $D_aF(x) = b$, where $D_aF(x) = F(x+a) + F(x)$ is the *derivative* of F in direction $a \in \mathbb{F}_{2^n}$. The largest value of $\Delta_F(a,b)$ among all $a \neq 0$ and all b is denoted by Δ_F and is called the *differential uniformity* of F. If $\Delta_F = 2$, we say that F is *almost perfect nonlinear (APN)*.

The *Walsh transform* of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the integer-valued function $W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot F(x) + a \cdot x}$ for $a, b \in \mathbb{F}_{2^n}$, where the scalar product can be defined as $a \cdot b = \mathrm{Tr}_1^n(ab)$ for $a, b \in \mathbb{F}_{2^n}$ without losing generality. The values of $W_F(a,b)$ for $a, b \in \mathbb{F}_{2^n}$ are the *Walsh coefficients* of F, and the multiset $\{W_F(a,b) : a, b \in \mathbb{F}_{2^n}\}$ is called the *Walsh spectrum* of F. The multiset $\{|W_F(a,b)| : a, b \in \mathbb{F}_{2^n}\}$ of the absolute values of the Walsh transform is the *extended Walsh spectrum*.

Two designs, $\mathrm{dev}(G_F)$ and $\mathrm{dev}(D_F)$, can be associated with a given APN function F over $\mathbb{F}_{2^n}$ [17]. In both cases, the set of points is $\mathbb{F}_{2^n}^2$. The set of blocks of $\mathrm{dev}(G_F)$, resp. $\mathrm{dev}(D_F)$ is $\{(x+a, F(x)+b) : x \in \mathbb{F}_{2^n}\}$ for $a, b \in \mathbb{F}_{2^n}$, resp. $\{(x+y+a, F(x) + F(y) + b) : x, y \in \mathbb{F}_{2^n}, x \neq y\}$ for $a, b \in \mathbb{F}_{2^n}$. The rank of the incidence matrix of $\mathrm{dev}(G_F)$, resp. $\mathrm{dev}(D_F)$ is called the Γ-*rank*, resp. Δ-*rank* of F.

Since the number of distinct (n,n)-functions, viz. $(2^n)^{2^n}$, grows rapidly with the dimension, (n,n)-functions are classified only up to a suitable equivalence relation which preserves the properties being studied. The most general known equivalence relation which preserves the differential uniformity is the so-called *Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence)*: we say that two (n,n)-functions F and F' are CCZ-equivalent if there is an affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}^2$ which maps the graph $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph $G_{F'}$ of G. Deciding whether two given functions F and F' are CCZ-equivalent computationally is a difficult problem in general, and is typically resolved via code isomorphism. More precisely, a linear code $\mathcal{C}_F$ with the generating matrix

$$\mathcal{C}_F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & \alpha & \dots & \alpha^{2^n-1} \\ F(0) & F(\alpha) & \dots & F(\alpha^{2^n-1}) \end{pmatrix}$$

can be associated with any given (n,n)-function F, where α is the primitive element of $\mathbb{F}_{2^n}$. Then F and F' are CCZ-equivalent if and only if $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ are isomorphic [6].

Various CCZ-invariants, i.e., properties that remain invariant under CCZ-equivalence, can be used to show that a pair of (n,n)-functions is CCZ-inequivalent. These include the differential uniformity, the extended Walsh spectrum and the Γ- and Δ-ranks. In particular, it is known that if F and F' are CCZ-equivalent, then they must necessarily have e.g. the same Γ-rank. Thus, if two functions have distinct Γ-ranks, then they are definitely CCZ-inequivalent (although the converse does not hold in general).

A special cases of CCZ-equivalence is the so-called *extended affine equivalence (EA-equivalence)*. Two (n,n)-functions F and F' are said to be EA-equivalent if $F' = A_1 \circ F \circ A_2 + A$ for affine $A_1, A_2, A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with A_1, A_2 bijective.

III. A NEW FAMILY OF APN QUADRINOMIALS

Let β denote the primitive element of $\mathbb{F}_{2^2}$. Note that $\overline{\beta} = \beta^2$. We know that $B(x) = x^3 + \beta x^{36}$ and $B'(x) = x^3 + \alpha^{11} x^{341}$, where α is primitive in $\mathbb{F}_{2^{10}}$ are APN over

$\mathbb{F}_{2^{10}}$ [16] but have not been classified into any infinite family yet. By means of the code isomorphism test, we establish that $B(x)$ and $B'(x)$ are CCZ-equivalent, and henceforth concentrate on $B(x)$ only. We look for polynomials $P(x)$ with a small number of terms such that $B(x) + P(x)$ is APN. We do not find any non-trivial (that is, not arising from simple EA-equivalence) monomial $P(x)$ for which $B(x)+P(x)$ is APN. We do, however, come across binomials $P(x)$ for which $B(x)+P(x)$ is APN and is CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$. A detailed description of the tests that we performed for disproving CCZ-equivalence can be found at the end of this section after Theorem 2.

Observation 1. *The quadrinomials* $x^3+\beta x^{36}+\beta^2 x^{96}+x^{129}$ *and* $x^3+\beta x^{129}+\beta^2 x^{96}+x^{36}$ *are APN over* $\mathbb{F}_{2^{10}}$*, and are CCZ-inequivalent to each other and to any other known APN function over* $\mathbb{F}_{2^{10}}$.

Note that $96 \equiv 332 \mod (2^{10}-1)$ and $129 \equiv 3632 \mod (2^{10}-1)$, i.e., $x^{96} = \overline{x^3}$, and $x^{129} = \overline{x^{36}}$ and, conversely, $x^{36} = \overline{x^{129}}$. Furthermore, $36 = 4 \cdot 9 = 4 \cdot (2^3+1)$. It is thus natural to consider functions of the form

$$C_i(x) = x^3 + \beta x^{2^i+1} + \beta^2 \overline{x^3} + \overline{x^{2^i+1}} \tag{1}$$

for $0 \le i \le n-1$. The APN-ness of such functions can be characterized by the solvability of the following system of equations.

Proposition 1. *Let* $n = 2m$*,* $3 \nmid m$*,* m *odd, and let* $C_i(x)$ *be defined as in* (1)*. Consider the system* E_i *defined by*

$$\begin{cases} a^3(x^2+x) \in \beta \cdot \mathbb{F}_{2^m} \\ a^{2^i+1}(x^{2^i}+x) \in \beta \cdot \mathbb{F}_{2^m}. \end{cases} \tag{2}$$

Given some integer $1 \le i \le n-1$*, the function defined by* $C_i(x)$ *is APN over* $\mathbb{F}_{2^n}$ *if, for any* $a \in \mathbb{F}_{2^n}^*$*, the system* E_i *from* (2) *only has trivial solutions in* x*, i.e., only* $x \in \mathbb{F}_2$ *can be a solution to* E_i*.*

Proof. Note that C_i is quadratic, so that proving its APN-ness is equivalent to showing that the equation $D_aC_i(ax) = D_aC_iF(0)$ has only $x \in \mathbb{F}_2$ as solutions for $a \neq 0$. The expression $D_aC_i(ax) + D_aC_iF(0)$ takes the form

$$a^3(x^2+x) + \beta a^{2^i+1}(x^{2^i}+x) + \beta^2\overline{a^3(x^2+x)} + \overline{a^{2^i+1}(x^{2^i}+x)}.$$

For simplicity, denote $A = a^3(x^2+x)$ and $B = a^{2^i+1}(x^{2^i}+x)$. Then the equation $D_aC_i(ax) + D_aC_i(0) = 0$ becomes

$$A + \beta B + \beta^2\overline{A} + \overline{B} = 0. \tag{3}$$

Taking the conjugate of (3) and multiplying it by β, we get $\beta^2 A+\beta B+\beta\overline{A}+\overline{B} = 0$, and, adding this to (3), we obtain $\beta A + \overline{A} = 0$ which implies $\beta^2 A = \beta\overline{A}$, hence $\beta^2 A = \overline{\beta^2 A}$ and thus $\beta^2 A \in \mathbb{F}_{2^m}$, i.e., $A \in \beta \cdot \mathbb{F}_{2^m}$. Multiplying the identity $\beta A+\overline{A} = 0$ by β^2 and substituting it back into (3), we obtain $\beta B + \overline{B} = 0$, so that we also have $B \in \beta \cdot \mathbb{F}_{2^m}$. The two inclusions, viz. $A \in \beta \cdot \mathbb{F}_{2^m}$ and $B \in \beta \cdot \mathbb{F}_{2^m}$, are precisely the equations in the system (2). Therefore, under the hypothesis, $D_aC_i(ax)+D_aC_i(0) = 0$ can only have trivial solutions, and thus $C_i(x)$ is APN. □

Next, we determine values of i for which system (2) only has trivial solutions. According to our experimental results, which encompass dimensions up to 46, there are precisely four such values of i for any given dimension n satisfying the conditions of Proposition 1. Two of these give rise to APN functions equivalent to some of the previously known ones, while the other two lead to infinite constructions of APN functions whose instances for $n = 10$, i.e the quadrinomials from Observation 1, are CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$.

In the proof of Theorem 2 we will need the following auxiliary results.

Lemma 1. *Let $n = 2m$ for m odd, and suppose that for some $c \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(c) = 0$ we have*

$$c(c + c^2 + c^4 + \cdots + c^{2^{m+1}}) \in \mathbb{F}_{2^m}. \tag{4}$$

Then c is a cube.

Proof. First, observe that all elements of $\mathbb{F}_{2^m}$ are cubes due to $(2^m - 1, 3) = 1$ for m odd.

For convenience, let us denote by $h(c) = c+c^2+\cdots+c^{2^{m-1}}$ the "half-trace" function. Then (4) can be written as $ch(c) + c^{2^m+1} + c^{2^{m+1}+1} \in \mathbb{F}_{2^m}$, and since $c^{2^m+1} = \mathrm{N}_m^n(c)$ is an element of $\mathbb{F}_{2^m}$, this becomes simply

$$ch(c) + c^{2^{m+1}+1} \in \mathbb{F}_{2^m}. \tag{5}$$

Observe that $h(c) + \overline{h(c)} = \mathrm{Tr}_1^n(c)$, and since $\mathrm{Tr}_1^n(c) = 0$ by assumption, we have $h(c) = \overline{h(c)}$. Conjugating (5), we get $h(c)(c + \overline{c}) = c\overline{c}(c + \overline{c})$, and, assuming that $c \neq \overline{c}$ (for otherwise c is already in $\mathbb{F}_{2^m}$ and thus a cube), this becomes $h(c) = c\overline{c}$.

From the definition of $h(c)$, we clearly have $h(c) + h(c)^2 = c + \overline{c}$. Hence $c + \overline{c} = c\overline{c} + c^2\overline{c}^2$, from which we get $c+\overline{c}+c\overline{c}+c^2 = c^2\overline{c}^2+c^2$ by adding c^2 to both sides, and, finally, $(c + \overline{c})(1 + c) = c^2(1 + \overline{c}^2)$. Now, observe that $(1 + \overline{c}^2)/(1 + c) = (1 + c)^{2^{m+1}-1}$, which is s cube for m odd, and that $c + \overline{c}$ lies in $\mathbb{F}_{2^m}$ and is thus a cube. Hence c^2, and thus also c is a cube, which completes the proof. □

Theorem 1. *[24] Let t_1 and t_2 denote the zeros of $t^2 + bt + a^3$ in $\mathbb{F}_{2^n}$ where $n = 2m$ and $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_{2^m}^*$. Let $f(x) = x^3 + ax + b$, then*

- *f has three zeros in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{a^3}{b^2} + 1) = 0$ and t_1, t_2 are cubes in $\mathbb{F}_{2^m}$ (if m is even), $\mathbb{F}_{2^n}$ (if m is odd).*
- *f has exactly one zero in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{a^3}{b^2} + 1) = 1$.*
- *f has no zeros in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{a^3}{b^2} + 1) = 0$ and t_1, t_2 are not cubes in $\mathbb{F}_{2^m}$ (if m is even), $\mathbb{F}_{2^n}$ (if m is odd).*

Lemma 2. *[15] Let r, n be positive integers, and let $a, b, c \in \mathbb{F}_{2^n}$. Then the quadratic polynomial $Q(x) = x^{2^r+1} + ax^{2^r} + bx + c$ has either 0, 1, 2, or $2^{r_0} + 1$ roots $x \in \mathbb{F}_{2^n}$, where $r_0 = \gcd(r, n)$.*

Using Lemma 2, we can obtain the following.

Lemma 3. *Let m and i be positive integers such that $\gcd(m, i) = 1$ and let $S \in \mathbb{F}_{2^m} \setminus \{0, 1\}$. Then the polynomial*

$$P(N) = (S^{2^i} + S)N^{2^{2i}} + (S^{2^{2i}} + S)N^{2^i} + (S^{2^{2i}} + S^{2^i})N$$

in N has four roots, viz. $N = 0$, $N = 1$, $N = S$, and $N = S + 1$.

Proof. Note that for $S \notin \{0, 1\}$ the coefficients of P are all non-zero. Dividing P by N and substituting $t = N^{2^i-1}$, we obtain a new polynomial $P'(t) = at^{2^i+1} + bt + c$, with $a = (S^{2^i} + S)$, $b = (S^{2^{2i}} + S)$ and $c = (S^{2^{2i}} + S^{2^i})$. Since $\gcd(i, m) = 1$ from the hypothesis, by Lemma 2 $P'(t)$ can have at most three roots. Due to $\gcd(i, m) = 1$, every element in $\mathbb{F}_{2^m}$ has a unique $(2^i - 1)$-st root, and hence every root t of P' corresponds to a unique root N of P. It remains to verify that for $N \in \{0, 1, S, S+1\}$, $P(N)$ does indeed evaluate to zero. □

We are now ready to prove the main result.

Theorem 2. *Let $n = 2m$ with m odd and $3 \nmid m$. Then the system E_i from* (2) *does not have any solutions $x \notin \mathbb{F}_2$ for the following values of i:*

1) $i = m - 2$*;*
2) $i = m$*;*
3) $i = (m - 2)^{-1} \mod n$*;*
4) $i = n - 1$.

Proof. First, observe that all elements of the half-field $\mathbb{F}_{2^m}$ are cubes in $\mathbb{F}_{2^n}$. If some $a \neq 0$ and $x \notin \mathbb{F}_2$ satisfy system (2), then $a^3(x^2+x) = \alpha_1\beta$ and $a^{2^i+1}(x^{2^i}+x) = \alpha_2\beta$ for some $\alpha_1, \alpha_2 \in \mathbb{F}_{2^m}$ with $\alpha_1 \neq 0$. We can write $\alpha_1 = c^3$ for some $c \in \mathbb{F}_{2^n}^*$. Dividing both sides of the first equation by c^3, we obtain $(a/c)^3(x^2 + x) = \beta$. Dividing both sides of the second equation by c^{2^i+1}, we obtain $(a/c)^{2^i+1}(x^{2^i} + x) = \alpha_2\beta c^{-(2^i+1)}$. Since $3 \mid 2^i + 1$ for odd i, $c^{-(2^i+1)}$ is in $\mathbb{F}_{2^m}$. Thus, system (2) has a non-trivial solution $x \notin \mathbb{F}_2$ if and only of the system

$$\begin{cases} a^3(x^2 + x) = \beta \\ a^{2^i+1}(x^{2^i} + x) = \alpha\beta \end{cases} \tag{6}$$

has a solution for some $\alpha \in \mathbb{F}_{2^m}$. In the following, we show that for each of the values of i given in the statement of the theorem, this reduced system (6) has no solutions.

Case 1 In the case of $i = m - 2$, we have the system

$$\begin{cases} a^3(x^2 + x) = \beta \\ a^{2^{m-2}+1}(x^{2^{m-2}} + x) = \beta \cdot \mathbb{F}_{2^m} \end{cases}$$

for some $\alpha \in \mathbb{F}_{2^m}$. Raising the second equation to the fourth power, we have $a^{2^m+4}(\overline{x}+x^4) = \alpha^4\beta$. From the first equation, we can write $a^3 = \beta/(x^2 + x)$. Substituting this into the previous equation, we obtain $a^{2^m+1}\frac{\overline{x}+x^4}{x^2+x} \in \mathbb{F}_{2^m}$. Since $a^{2^m+1} \in \mathbb{F}_{2^m}$, this simply means $(\overline{x} + x^4)/(x^2 + x) \in \mathbb{F}_{2^m}$. Thus

$$\frac{\overline{x} + x^4}{x^2 + x} = \frac{x + \overline{x}^4}{\overline{x}^2 + \overline{x}}$$

and hence $(x^2 + x)(x + \overline{x}^4) \in \mathbb{F}_{2^m}$. Denoting $c = x^2 + x$, we can express $x + \overline{x}^4 = x + x^{2^{m+2}}$ as $c+c^2+c^4+\cdots+c^{2^{m+1}}$. We now have $\mathrm{Tr}_1^n(c) = 0$ and $c(c+c^2+\cdots+c^{2^{m+1}}) \in \mathbb{F}_{2^m}$, so according to Lemma 1, $c = x^2 + x$ must be a cube. But then $a^3(x^2 + x) \in \beta \cdot \mathbb{F}_{2^m}$ implies that β is a cube which is impossible when $3 \nmid m$.

Case 2 The case $i = m$ trivially has no solutions since if $a^{2^m+1}(x^{2^m} + x) = \alpha\beta$ for some $\alpha \in \mathbb{F}_{2^m}$, then conjugating both sides yields $a^{2^m+1}(x^{2^m} + x) = \alpha\beta^2$, implying $\beta = \beta^2$.

Case 3 In the case of $i = (m-2)^{-1} \mod n$, we have the equation system

$$\begin{cases} a^{i(m-2)+1}(x^{2^{i(m-2)}} + x) = \beta \\ a^{2^i+1}(x^{2^i} + x) = \alpha\beta \end{cases} \tag{7}$$

for some $\alpha \in \mathbb{F}_{2^m}$. Raising the first equation to the power 2^{2i}, we obtain

$$a^{2^{im}+2^{2i}}(x^{2^{im}} + x^{2^{2i}}) = \beta, \tag{8}$$

and raising the second equation to the power $2^i - 1$ yields

$$a^{2^{2i}-1}(x^{2^i} + x)^{2^i-1} = \alpha^{2^i-1}\beta. \tag{9}$$

From (8) and (9) we obtain the identity

$$\frac{\alpha^{2^i-1}\beta a^{2^{im}+2^{2i}}}{\beta a^{2^{2i}-1}} = \frac{(x^{2^i} + x)^{2^i-1}}{x^{2^{im}} + x^{2^{2i}}}. \tag{10}$$

The left-hand side of (10) simplifies to $\alpha^{2^i-1}a^{2^{im}+1}$. Since $a^{2^{im}+1} = a^{2^m+1}$ is in $\mathbb{F}_{2^m}$ for any $a \in \mathbb{F}_{2^n}$, we have that $(x^{2^{im}} + x^{2^{2i}})/(x^{2^i} + x)^{2^i-1} \in \mathbb{F}_{2^m}$, i.e.,

$$\frac{(\overline{x} + x^{2^{2i}})(x^{2^i} + x)}{(x^{2^i} + x)^{2^i}} = \frac{(x + \overline{x}^{2^{2i}})(\overline{x}^{2^i} + \overline{x})}{(\overline{x}^{2^i} + \overline{x})^{2^i}}$$

and hence

$$(\overline{x} + x^{2^{2i}})(x^{2^i} + x)(\overline{x}^{2^{2i}} + \overline{x}^{2^i}) = (x + \overline{x}^{2^{2i}})(\overline{x}^{2^i} + \overline{x})(x^{2^{2i}} + x^{2^i}). \tag{11}$$

The left-hand side of (11) takes the form

$$A(x) = x^{2^i}\overline{x}^{2^{2i}+1} + x^{2^i}\overline{x}^{2^i+1} + x^{2^{2i}+2^i}\overline{x}^{2^{2i}} + x^{2^{2i}+2^i}\overline{x}^{2^i} + x\overline{x}^{2^{2i}+1} + x\overline{x}^{2^i+1} + x^{2^{2i}+1}\overline{x}^{2^{2i}} + x^{2^{2i}+1}\overline{x}^{2^i}.$$

Denoting $S = x + \overline{x}$ and $N = x\overline{x}$, and observing that $A(x) + A(\overline{x}) = 0$, we can write

$$A(x) + A(\overline{x}) = (S^{2^i} + S)N^{2^{2i}} + (S^{2^{2i}} + S)N^{2^i} + (S^{2^{2i}} + S^{2^i})N = 0. \tag{12}$$

We now consider the expression on the right-hand side of (12) as a polynomial in S and N and determine its possible roots by Lemma 3. Before doing so, we need to rule out the cases when $N = 0$ and $S \in \{0, 1\}$. Unless $x = 0$, we must clearly have $N \neq 0$. If $S = x + \overline{x} = 0$, then we must have $x \in \mathbb{F}_{2^m}$ so that $(x^2 + x)$ is in $\mathbb{F}_{2^m}$ and is hence a cube. But then the equation $a^3(x^2 + x) = \beta$ from (7) implies that β is a cube, which is impossible under the assumption $3 \nmid m$. If $S = x + \overline{x} = 1$, then from the identity $x^2 + (x + \overline{x})x = x\overline{x}$ we get $x^2 + x = x\overline{x} = N$ and we once again infer that $x^2 + x$ must be a cube, which is impossible.

We can now apply Lemma 3 to see that only $N = 1$, $N = S$, and $N = S + 1$ are solutions to (12). We can additionally assume $N \neq S + 1$, since otherwise we have $x\overline{x} = x + \overline{x} + 1$; multiplying both sides by x and adding this to the original expression then gives us $(x^2 + 1)(\overline{x} + 1) = 0$, which implies $x = 1$. We thus only need to consider the cases $N = 1$ and $N = S$.

By adding $a^3(x^2 + x) = \beta$ and $x^2 + Sx + N = 0$ together, we obtain $(S + 1)x + N = \beta/a^3$ and hence

$$x = (N + \beta/a^3)/(S + 1). \tag{13}$$

Since $N = x\overline{x}$ and thus $x = N/\overline{x}$, we obtain

$$\frac{N + \beta/a^3}{S + 1} = \frac{N(S + 1)}{N + \overline{(\beta/a^3)}}$$

leading to

$$\begin{aligned} N(S + 1)^2 = (N + \beta/a^3)(N + \overline{\beta/a^3}) = \\ N^2 + (\beta/a^3 + \overline{\beta/a^3})N + \beta/a^3\overline{\beta/a^3}. \end{aligned} \tag{14}$$

From (13), we get $S = x + \overline{x} = \frac{N+\beta/a^3+N+\overline{\beta/a^3}}{S+1} = \frac{\beta/a^3+\overline{\beta/a^3}}{S+1}$ so that

$$S^2 + S = \beta/a^3 + \overline{\beta/a^3}. \tag{15}$$

Substituting this into (14), we obtain $N(S + 1)^2 = N^2 + (S^2 + S)N + \beta/a^3\overline{\beta/a^3}$, which implies

$$N^2 + (S + 1)N + \beta/a^3\overline{\beta/a^3} = 0.$$

When $N \in \{1, S\}$, this implies $S = a^{-3}\overline{a^{-3}}$. Hence $S^2 + S = a^{-6}\overline{a^{-6}} + a^{-3}\overline{a^{-3}}$. Combining this with (15), we see that $\beta/a^3 + \overline{\beta/a^3} = a^{-6}\overline{a^{-6}} + a^{-3}\overline{a^{-3}}$ and hence $t_1 = \beta/a^3$ and $t_2 = \overline{\beta/a^3}$ are roots of the polynomial $t^2+(a^{-6}\overline{a^{-6}}+a^{-3}\overline{a^{-3}})t+a^{-3}\overline{a^{-3}}$.

If we denote $c_1 = (a\overline{a})^{-1}$, $c_2 = c_1^6+c_1^3$, we can write it more succinctly as $t^2+c_2t+c_1^3$. Dividing both sides by c_2^2 and denoting $y = t/c_2$, this becomes $y^2 + y + (c_1^3)/(c_2^2)$.

Since a quadratic equation $y^2 + y = v$ for $v \in \mathbb{F}_{2^k}$ has solutions in $\mathbb{F}_{2^k}$ if and only if $\mathrm{Tr}_1^k(v) = 0$ [1], we have that $\mathrm{Tr}_1^m(\frac{c_1^3}{c_2^2}) = 1$, and hence $\mathrm{Tr}_1^m(\frac{c_1^3}{c_2^2} + 1) = 0$ due to m being odd.

Letting $f(y) = y^3 + c_1y + c_1^6 + c_1^3$, by Theorem 1, f has either three roots, or none at all. However, c_1^2 can easily be seen to be a root, so that f must have three roots. Again by Theorem 1, this implies that t_1 and t_2 have to be cubes, which is impossible for $3 \nmid m$.

Case 4 When $i = n - 1$, we have the system

$$\begin{cases} a^3(x^2 + x) = \beta \\ a^{2^{n-1}+1}(x^{2^{n-1}} + x) = \alpha\beta \end{cases}$$

for $\alpha \in \mathbb{F}_{2^m}$.

Raising the second equation to the second power yields $a^3(x^2 + x) = \alpha^2\beta^2$ so that we have $\alpha^2\beta^2 = \beta$, implying that β lies in $\mathbb{F}_{2^m}$. □

According to our experimental results up to dimension $n = 46$, the values of i given in Theorem 2 are the only ones for which $C_i(x) = x^3 + \beta x^{2^i+1} + x^{3\cdot 2^m} + x^{2^{i+m}+2^m}$ is APN. We can generalize C_i to the form $C_i'(x) = x^3+\beta(x^{2^i+1})^{2^k}+\beta^2\overline{x^3}+\overline{(x^{2^i+1})^{2^k}}$ for some non-negative integer k. The APN-ness of such a function can be characterized by the solvability of the system

$$\begin{cases} a^3(x^2 + x) \in \beta \cdot \mathbb{F}_{2^m} \\ (a^{2^i+1}(x^{2^i} + x))^{2^k} \in \beta \cdot \mathbb{F}_{2^m}. \end{cases} \tag{16}$$

Note that raising β to an even power of two leaves it unchanged. Thus, for even values of k, system (16) has non-trivial solutions if and only if (2) does. Therefore, for $i \in \{m-2, m, n-1, (m-2)^{-1} \mod n\}$ and even k the generalized quadrinomial $C_i'(x)$ is APN.

If k is odd, we obtain a slightly different system.

Lemma 4. *Let k be odd. Then the system*

$$\begin{cases} a^3(x^2+x) \in \beta \cdot \mathbb{F}_{2^m} \\ (a^{2^i+1}(x^{2^i}+x))^{2^k} \in \beta \cdot \mathbb{F}_{2^m}. \end{cases} \tag{17}$$

has only trivial solutions for $i \in \{m+2, m, (m+2)^{-1} \mod n\}$.

Proof. Suppose $i = m+2$. Since raising β to an odd power of two yields β^2, raising the second equation of system (17) to the power 2^{n-k} leaves us with $a^{2^{m+2}+1}(x^{2^m+2} + x) = \alpha'\beta^2$ for $\alpha' = \alpha^{2^{n-k}}$. Raising it again to the power (2^{m-2}) and, noting that $m-2$ is odd, we obtain $a^{2^{m-2}} + 1(x^{2^{m-2}} + x) = \alpha''\beta$ with $\alpha'' = \alpha'^{2^{m-2}}$, which is the same as system (2). Similarly, when $i = (m+2)^{-1}$, we first raise the second equation to the power 2^{n-k}, and then to the power $2^{(m-2)^{-1} \mod n}$; again, $(m-2)^{-1} \mod n$ is odd, so that we come back to system (7). In the case of $i = m$, it suffices to conjugate the equation $a^{2^m+1}(x^{2^m} + x) = \alpha'\beta^2$ in order to derive a contradiction in the same way as in the proof of Theorem 2. □

When k is odd, the case of $i = n-1$ does allow non-trivial solutions, which can easily be seen by taking $\alpha = 1$ and any $a \in \mathbb{F}_{2^n}^*$ for which $x^2 + x = \beta/a^3$ is solvable. According to our data for dimension $n = 10$ (which is the highest dimension for which we can computationally test CCZ-equivalence by our current means), the polynomials C_i' for odd values of k are equivalent to some C_i, so that we may assume $k = 0$. Furthermore, for $i = m$ and $i = n-1$, the polynomial C_i over $\mathbb{F}_{2^{10}}$ is CCZ-equivalent to one of the known CCZ-equivalence classes: in the case of $i = n-1$, C_i is equivalent to the Gold function x^3, and in the case of $i = m$ it is equivalent to family F3 from Table II.

The remaining two values of i, viz. $m-2$ and $(m-2)^{-1} \mod n$ yield for dimension $n = 10$ the two CCZ-inequivalent APN quadrinomials from Observation 1, C_3 and C_7, which are, in addition, CCZ-inequivalent to any currently known APN function over $\mathbb{F}_{2^{10}}$. We have verified this computationally in two ways. First, we used the code isomorphism test described in Section II to compare C_3 and C_7 against representatives from the known infinite families, against the sporadic binomials $B(x)$ and $B'(x)$, and, finally, against themselves. These tests typically take less than half a minute for any given pair of functions, and show that C_3 and C_7 are indeed CCZ-inequivalent to any other known APN function over $\mathbb{F}_{2^{10}}$. Second, we have computed the Γ-ranks of C_3 and C_7, B, and representatives from the equivalence classes of the known APN functions. The results are summarized in Table III below and further confirm these results.

Family F12 in Table II gives six CCZ-inequivalent representatives over $\mathbb{F}_{2^{10}}$. Since their polynomial form is quite complicated, we omit it in Table III, and only list their Γ-ranks; we note that only five values are given, since two of these six CCZ-inequivalent representatives have the same Γ-rank.

In any case, by inspecting the Γ-ranks of the known APN functions in the table, it is evident that C_3 and C_7 are inequivalent to any of them. As a consequence, we collect all the above results in the following corollary and construct a new family of APN functions.

Corollary 1. *Let $n = 2m$ with m odd and $3 \nmid m$. Consider the quadrinomial*

$$C(x) = x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}.$$

Then $C(x)$ is APN over $\mathbb{F}_{2^n}$ in the following cases:

1) $n = 10$, $(a, b, c) = (\beta, 0, 0)$, $i = 3$, $k = 2$ *(this gives us the binomial $B(x)$);*
2) $(a, b, c) = (\beta, \beta^2, 1)$, $i = m - 2$, k *even;*
3) $(a, b, c) = (\beta, \beta^2, 1)$, $i = (m - 2)^{-1}$, k *even;*
4) $(a, b, c) = (\beta, \beta^2, 1)$, $i = m$, k *even;*
5) $(a, b, c) = (\beta, \beta^2, 1)$, $i = n - 1$, k *even*
6) $(a, b, c) = (\beta, \beta^2, 1)$, $i = m + 2$, k *odd;*
7) $(a, b, c) = (\beta, \beta^2, 1)$, $i = (m + 2)^{-1}$, k *odd;*
8) $(a, b, c) = (\beta, \beta^2, 1)$, $i = n - 1$, k *odd .*

Furthermore, in dimension $n = 10$, the functions in items 2 and 3 lie in distinct classes with respect to CCZ-equivalence and are CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$, including $B(x)$.

TABLE III
Γ-RANKS OF ALL KNOWN CCZ-INEQUIVALENT APN FUNCTIONS OVER $\mathbb{F}_{2^{10}}$

Function	Family	Γ-rank
x^3	Gold	125042
x^9	Gold	136492
x^{57}	Kasami	186416
x^{339}	Dobbertin	280604
$x^6 + x^{33} + \alpha^{31}x^{192}$	F3	151216
$x^{33} + x^{72} + \alpha^{31}x^{258}$	F3	153896
$x^3 + \mathrm{Tr}_1^{10}(x^9)$	F4	153896
$x^3 + \alpha^{-1}\mathrm{Tr}_1^{10}(a^3x^9)$	F4	164098
-	F12	162550, 163308, 163398, 163400, 164026
$B(x) = x^3 + \alpha^{341}x^{36}$	[16]	169984
C_3	new	166068
C_7	new	166168

CONCLUSION

We have constructed a family of quadrinomial functions over finite fields $\mathbb{F}_{2^n}$ with $n = 2m$, m odd and $3 \nmid m$ which contains the previously unclassified binomial $x^3 + \beta x^{36}$ (discovered in 2006 as the first example of an APN function CCZ-inequivalent to a power function) in the sense that $B(x)$ can be obtained by setting two of the coefficients in the quadrinomial construction to zero. We have shown two infinite constructions of APN functions belonging to this family, and demonstrated that their instances over $\mathbb{F}_{2^{10}}$ are CCZ-inequivalent to any known APN function over this field,

including the sporadic binomial $B(x)$, and that they are CCZ-inequivalent to each other. We have also characterized the APN-ness of all quadrinomials of the form $x^3 + \beta(x^{2^i+1})^{2^k} + \beta^2 x^{3\cdot 2^m} + (x^{2^{i+m}+2^m})^{2^k}$ in terms of the solvability of a system of equations.

ACKNOWLEDGEMENTS

The research presented in this paper was supported by the Trond Mohn Foundation, and by the Research Council of Norway under contract 247742/O70.

REFERENCES

[1] E. R. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Information and control*, vol. 10, no. 6, pp. 553–564, 1967.

[2] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 65–76.

[3] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, Jan 1991. [Online]. Available: https://doi.org/10.1007/BF00630563

[4] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," *Finite Fields and Their Applications*, vol. 14, no. 3, pp. 703–714, 2008.

[5] ——, "A few more quadratic APN functions," *Cryptography and Communications*, vol. 3, no. 1, pp. 43–53, 2011.

[6] K. Browning, "APN polynomials and related codes," *Special volume of Journal of Combinatorics, Information and System Sciences*, vol. 34, pp. 135–159, 2009.

[7] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa, "Constructing APN functions through isotopic shifts," Cryptology ePrint Archive, Report 2018/769, 2018.

[8] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2354–2357, 2008.

[9] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4218–4229, 2008.

[10] ——, "Constructing new APN functions from known ones," *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 150–159, 2009.

[11] ——, "On a construction of quadratic APN functions," in *2009 IEEE Information Theory Workshop*, 2009, pp. 374–378.

[12] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case," *Information & Computation*, vol. 151, no. 1, pp. 57–72, 1999.

[13] ——, "Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1271–1275, 1999.

[14] ——, "Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5," *International Conference on Finite Fields and Applications*, pp. 113–121, 2001.

[15] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 613–627, 2006.

[16] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 744–747, 2006.

[17] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic," *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 59–81, 2009.

[18] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)," *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[19] H. Janwa and R. M. Wilson, "Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes," in *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. Springer, 1993, pp. 180–194.

[20] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes," *Information & Computation*, vol. 18, no. 4, pp. 369–394, 1971.

[21] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge university press, 1997, vol. 20.

[22] K. Nyberg, "Differentially uniform mappings for cryptography," *Lecture Notes in Computer Science*, vol. 765, pp. 55–64, 1994.

[23] H. Taniguchi, "On some quadratic APN functions," *Designs, Codes and Cryptography*, pp. 1–11, 2019.

[24] K. S. Williams, "Note on cubics over $GF(2^n)$ and $GF(3^n)$," *Journal of Number Theory*, vol. 7, no. 4, pp. 361–365, 1975.

[25] Y. Yu, M. Wang, and Y. Li, "A matrix approach for constructing quadratic APN functions," *Designs, codes and cryptography*, vol. 73, no. 2, pp. 587–600, 2014.

[26] Y. Zhou and A. Pott, "A new family of semifields with 2 parameters," *Advances in Mathematics*, vol. 234, pp. 43–60, 2013.

Paper V

Deciding EA-equivalence via invariants

Nikolay S. Kaleyski
Submitted to *Cryptography and Communications*

Deciding EA-equivalence via invariants

Nikolay Kaleyski

Department of informatics, University of Bergen

Abstract

We define a family of efficiently computable invariants for (n, m)-functions under EA-equivalence, and observe that, unlike the known invariants such as the differential spectrum, algebraic degree, and extended Walsh spectrum, in the case of quadratic APN functions over $\mathbb{F}_{2^n}$ with n even, these invariants take on many different values for functions belonging to distinct equivalence classes. We show how the values of these invariants can be used constructively to implement a test for EA-equivalence of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$; to the best of our knowledge, this is the first algorithm for deciding EA-equivalence without resorting to testing the equivalence of associated linear codes.

I. Introduction

Let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements for some positive integer n, and let $\mathbb{F}_{2^n}^*$ denote its multiplicative group. The vector space of dimension n over $\mathbb{F}_2$ will be denoted by $\mathbb{F}_2^n$. An (n, m)-*function*, or *vectorial Boolean function*, is any mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ or, equivalently, from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. We typically assume that $m = n$, i.e. we concentrate on functions from a finite field of characteristic two to itself; however, the approach given in the present paper can be applied to an arbitrary pair of dimensions (n, m).

In the particular case of $n = m$, we can conveniently represent (n, n)-functions by univariate polynomials over $\mathbb{F}_{2^n}$; more precisely, any (n, n)-function F can be written as $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ for some coefficients $c_i \in \mathbb{F}_{2^n}$. This form, called the *univariate representation* of F, always exists, and is unique. In the general case, any (n, m)-function F can be represented uniquely as a multivariate polynomial of the form $F(x) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}$ for $a_u \in \mathbb{F}_2^m$, where v_i denotes the i-th component of the vector $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_2^n$. We will not concern ourselves too deeply with the choice of representation here, as it is typically only important when defining and classifying (n, m)-functions. However, when illustrating some of the concepts of the EA-equivalence test with examples, we will mostly use (n, n)-functions and the univariate representation.

As suggested above, the finite field $\mathbb{F}_{2^n}$ can be identified with the vector space $\mathbb{F}_2^n$, and so the elements of $\mathbb{F}_{2^n}$ can be identified with binary vectors of n bits; thus, (n, m)-functions can be understood as transformations that take an n-bit sequence as input, and produce an m-bit sequence as output. Thanks to this interpretation, vectorial Boolean functions naturally find applications in the theory and practice of various areas of mathematics and computer science. In particular, vectorial Boolean functions are used in modern block ciphers in the role of so-called "S-boxes", or "substitution boxes", and typically constitute the only non-linear part of the cipher. Consequently, the security of the cipher directly depends on the properties of the underlying S-boxes, which motivates the study of vectorial Boolean functions with respect to their cryptographic properties. It is also intuitively clear that (n, n)-functions constitute one

of the most practically significant cases, since in cryptography one typically wants to replace a bit sequence with a different bit sequence of the same length.

A basic property of any (n, m)-function, which also has cryptographic implications, is its algebraic degree. Given an (n, m)-function with ANF

$$F(x) = \sum_{u \in \mathbb{F}_2^n} u \prod_{i=1}^{n} x_i^{u_i},$$

the *algebraic degree* of F is defined as the largest degree of any term $x_i^{u_i}$ that has a non-zero coefficient a_u. In other words, the algebraic degree of F is the multivariate degree of its ANF. Thus, for instance, $F(x) = x_1x_2x_4 + x_2x_3$ would have algebraic degree 3. In the case of an (n, n)-function given by its univariate representation, the algebraic degree also has a natural interpretation. Given a positive integer i, the *binary weight* of i is the number of non-zero entries in its binary representation; for example, 19 is written as 10011 in binary, and hence has binary weight 3. The *algebraic degree* of $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ is the largest binary weight of any exponent i with $c_i \neq 0$. Functions of algebraic degree 1, 2, and 3, are called *affine*, *quadratic*, and *cubic*, respectively. An affine function A with $A(0) = 0$ is called *linear*. An affine (n, n)-function A satisfies $A(x) + A(y) + A(z) = A(x + y + z)$ for any $x, y, z \in \mathbb{F}_{2^n}$; similarly, a linear (n, n)-function L satisfies $L(x) + L(y) = L(x + y)$ for any $x, y \in \mathbb{F}_{2^n}$. It is desirable for vectorial Boolean functions used as S-boxes to have a high algebraic degree, since the latter indicates a good resistance to higher-order differential attacks [12], [23].

Two of the most important cryptographic properties of (n, m)-functions are the differential uniformity and the nonlinearity. Suppose that F is an (n, m)-function for some positive integers n and m. Let $\delta_F(a, b)$ denote the number of solutions $x \in \mathbb{F}_2^n$ to the equation $F(x + a) + F(x) = b$ for any $0 \neq a \in \mathbb{F}_2^n$ and any $b \in \mathbb{F}_2^m$. The multiset $\{\delta_F(a, b) : 0 \neq a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\}$ is called the *differential spectrum* of F. The largest value in the differential spectrum is denoted by δ_F and is called the *differential uniformity* of F.

The existence of a large number of solutions x to some equation of the form $F(x) + F(a + x) = b$ for some $a \neq 0$ and b makes the function F vulnerable to differential cryptanalysis [3]. The value of δ_F should thus be as low as possible. Since $x + a$ is a solution to the aforementioned equation whenever x is, the minimum possible value of δ_F is 2; the class of (n, n)-functions attaining this optimal value is called the class of almost perfect nonlinear (APN), and has been an object of intense study since its introduction by Nyberg in the 90's [25].

The *nonlinearity* $\mathcal{NL}(F)$ of F is simply the minimum Hamming distance between any component function of F and any affine $(n, 1)$-function, the *component functions* of F being the $(n, 1)$-functions F_c of the form $F_c(x) = \mathrm{Tr}_m(cF(x))$, where $\mathrm{Tr}_m : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is the *absolute trace* defined by $\mathrm{Tr}_m(x) = \sum_{i=0}^{m-1} x^{2^i}$ for any $x \in \mathbb{F}_{2^n}$; when the dimension m is clear from context, we will sometimes write just Tr instead of Tr_m. The nonlinearity should be high in order to resist linear cryptanalysis [24].

When studying "linear properties" of functions, such as their nonlinearity, it is useful to adapt some linear-algebraic notions from the vector space $\mathbb{F}_2^n$ even in the case when we are working with the finite field $\mathbb{F}_{2^n}$. The *linear span* of a set $S \subseteq \mathbb{F}_{2^n}$ is simply the set of all possible linear combinations of the elements in S, i.e. if

$S = \{s_1, s_2, \ldots, s_k\}$ for some positive integer k and for $s_i \in \mathbb{F}_{2^n}$, then $\mathrm{Span}(S) = \{c_1 s_1 + c_2 s_2 + \cdots + c_k s_k : c_1, c_2, \ldots, c_k \in \mathbb{F}_2\}$; obviously, the span can be defined in the same way in the case of the vector space $\mathbb{F}_2^n$. Having formalized the linear span, it is straightforward to carry over other notions from $\mathbb{F}_2^n$, such as that of linear independence, and that of a basis of $\mathbb{F}_{2^n}$ (being a linearly independent set $B \subseteq \mathbb{F}_{2^n}$ with $\mathrm{Span}(B) = \mathbb{F}_{2^n}$).

A useful tool for analyzing vectorial Boolean functions is the *Walsh transform*, which is an integer valued function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ associated with $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, and given by the prescription

$$W_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathrm{Tr}_m(bF(x)) + \mathrm{Tr}_n(ax)}$$

for $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m$. In the case of (n, n)-functions, we can more succinctly write

$$W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} \chi(bF(x) + ax),$$

where $\chi(x) = (-1)^{\mathrm{Tr}(x)}$. The values of W_F are called *Walsh coefficients*, and the multiset $\{W_F(a, b) : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\}$ is called the *Walsh spectrum* of F. The multiset of the absolute values of F, i.e. the multiset $\{|W_F(a, b)| : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\}$, is called the *extended Walsh spectrum* of F.

Due to the huge number of (n, m)-functions even for small values of n and m, their classification is typically only performed up to some equivalence relation that preserves the properties being studied. In the case of cryptographically optimal vectorial Boolean functions, the most general equivalence relation preserving both the differential uniformity and the nonlinearity is the so-called Carlet-Charpin-Zinoviev-equivalence, or CCZ-equivalence [11]. Two (n, m)-functions F and G are said to be *CCZ-equivalent* if there is an affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ mapping the graph $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ of F to the graph Γ_G of G.

Testing whether two given functions F and G are CCZ-equivalent is usually done by means of the equivalence of linear codes [7], [19]. More precisely, a particular linear code $\mathcal{C}_F$ is associated with F, and a particular linear code $\mathcal{C}_G$ is associated with G; F and G are then CCZ-equivalent if and only if $\mathcal{C}_F$ and $\mathcal{C}_G$ are equivalent. Testing whether two given linear codes are equivalent has the advantage that it is usually already implemented in most mathematical software, such as the *Magma* programming language that we use for most of our computations [5].

Unfortunately, computationally testing CCZ-equivalence in this way can reliably be performed only when the dimensions m and n are relatively small; in the case of (n, n)-functions, this means $n \leq 9$, since for higher values of n, the memory consumption becomes overwhelming, and the test cannot be performed in a lot of cases. Furthermore, the current implementation of *Magma* can give false negatives due to insufficient memory; in other words, if the equivalence test outputs "false", we have no reliable way of determining whether this is due to insufficient memory, or due to a successfully completed exhaustive search proving the inequivalence of the linear codes (and hence, vectorial Boolean functions) in question.

Ruling out e.g. CCZ-equivalence can be facilitated by means of invariants, i.e. properties or statistics that are preserved under CCZ-equivalence. The differential

spectrum and the extended Walsh spectrum are invariant under CCZ-equivalence, i.e. if two (n, m)-functions F and G are CCZ-equivalent, then their differential spectra and extended Walsh spectra are the same. Unfortunately, the Walsh spectra and differential spectra of all known APN functions are the same (with some rare exceptions in the case of the Walsh spectrum), rendering these invariants nearly useless in practice. Other invariants, such as the Γ-rank and Δ-rank have been introduced [18], that can take different values for distinct CCZ-classes of functions, and can therefore be used to rule out CCZ-equivalence in some cases. The major drawback of these invariants is that they require significant computational resources, meaning that, on the one hand, their calculation takes a long time, e.g. around ten days for a single Γ-rank over $\mathbb{F}_{2^{10}}$, and, on the other hand, computing these invariants for $\mathbb{F}_{2^n}$ with $n > 10$ is impossible at the moment due to overwhelming memory requirements.

A special case of CCZ-equivalence is extended affine equivalence, or EA-equivalence. Two (n, m)-functions F and G are said to be *EA-equivalent* if there exist affine functions $A_1 : \mathbb{F}_2^m \to \mathbb{F}_2^m$, $A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and $A : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that

$$A_1 \circ F \circ A_2 + A = G, \tag{1}$$

with A_1 and A_2 being bijective. We will refer to A_1 as the *outer permutation* and to A_2 as the *inner permutation* throughout the paper. CCZ-equivalence is strictly more general than EA-equivalence combined with taking inverses [9], but in certain cases, such as for quadratic and monomial functions, checking whether two functions (or, potentially, their inverses) are EA-equivalent is enough to decided CCZ-equivalence: two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [27]; and two power functions are CCZ-equivalent if and only if they are cyclotomic equivalent [14]. Recall that two power functions $F(x) = x^d$ and $G(x) = x^e$ over $\mathbb{F}_{2^n}$ are said to be cyclotomic equivalent if $e \equiv 2^k d \mod (2^n - 1)$ or $e^{-1} \equiv 2^k d \mod (2^n - 1)$; furthermore, cyclotomic equivalence is a special case of EA-equivalence and taking inverses. This is particularly interesting when one takes into account that all known APN functions (which fall into more than 20000 distinct CCZ-equivalence classes) are CCZ-equivalent to a monomial or quadratic function, with only a single exception in dimension $n = 6$. Thus, from a practical point of view, being able to test functions for EA-equivalence is virtually as useful as being able to test them for CCZ-equivalence, at least as far as the classification of APN functions is concerned.

Surprisingly, despite its simple definition, the only known algorithm to date for computationally testing the EA-equivalence of two given functions is one by means of associated linear codes, much like in the case of CCZ-equivalence [19]; the associated codes used in this approach are of a somewhat more complicated form than the ones used in the CCZ-equivalence test, and so this approach is even more restrictive with respect to computational resources and memory requirements. Indeed, testing EA-equivalence for quadratic functions (which coincides with CCZ-equivalence) is typically done by testing them for CCZ-equivalence. Algorithms for testing the EA-equivalence of two functions in some other special cases (grouped under the umbrella term "restricted EA-equivalence") have previously been studied in [4], [10], and [26].

Since EA-equivalence is a special case of CCZ-equivalence, any CCZ-invariant is also an EA-invariant. As mentioned above, the extended Walsh spectrum and differential spectrum are practically useless in the case of APN functions, as they

almost always take the same value in the APN case, while the Γ- and Δ-rank involve somewhat laborious computations. EA-equivalence being less general than CCZ-equivalence, it is natural to expect to have properties that are EA-invariant but not CCZ-invariant. One such property is the algebraic degree, which is preserved by EA-equivalence, but not by CCZ-equivalence. Unfortunately, this is not terribly useful for classifying APN function either since, as mentioned above, nearly all known instances of APN functions are quadratic.

In this paper, we present an approach for computationally testing the EA-equivalence of two (n, m)-functions by first guessing the outer permutation A_1, applying its inverse to (1) to obtain a relation of the form $F \circ A_2 + A' = G'$, and then solving the latter for A_2 and A'. In the case of (n, n)-functions with n even, our approach allows the set of possible affine permutations A_1 to be drastically reduced (as opposed to exhaustive search), which makes the entire procedure computationally feasible. Our approach has the advantage that it can be broken down into a multitude of small independent steps, which makes the resulting algorithm easily parallelizable. Unlike the CCZ-equivalence test and EA-equivalence test described in [19], which rely on testing the equivalence of a pair of linear codes (and therefore require specialized and rather complex algorithms), our approach uses only basic arithmetics and linear algebra, and can be easily implemented in any general-purpose programming language, and ran on any computer. Furthermore, each of the individual steps comprising the algorithm has a concrete and meaningful input and output that can be monitored and verified. This precludes the possibility of false positives or negatives as in the case of the current CCZ-equivalence test.

II. A FAMILY OF EA-INVARIANTS

Let m, n, k be positive integers, and t be an element of $\mathbb{F}_2^n$. We denote by $\mathcal{T}_k(t)$ the set of all k-tuples of elements from $\mathbb{F}_2^n$ that add up to t, i.e.

$$\mathcal{T}_k(t) = \{(x_1, x_2, \ldots, x_k) \in (\mathbb{F}_2^n)^k \mid \sum_{i=1}^{k} x_i = t\}.$$

If A is an affine (n, n)-permutation, then the image of any k-tuple $(x_1, x_2, \ldots, x_k)$ from $\mathcal{T}_k(t)$ is a k-tuple $(A(x_1), A(x_2), \ldots, A(x_k))$, the sum of whose elements is

$$A(x_1) + A(x_2) + \cdots + A(x_k) = \begin{cases} A(x_1 + x_2 + \cdots + x_k) & k \text{ odd;} \\ A(x_1 + x_2 + \cdots + x_k) + A(0) & k \text{ even.} \end{cases}$$

Equivalently, A is a one-to-one mapping from $\mathcal{T}_k(t)$ to $\mathcal{T}_k(t')$, where $t' = A(t)$ when k is odd, and $t' = A(t) + A(0)$ when k is even. In particular, a linear A always permutes $\mathcal{T}_k(0)$.

For any (n, m)-function F, let $\Sigma_k^F(t)$ denote the multiset of all sums of the form $F(x_1) + F(x_2) + \cdots + F(x_k)$ for all k-tuples $(x_1, x_2, \ldots, x_k) \in \mathcal{T}_k(t)$. Symbolically:

$$\Sigma_k^F(t) = \left\{ \sum_{i=1}^{k} F(x_i) : (x_1, x_2, \ldots, x_k) \in \mathcal{T}_k(t) \right\}.$$

The multiplicities of $\Sigma_k^F(0)$ are then an EA-invariant for any even value of k.

Proposition 1. Let F and G be (n,m)-functions with $A_1 \circ F \circ A_2 + A = G$ for some affine functions $A_1 : \mathbb{F}_2^m \to \mathbb{F}_2^m, A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n, A : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with A_1, A_2 bijective. Let k be a positive integer. Then

$$\Sigma_k^G(0) = \begin{cases} \{A_1(s) + A(0) : s \in \Sigma_k^F(A_2(0))\} & k \text{ odd;} \\ \{A_1(s) + A_1(0) : s \in \Sigma_k^F(0)\} & k \text{ even.} \end{cases}$$

In particular, the multiplicities of $\Sigma_k^F(0)$ and $\Sigma_k^G(0)$ (that is, the number of times that each element occurs in each multiset) are the same when k is even.

Proof. Consider a k-tuple $(x_1, x_2, \ldots, x_k)$ with $x_1 + x_2 + \cdots + x_k = 0$. The sum of the images of x_i under A_2 is $A_2(x_1) + A_2(x_2) + \cdots + A_2(x_k)$, which becomes $A_2(x_1 + x_2 + \cdots + x_k)$ for odd values of k, and $A_2(x_1 + x_2 + \cdots + x_k) + A_2(0)$ for even values of k. Since $x_1 + x_2 + \cdots + x_k = 0$ by assumption, the sum $A_2(x_1) + \cdots + A_2(x_k)$ is then $A_2(0)$ for odd k, and 0 for even k. Thus, computing all sums of the form $F \circ A_2(x_1) + F \circ A_2(x_2) + \cdots + F \circ A_2(x_k)$ for $(x_1, x_2, \ldots, x_k) \in \mathcal{T}_k(0)$ is equivalent to computing all sums of the form $F(x_1)+F(x_2)+\cdots+F(x_k)$ for $(x_1, x_2, \ldots, x_k) \in \mathcal{T}_k(q)$, with $q = 0$, resp. $q = A_2(0)$ for k even, resp. k odd. Thanks to the affinity of A_1, computing the sums of values of $A_1 \circ F \circ A_2$ amounts to computing the corresponding sums of values of $F \circ A_2$, and then taking their image under A_1, up to the addition of the constant $A_1(0)$ in the case of even k. Finally, the sum $A(x_1) + A(x_2) + \cdots + A(x_k)$ of the images of $x_1, \ldots, x_k$ under A is equal to $A(0)$ for k odd, and is equal to 0 for k even. Computing the sums of values of $G = A_1 \circ F \circ A_2 + A$ is thus the same as computing the sums of values of $A_1 \circ F \circ A_2$, up to the addition of the constant $A(0)$ in the case of odd k. The particular statement follows immediately from the above by observing that the elements of $\Sigma_k^G(0)$ are simply the images of the elements in $\Sigma_k^F(0)$ under the linear part of the permutation A_1. □

Recall that the majority of known APN functions are quadratic, and that testing the equivalence of quadratic (n,n)-functions represents the case of highest practical interest. One very useful observation that we can make in the quadratic case is that we can assume $A_1(0) = A_2(0) = 0$, which (as we see later), greatly simplifies the complexity of the entire EA-equivalence test; and, in particular, means that the multiplicities of $\Sigma_k^F(0)$ are an EA-invariant for quadratic functions in the case of odd values of k as well.

Proposition 2. Let F, G be quadratic (n,n)-functions for some positive integer n, and suppose that $A_1 \circ F \circ A_2 + A = G$ for some affine (n,n)-functions A_1, A_2, A with A_1, A_2 bijective. Furthermore, let $c_1 = A_1(0)$, $c_2 = A_2(0)$, and $L_1(x) = A_1(x) + c_1$, $L_2(x) = A_2(x) + c_2$ so that L_1 and L_2 are linear. Then there exists an affine (n,n)-function A' such that

$$L_1 \circ F \circ L_2 + A' = G.$$

Proof. We can assume that F is purely quadratic, i.e. of the form

$$F(x) = \sum_{0 \le i < j < n} c_{ij} x^{2^i + 2^j}$$

for some coefficients $c_{ij} \in \mathbb{F}_{2^n}$. The composition $F \circ A_2$ expands to

$$\begin{aligned} F(A_2(x)) &= F(L_2(x) + c_2) = \sum_{ij} c_{ij}(L_2(x) + c_2)^{2^i+2^j} \\ &= \sum_{ij} c_{ij} L_2(x)^{2^i+2^j} + \sum_{ij} c_{ij}(c_2^{2^j} L_2(x)^{2^i} + c_2^{2^i} L_2(x)^{2^j} + c_2^{2^i+2^j}) \\ &= F(L_2(x)) + A''(x), \end{aligned}$$

where $A''(x) = \sum_{ij} c_{ij}(c_2^{2^j} L_2(x)^{2^i} + c_2^{2^i} L_2(x)^{2^j} + c_2^{2^i+2^j})$ is an affine function. Then the composition $A_1 \circ F \circ A_2$ becomes

$$A_1(F(A_2(x))) = L_1((F \circ L_2)(x) + A''(x)) + c_1 = L_1 \circ F \circ L_2(x) + A'''(x),$$

where $A'''(x) = L_1(A''(x)) + c_1$. Finally, taking $A' = A'''(x) + A(x)$, we have

$$L_1 \circ F \circ L_2 + A' = G$$

as desired. □

As suggested above, Proposition 2 implies that the multiplicities of $\Sigma_k^F(0)$ are an invariant for both odd and even values of k in the quadratic case. Note that the condition of the function being quadratic is necessary, as witnessed by e.g. $F(x) = x^{15}$ and $G(x) = (x+\alpha)^{15}$ over $\mathbb{F}_{2^6}$, where α is a primitive element of $\mathbb{F}_{2^6}$: the elements of the finite field in question fall into three distinct classes based on their multiplicities in $\Sigma_3^F(0)$, but into five distinct classes based on their multiplicities in $\Sigma_3^G(0)$.

Corollary 1. Following the notation and hypothesis of Proposition 1, if F and G are in addition quadratic, then the multiplicities of $\Sigma_k^F(0)$ and $\Sigma_k^G(0)$ are the same for any value of k.

The complexity of computing the multiplicities of $\Sigma_k^F(t)$ for an (n,m)-function F increases exponentially with each increment of k. Fortunately, computing the multiplicities via the Walsh transform of F results in a complexity that does not depend on the value of k.

Proposition 3. Let F be an (n,m)-function, k be a positive integer, $t \in \mathbb{F}_2^n$ and $s \in \mathbb{F}_2^m$. Let $M_k^F(t,s)$ denote the number of k-tuples $(x_1, x_2, \ldots, x_k)$ such that $x_1 + x_2 + \cdots + x_k = t$ and $F(x_1) + F(x_2) + \cdots + F(x_k) = s$. Then

$$2^{m+n} M_k^F(t,s) = \sum_{a \in \mathbb{F}_2^n} (-1)^{\mathrm{Tr}_n(at)} \sum_{b \in \mathbb{F}_2^m} (-1)^{\mathrm{Tr}_m(bs)} W_F^k(a,b). \tag{2}$$

Proof. From the definition of the Walsh transform, the expression

$$\sum_{a \in \mathbb{F}_2^n} (-1)^{\mathrm{Tr}_n(at)} \sum_{b \in \mathbb{F}_2^m} (-1)^{\mathrm{Tr}_m(bs)} W_F^k(a,b)$$

expands to

$$\sum_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m} \sum_{x_1, \ldots, x_k \in \mathbb{F}_2^n} (-1)^{\mathrm{Tr}_m(b(s + \sum_{i=1}^k F(x_i))) + \mathrm{Tr}_n(a(t + \sum_{i=1}^k x_i))}.$$

By changing the order of summation, this becomes

$$\sum_{b\in\mathbb{F}_2^m}\sum_{x_1,\ldots,x_k\in\mathbb{F}_2^n}(-1)^{\mathrm{Tr}_m(b(s+\sum_{i=1}^k F(x_i)))}\sum_{a\in\mathbb{F}_2^n}(-1)^{\mathrm{Tr}_n(a(t+\sum_{i=1}^k x_i))}.$$

The statement then follows by recalling that $\sum_{a\in\mathbb{F}_2^n}(-1)^{\mathrm{Tr}_n(ax)}$ evaluates to 0 for any $0\neq x\in\mathbb{F}_2^n$, and evaluates to 2^n for $x=0$. □

Finding the multiplicity of a given element $s\in\mathbb{F}_2^m$ in $\Sigma_k^F(t)$ now amounts to computing the Walsh coefficients $W_F(a,b)$ of F, raising them to the power k, and combining them according to (2). We note that for the purposes of testing EA-equivalence, we always assume $t=0$, and hence (2) simplifies to $2^{m+n}M_k^F(0,s)=\sum_{a\in\mathbb{F}_2^n,b\in\mathbb{F}_2^m}(-1)^{\mathrm{Tr}_m(bs)}W_F^k(a,b)$. Furthermore, the Walsh coefficients $W_F(a,b)$ can be precomputed for all F from a known set of EA-representatives, allowing the computations to be sped up at the cost of storing the precomputed result.

Remark 1. We note that, in the case of APN functions, the multiset of the multiplicities of $\Sigma_3^F(0)$ is essentially the same as the multiset Π_F^0 studied in [8]. The latter, given an (n,n)-function F, is defined as the multiset

$$\Pi_F^0=\{\#\{a\in\mathbb{F}_{2^n}\mid(\exists x\in\mathbb{F}_{2^n})F(x)+F(a+x)+F(a)=b\}:b\in\mathbb{F}_{2^n}\}.$$

The equation $F(x)+F(a+x)+F(a)=b$ has either 0 or 2 solutions for any $0\neq a\in\mathbb{F}_{2^n}$ and any $b\in\mathbb{F}_{2^n}$ if F is APN. Thus, an equivalent invariant would be the multiset

$$\{F(x)+F(a+x)+F(a):a,x\in\mathbb{F}_{2^n}\},$$

and it is easy to see that this can equivalently be rewritten as

$$\{F(x_1)+F(x_2)+F(x_3):(x_1,x_2,x_3)\in\mathbb{F}_{2^n}^3\mid x_1+x_2+x_3=0\},$$

which is essentially the same as $\Sigma_3^F(0)$. As pointed out in [8], the multiset Π_F^0 is a CCZ-invariant for quadratic APN functions.

III. Guessing the outer permutation

Suppose that we are given two EA-equivalent functions F and G from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ for some positive integers n,m, so that $A_1\circ F\circ A_2+A=G$ for some affine functions $A_1:\mathbb{F}_2^m\to\mathbb{F}_2^m$, $A_2:\mathbb{F}_2^n\to\mathbb{F}_2^n$ and $A:\mathbb{F}_2^n\to\mathbb{F}_2^m$, with A_1 and A_2 bijective. Let $c_1=A_1(0)$ and $c=A(0)$ so that $L_1(x)=A_1(x)+c_1$ and $L(x)=A(x)+c$ are the linear parts of A_1 and A, respectively. We note that if $A_1\circ F\circ A_2+A=G$, then also $A_1'\circ F\circ A_2+A'=G$ where $A_1'(x)=A_1(x)+\Delta$ and $A'(x)=A(x)+\Delta$ for any $\Delta\in\mathbb{F}_2^m$. In particular, we can always assume that $c_1=0$ without loss of generality, so that A_1 is linear. In the following, we will write simply $G=L_1\circ F\circ A_2+A$.

By Proposition 1, for even values of k, we have

$$\Sigma_k^G(0)=\{L_1(a):a\in\Sigma_k^F(0)\}.$$

Besides justifying that the multiset of multiplicities of $\Sigma_k^F(0)$ is an EA-invariant for any positive even integer k, the above relation gives us some information about L_1; namely, it implies that if $L_1(x)=y$ for some $x,y\in\mathbb{F}_2^m$, then the multiplicity of x in

$\Sigma_k^F(0)$ should be the same as that of y in $\Sigma_k^G(0)$. If the elements of $\mathbb{F}_2^m$ are partitioned according to the multiplicities of F as

$$\mathbb{F}_2^m = K_1 \oplus K_2 \oplus \cdots \oplus K_s$$

for some positive integer s, so that all elements in K_i for every $1 \leq i \leq s$ have the same multiplicity in $\Sigma_k^F(0)$, and elements in K_i and K_j have distinct multiplicities for $i \neq j$; and, similarly, as

$$\mathbb{F}_2^m = C_1 \oplus C_2 \oplus \cdots \oplus C_s$$

according to the multiplicities of G, then we must have

$$L_1(K_i) = C_i$$

for all $1 \leq i \leq s$. We will say that any permutation L_1 satisfying $L_1(K_i) = C_i$ for all i *respects* the two partitions of $\mathbb{F}_2^m$. Consequently, we obtain conditions that can be used to restrict the possible choices for L_1. Intuitively, the larger the number of classes s in the partition of $\mathbb{F}_2^m$, the fewer linear permutations L_1 can satisfy the conditions thus obtained. In particular, if all elements of $\mathbb{F}_2^m$ occur with the same multiplicity, we do not obtain any information on L_1. This is clearly the case when F is a permutation. Furthermore, the same appears to be true for all APN (n, n)-functions with odd n (regardless of whether they are permutations or not), which is why we concentrate on fields of even extension degree in our work.

All linear permutations L respecting the partitions $\mathbb{F}_2^m = K_1 \oplus \cdots \oplus K_s$ and $\mathbb{F}_2^m = C_1 \oplus \cdots \oplus C_s$ can now be found by trying to guess the values of L on a basis of $\mathbb{F}_2^m$, and backtracking whenever some assignment violates these partitions. An algorithmic description of this procedure is provided below under Algorithm 1 and Algorithm 2. The former presents the general framework for partitioning $\mathbb{F}_2^m$ according to the multiplicities of sums of values of F and G, while the latter describes the process of reconstructing all linear permutations that respect the constructed partitions. We remark that the algorithm is described for the particular case of $k = 4$ (which is what we have mostly used in practice for our computational experiments), but the principle trivially generalizes to any value of k. We also note that computing the number $M_k^F(0, s)$ of k-tuples whose values under F add up to a given $s \in \mathbb{F}_2^m$ can be done via the values of the Walsh transform as described in Proposition 3; this is particularly useful if the selected value of k is large, or if a precomputed table of the Walsh coefficients for one (or both) of the tested functions is available.

Let us take a closer look at Algorithm 1. We first fix an even value of k, for instance $k = 4$. Given two (n, n)-functions, F and G, that we would like to test for equivalence, we begin by computing the multiplicities of the elements in the multisets $\Sigma_k^F(0)$ and $\Sigma_k^G(0)$. The number of times that the element $s \in \mathbb{F}_2^m$ appears in $\Sigma_k^F(0)$ is denoted by $M_k^F(0, s)$ (this means that $M_k^F(0, s)$ k-tuples $(x_1, x_2, \ldots x_k)$ with $x_1 + x_2 + \cdots + x_k = 0$ satisfy $F(x_1) + F(x_2) + \cdots + F(x_k) = s$).

Using these multiplicities, we partition $\mathbb{F}_2^m$ in two ways: using the multiplicities $\{M_k^F(0, s) : s \in \mathbb{F}_2^m\}$, and using the multiplicities $\{M_k^G(0, s) : s \in \mathbb{F}_2^m\}$. More precisely, we write $\mathbb{F}_2^m$ as $\mathbb{F}_2^m = K_1 \oplus K_2 \oplus \cdots \oplus K_s$, with $K_1, K_2, \ldots, K_s$ being disjoint sets of elements; two elements s_1 and s_2 are in the same block K_i of the partition if and only if $M_k^F(0, s_1) = M_k^F(0, s_2)$, i.e. if s_1 and s_2 occur with the same multiplicity

in $\Sigma_k^F(0)$. Equivalently, we could say that the multiplicities $M_k^F(0,s)$ induce an equivalence relation, in which two elements $s_1, s_2 \in \mathbb{F}_2^m$ are equivalent precisely when $M_k^F(0,s_1) = M_k^F(0,s_2)$; the blocks $K_1, K_2, \ldots, K_s$ are then the equivalence classes of this equivalence relation. In the same way that $K_1, K_2, \ldots, K_s$ is the partition induced by $\Sigma_k^F(0)$, $C_1, C_2, \ldots, C_{s'}$ is the partition induced by $\Sigma_k^G(0)$.

If F and G are EA-equivalent, then the number of blocks in both partitions must be the same, and the individual blocks must have the same sizes. Thus, if $s \neq s'$, or if the multiset $\{\#K_i : i = 1, 2, \ldots, s\}$ is not equal to $\{\#C_i : i = 1, 2, \ldots, s\}$, we can immediately conclude that F and G are not EA-equivalent. Otherwise, we can rearrange the blocks $K_1, K_2, \ldots, K_s$ and $C_1, C_2, \ldots, C_s$ in such a way that $\#K_i = \#C_i$ for $i = 1, 2, \ldots, s$. At this point, we know that if F and G are equivalent via $L_1 \circ F \circ A_2 + A = G$, then L_1 must map K_i to C_i for $i = 1, 2, \ldots s$. This additional information allows us to significantly reduce the number of linear permutations L_1 that needs to be considered.

The set of all linear permutations preserving the partitions can be found using Algorithm 2. The latter is essentially an exhaustive search that tries to guess the values of L_1 on a basis $B = \{b_1, b_2, \ldots, b_m\}$ of $\mathbb{F}_2^m$. After we have guessed the values of L_1 on $b_1, b_2, \ldots, b_i$ for some $i \leq m$, we know the values of L_1 on all elements of $\mathbb{F}_2^m$ generated by $\{b_1, b_2, \ldots, b_i\}$. For any such element x, we can find the indices j, j' such that $x \in K_j$ and $L_1(x) \in C_{j'}$. If $j \neq j'$, then L_1 does not respect the partitions, and so we backtrack, attempting a different guess for b_i. If we do not find any contradiction of this type, we proceed to guessing the value of b_{i+1}. We continue in this manner until we have exhausted all possibilities.

The partitions $\mathbb{F}_2^m = K_1 \oplus K_2 \oplus \cdots \oplus K_s$ can be precomputed for representatives from e.g. all known EA-classes of APN functions; in particular, we refer to our computational results described in Section V where we describe how we provide such pre-computed results for all currently known APN functions over $\mathbb{F}_{2^n}$ up to dimension $n = 10$. When using Algorithms 1 and 2 to find all possibilities for the outer permutation L_1 in $L_1 \circ F \circ A_2 + A = G$, however, we need to know the partitions according to both F and G, which makes the precomputation of the permutations L_1 impossible.

Nonetheless, we can observe that the set of linear permutations L_1 mapping K_i to C_i for every $1 \leq i \leq s$ is simply a coset in the symmetric group of $\mathbb{F}_2^m$ of the subgroup of linear permutations mapping K_i to K_i for $1 \leq i \leq s$. The latter can be precomputed for known EA-representatives, and hence finding a single linear permutation mapping every K_i to C_i with $1 \leq i \leq s$ allows us to reconstruct all such permutations by composing it with the precomputed ones. This can be formalized as follows.

Proposition 4. Let n be a positive integer, and $\mathbb{F}_2^n = K_1 \oplus K_2 \oplus \cdots \oplus K_s$ and $\mathbb{F}_2^n = C_1 \oplus C_2 \oplus \cdots \oplus C_s$ be two partitions of the elements of $\mathbb{F}_2^n$ such that $\#K_i = \#C_i$ for every $1 \leq i \leq s$. Let $\mathcal{K}$ be the set of all linear permutations L of $\mathbb{F}_2^n$ such that $L(K_i) = K_i$ for all $1 \leq i \leq s$, and let $\mathcal{P}$ be the set of all linear permutations L of $\mathbb{F}_2^n$ such that $L(K_i) = C_i$ for $1 \leq i \leq s$. Then $\mathcal{K}$ is a subgroup of the symmetric group of $\mathbb{F}_2^n$, and $\mathcal{P}$ is a coset of $\mathcal{K}$.

Proof. The composition of two linear permutations is clearly a linear permutation itself, and so is the inverse of a linear permutation. Furthermore, if L_1 and L_2 are linear permutations that permute some set $K_i \subseteq \mathbb{F}_2^n$, then their composition and their

Algorithm 1: General framework for reconstructing the outer permutation

Input : Two (n, m)-functions F and G
Output: All linear permutations L_1 of $\mathbb{F}_2^m$ respecting the partitions induced by F and G
for $s \in \mathbb{F}_2^m$ **do**
  compute the number $M_4^F(0, s)$ of $(x_1, x_2, x_3, x_1 + x_2 + x_3) \in \mathcal{T}_4(0)$ such that $F(x_1) + F(x_2) + F(x_3) + F(x_1 + x_2 + x_3) = s$;
  compute the number $M_4^G(0, s)$ of $(x_1, x_2, x_3, x_1 + x_2 + x_3) \in \mathcal{T}_4(0)$ such that $G(x_1) + G(x_2) + G(x_3) + G(x_1 + x_2 + x_3) = s$;
end
partition $\mathbb{F}_2^m = K_1 \oplus K_2 \oplus \cdots \oplus K_s$ so that $M_4^F(0, s_1) = M_4^F(0, s_2)$ for $s_1 \in K_i$ and $s_2 \in K_j$ if and only if $i = j$;
partition $\mathbb{F}_2^m = C_1 \oplus C_2 \oplus \cdots \oplus C_{s'}$ so that $M_4^G(0, s_1) = M_4^G(0, s_2)$ for $s_1 \in C_i$ and $s_2 \in C_j$ if and only if $i = j$;
if $s \neq s'$ **then**
  return $\emptyset$
end
rearrange $C_1, C_2, \ldots, C_s$ if necessary so that $M_4^F(0, s_1) = M_4^G(0, s_2)$ where $s_1 \in K_i$, $s_2 \in C_i$ for any $1 \leq i \leq s$;
if $\#C_i \neq \#K_i$ *for some* i *in* $1 \leq i \leq s$ **then**
  return $\emptyset$
end
select $\mathcal{I} \subseteq \{1, \ldots, s\}$ such that $U = \bigcup_{i \in \mathcal{I}} K_i$ contains a basis $B = \{b_1, \ldots, b_m\}$ of $\mathbb{F}_2^m$ and $\#U$ is as small as possible ;
return *all linear permutations* L_1 *of* $\mathbb{F}_{2^n}$ *mapping* K_i *to* C_i *for* $1 \leq i \leq s$ *as per Algorithm 2*

inverses do so as well. Thus, $\mathcal{K}$ is closed under composition and taking inverses, and is a subgroup of the symmetric group of $\mathbb{F}_2^n$.

Now, suppose that L is a linear permutation of $\mathbb{F}_2^n$ mapping some subset $K_i \subseteq \mathbb{F}_2^n$ onto some $C_i \subseteq \mathbb{F}_2^n$. Then $K \circ L$ is also a linear permutation mapping K_i onto C_i for any $K \in \mathcal{K}$. Thus, $K \mapsto K \circ L$ maps $\mathcal{K}$ to $\mathcal{P}$, and is clearly invertible since L is a permutation. Consequently, $\mathcal{P}$ is a coset of $\mathcal{K}$ represented by L. □

Besides delegating a large portion of the work in constructing $\mathcal{P}$ to the precomputation of $\mathcal{K}$, Proposition 4 allows us to estimate the complexity of testing EA-equivalence between a function F (which we can assume is a known EA-representative) and another function G inducing a partition of $\mathbb{F}_2^m$ compatible with the one induced by F.

Furthermore, it is clear that the size of the group $\mathcal{K}$ of linear permutations that preserve the partition $\mathbb{F}_2^m = K_1 \oplus \cdots \oplus K_s$ induced by the multiplicities in $\Sigma_F^k(0)$ is an EA-invariant. What makes this interesting, is that it is more discriminating than the sizes of the partition classes: for instance, the APN functions $F(x) = x^3$ and $G(x) = x^3 + \alpha^{11}x^6 + \alpha x^9$ over $\mathbb{F}_{2^6}$ (where α is primitive in $\mathbb{F}_{2^6}$) both partition $\mathbb{F}_{2^6}$ into three classes of size 1, 21, and 42, respectively; but the group of linear permutations preserving the partition of $F(x)$ contains 1008 elements, while the group of linear permutations preserving the partition of G has 336 elements. Thus, precomputing the groups $\mathcal{K}$ of linear permutations preserving the partition for representatives from the

Algorithm 2: Finding all linear permutations respecting a pair of partitions

Input : Two partitions $\mathbb{F}_2^m = K_1 \oplus K_2 \oplus \cdots \oplus K_s$ and $\mathbb{F}_2^m = C_1 \oplus C_2 \oplus \cdots \oplus C_s$ of the vector space $\mathbb{F}_2^m$, a basis $B = \{b_1, b_2, \cdots, b_m\}$ of $\mathbb{F}_2^m$, and a set U of possible values for the images of B

Output: All linear permutations L_1 of $\mathbb{F}_2^m$ such that $L_1(K_i) = C_i$ for $1 \leq i \leq s$

Set $L_1(0) \leftarrow 0$;
return $assign(1)$

procedure assign(i) ;
if $i = m + 1$ **then**
  return $\{L_1\}$;
end
$Results \leftarrow \emptyset$;
for $c_i \in U$ **do**
  $partitionPreserved \leftarrow true$;
  for $x \in \mathrm{Span}(\{b_1, \cdots, b_{i-1}\})$ **do**
    $L_1(x + b_i) \leftarrow L_1(x) + c_i$;
    find j such that $x + b_i \in K_j$;
    if $L_1(x + b_i) \notin L_j$ **then**
      $partitionPreserved \leftarrow false$;
      break ;
    end
  end
  if $partitionPreserved$ **then**
    $Results \leftarrow Results \cup assign(i + 1)$;
  end
end
return $Results$

known classes of APN functions has the additional advantage that it allows us to rule out equivalence in more cases (using a stronger invariant). We note that the actual elements of the group $\mathcal{K}$ are not, in general, invariant under EA-equivalence.

To give some basic idea of how efficient these processes are, we have computed the groups $\mathcal{K}$ for representatives from all switching classes of APN functions over $\mathbb{F}_{2^n}$ with $n \in \{6, 8\}$ [18]. The results are presented in Table I below. The first column gives the dimension n of $\mathbb{F}_{2^n}$. The functions are indexed in the second column in the same way as in [18]. The next two columns give the time in seconds for computing the partition of $\mathbb{F}_{2^n}$ according to the quadruple sums of F directly and using the Walsh transform, respectively (including the time in seconds for precomputing the Walsh coefficients). The following column gives the time for computing all linear permutations preserving the corresponding partition. The last column gives the number of linear permutations found in each case, which is a direct measure of the complexity of an EA-equivalence test by our method, as the approach for guessing the inner permutation (described in the following Section IV) has to be applied to every possible choice of the outer permutation.

We note that the running times are highly dependent on the programming language, implementation, and computational equipment used, and the ones presented in the paper are given only for illustrative purposes.

n	ID	Sums	Walsh	Time	Permutations
6	1.1	1.650	1.250	1.030	1008
	1.2	1.510	1.390	0.300	336
	2.1	1.390	1.450	0.010	10
	2.2	1.250	1.250	0.380	336
	2.3	1.240	1.450	0.970	1008
	2.4	1.260	1.250	0.010	8
	2.5	1.300	1.310	0.050	60
	2.6	1.260	1.290	0.010	8
	2.7	1.310	1.290	0.010	10
	2.8	1.310	1.310	0.010	8
	2.9	1.300	1.310	0.010	7
	2.10	1.580	1.300	0.010	8
	2.11	1.290	1.290	0.000	8
	2.12	2.450	2.470	0.030	48
8	1.1	103.580	74.910	23.090	680
	1.2	92.140	86.570	206.830	680
	1.3	244.540	238.560	78.180	8
	1.4	146.520	140.710	12.530	8
	1.5	112.860	107.580	58.300	4
	1.6	111.810	106.920	62.580	4
	1.7	127.330	121.320	10.020	1
	1.8	126.210	121.740	26.670	4
	1.9	127.250	121.730	40.370	4
	1.10	127.090	121.270	10.400	2
	1.11	127.410	122.560	50.560	4
	1.12	127.950	121.240	46.520	4
	1.13	127.850	122.320	10.530	2
	1.14	132.900	127.100	0.010	2
	1.15	126.410	121.940	22.580	1
	1.16	127.020	121.040	9.970	2
	1.17	126.860	120.790	69.860	2
	2.1	99.690	94.340	27.380	360
	3.1	118.870	112.990	57.480	4
	4.1	115.700	110.040	0.070	16
	5.1	102.470	96.640	0.030	8
	6.1	110.940	105.610	0.040	8
	7.1	98.650	93.330	49.350	680

TABLE I: Computational experiments for finding the outer permutation

For comparison, there are 27998208 linear permutations of $\mathbb{F}_{2^6}$, and 132640470466560 linear permutations of $\mathbb{F}_{2^8}$.

IV. Guessing the inner permutation

If, in addition to the (n, m)-functions F and G, we know the linear permutation L_1 in the relation $L_1 \circ F \circ A_2 + A = G$, we can apply its inverse, L_1^{-1} to both sides, obtaining

$$F \circ A_2 + A' = G', \tag{3}$$

where $A' = L_1^{-1} \circ A$ and $G' = L_1^{-1} \circ G$. A pair of affine (n, m)-functions A_2, A' satisfying the above relation then exists if and only if F is EA-equivalent to G.

Once again, let us write $c = A'(0)$ and $c_2 = A_2(0)$, and $L_2 = A_2 + c_2$ and $A = L + c$ for the linear parts of A_2 and A, respectively. Substituting 0 for x in (3) yields $F(c_2) + c = G'(0)$. Since we know G', and hence also $G'(0)$, this means that any choice of c_2 uniquely determines c. It is thus enough to loop over all possible choices of $c_2 \in \mathbb{F}_2^n$ and take $c = F(c_2)+G'(0)$ in order to exhaust all possibilities for (c_2, c'). As observed in Proposition 2, if F and G are quadratic, then we can assume that $c_2 = 0$

and $c = G'(0)$ without loss of generality; for functions of higher algebraic degree, we have to consider all possible values of c_2. In the following, we assume that we have guessed the constants c_2 and c, and rewrite (3) as

$$F \circ L_2 + L' = G'', \tag{4}$$

where $G''(x) = G'(x + c_2) + c$. It now remains to look for a pair of functions $L_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$ satisfying (4).

To guess the permutation L_2, we observe that, given some k-tuple $(x_1, x_2, \cdots, x_k) \in \mathcal{T}_k(0)$, by Proposition 1, we have

$$G''(x_1) + \cdots + G''(x_k) = F(L_2(x_1)) + \cdots + F(L_2(x_k)),$$

and thus, if some element $x_i \in \mathbb{F}_2^n$ is part of a k-tuple whose sum under G is t, then its image $L_2(x_i)$ under L_2 must be part of some k-tuple whose sum under F is t. We state this formally as follows.

Proposition 5. Let F and G be (n, m)-functions for some positive integers n, m such that $F \circ L_2 + L = G$ for L_2, L linear and L_2 bijective. Let k be a positive integer, and, for any $t \in \mathbb{F}_2^m$, denote

$$O_k^F(0, t) = \{(x_1, x_2, \cdots, x_k) \in \mathcal{T}_k(0) \mid F(x_1) + F(x_2) + \cdots + F(x_k) = t\}.$$

Then, if $(x_1, x_2, \cdots x_k) \in \mathcal{T}_k(0)$ with $G(x_1) + \cdots + G(x_k) = t$, we must have $L_2(x_i) \in M_k^F(0, t)$ for all $1 \leq i \leq k$. Consequently,

$$L_2(x) \in \bigcap_{t \in \sum_k^G(0,x)} \left(\bigcup O_k^F(0, t) \right), \tag{5}$$

where

$$\Sigma_k^G(0, x) = \{G(x_1) + \cdots + G(x_k) : (x_1, \ldots, x_k) \in \mathcal{T}_k(0) \mid x \in (x_1, \ldots x_k)\}.$$

Using (5) for $k = 3$, we can significantly reduce the *domains* of $L_2(x)$ for $x \in \mathbb{F}_2^m$, i.e. the ranges of possible values that $L_2(x)$ can take. A large number of the domains end up consisting of three elements (although we do obtain larger domains in some cases). Since guessing L_2 amounts to guessing its values on a basis of $\mathbb{F}_2^m$, the elements of the basis can be chosen in such a way that the Cartesian product of the respective domains is small. In most cases, we can indeed choose the basis elements in such a way that all domains consist of three elements, and thus end up with only 3^n possibilities for L_2.

In addition, assuming that e.g. F is a known representative, some precomputations are possible; namely, the sets $O_k^F(0, t)$ can be precomputed for $k = 3$ and all values of t. Alternatively, the roles of F and G in (4) can be swapped by composing both sides with the inverse of L_2 from the right, in which case the sets $\Sigma_k^F(0, x)$ can be precomputed for $k = 3$ and for all $x \in \mathbb{F}_2^m$.

We note that for values of k greater than 3, it seems to always be possible to express all elements in $\mathbb{F}_{2^n}$ as the sum of four values of F for an APN function F, in which case $\sum_k^G(0, x) = \mathbb{F}_2^m$ for all $x \in \mathbb{F}_2^m$, and consequently the domains of all $x \in \mathbb{F}_2^m$ end up being the entire field $\mathbb{F}_2^m$. Since the definitions of $\mathcal{T}_k(0)$ and $\sum_k^F(0)$ only make sense for values of k greater than 2, $k = 3$ remains the only practically useful choice for the value of k (at least in the case of APN functions).

Algorithm 3 describes the approach for reconstructing L_2 from (3) suggested by the above considerations. The first part of the algorithm computes the domains $\mathcal{D}(x)$ for all elements $x \in \mathbb{F}_2^n$; we then know that for any $x \in \mathbb{F}_2^n$ we must have $L_2(x) \in \mathcal{D}(x)$. All domains are initially set to $\mathbb{F}_2^n$, i.e. no restrictions on the value of $L_2(x)$ is made. We then compute the sets $O_3^F(t)$ of all triples $(x_1, x_2, x_1 + x_2)$ with $F(x_1) + F(x_2) + F(x_1 + x_2) = t$. For any element y_1 belonging to a triple $(y_1, y_2, y_1 + y_2)$ with $G(y_1) + G(y_2) + G(y_1 + y_2) = t$, we know that $L_2(y_1)$ must belong to $O_3^F(t)$; we use this to reduce the domain $\mathcal{D}(y_1)$ of y_1.

Having computed the domains, the second part of the algorithm consists of finding a basis $B = \{b_1, b_2, \ldots, b_n\}$ of $\mathbb{F}_2^n$, and constructing all linear permutations L_2 for which $L_2(b_i) \in \mathcal{D}(b_i)$ for $i = 1, 2, \ldots, n$. Since we assume that $F \circ A_2 + A = G$ (with $A_2 = L_2 + c_2$, where we also guess the value of c_2 by going through all possibilities), if the choice of L_2 is correct, then $A = F \circ A_2 + G$ must be affine. For every possible of choice of L_2 and c_2, we thus compute A and check whether its algebraic degree is at most 1; if so, then we have found the equivalence between F and G.

Recall that by Proposition 2 we can assume that $c_2 = 0$ if the functions being tested for equivalence are quadratic, which significantly reduces the computation time.

We note that Algorithm 3 will return all affine permutations A_2 for which $A = F \circ A_2 + G$ is affine. If our goal is to check whether such a permutation exists (which is all that we need for the purposes of the EA-equivalence test), we can immediately terminate as soon as a single such permutation is found. Furthermore, we remark that if (3) is obtained by applying the inverse L_1^{-1} of the outer permutation, and a solution (A_2, A) of (3) is found, then this already witnesses that F and G are EA-equivalent.

In order to get an idea of the efficiency of this method, we once again run a number of experiments on representatives from the known APN functions for $n = 6$ and $n = 8$. For every pair (F, G) of representatives from the switching classes in [18], we generate a random affine permutation A_2 and a random affine function A, and use Algorithm 3 to attempt to reconstruct A_2 and A from F and G. In the cases when F and G are not EA-equivalent this, of course, will fail; in the remaining cases (when F and G do belong to the same EA-equivalence class), we stop as soon as we find the first pair of affine functions (A_2, A) solving $F \circ A_2 + A = G$. For each combination of F and G, we generate 10 pairs of (A_2, A). Table II gives the average running time for solving $F \circ A_2 + A = G$ for dimensions $n = 8$. There are 23 switching APN representatives in $\mathbb{F}_{2^8}$, and we index them from 1 to 23 in Table II in the same order that they are listed in [18]. In the case of $n = 6$, the running time does not exceed 0.2 seconds in the worst case; we omit a detailed table of the running times for the sake of brevity. The running times are given in seconds, multiplied by a factor of 100; e.g. deciding that $F \circ A_2 + A = G$ is unsolvable when F is 1.1 and G is 1.2 from [18] takes 7.51 seconds.

V. Computational results

A recent paper [1] introduces 12 923 new APN functions over $\mathbb{F}_{2^8}$, in addition to the more than 8000 instances previously found and documented in [28]. For the purposes of measuring how efficient the multiplicities of the elements in $\Sigma_k^F(0)$ are as an invariant, and for speeding-up potential EA-equivalence tests, we have computed the exact partitions for $k = 4$ for all of these functions. We also perform similar

Algorithm 3: Reconstructing the inner permutation A_2

Input : Two (n, m)-functions F and G with $F(0) = G(0) = 0$
Output: All affine permutations A_2 of $\mathbb{F}_2^m$ such that $F \circ A_2 + G$ is affine
for $x \in \mathbb{F}_{2^n}$ **do**
  $\mathcal{D}(x) \leftarrow \mathbb{F}_{2^n}$ (initialize domains) ;
  $O_3^F(x) \leftarrow \emptyset$;
end
for $(x_1, x_2) \in (\mathbb{F}_2^m)^2$ **do**
  $t \leftarrow F(x_1) + F(x_2) + F(x_1 + x_2)$;
  $O_3^F(t) \leftarrow O_3^F(t) \cup (x_1, x_2, x_1 + x_2)$;
end
for $(x_1, x_2) \in (\mathbb{F}_2^m)^2$ **do**
  $t \leftarrow G(x_1) + G(x_2) + G(x_1 + x_2)$;
  $\mathcal{D}(x_1) \leftarrow \mathcal{D}(x_1) \cap O_3^F(t)$;
  $\mathcal{D}(x_2) \leftarrow \mathcal{D}(x_2) \cap O_3^F(t)$;
  $\mathcal{D}(x_1 + x_2) \leftarrow \mathcal{D}(x_1 + x_2) \cap O_3^F(t)$;
end
Order the elements $x \in \mathbb{F}_2^m$ into x_i for $1 \le i \le 2^n$, so that
 $i < j \implies \#\mathcal{D}(x_i) \le \#\mathcal{D}(x_j)$;
$B \leftarrow \emptyset$ (basis) ;
$Results \leftarrow \emptyset$;
for $i = 1, 2, \ldots, 2^m$ **do**
  if $x_i \notin \mathrm{Span}(B)$ **then**
    $B \leftarrow B \cup \{x_i\}$;
    if $\#B = m$ **then**
      break ;
    end
  end
end
for $c_2 \in \mathbb{F}_2^m$ **do**
  for $(v_1, v_2, \ldots, v_n) \in \prod_{x \in B} \mathcal{D}(x)$ **do**
    Let L_2 be linear with $L_2(b_i) = v_i$ for $B = (b_1, \ldots, b_m)$;
    $A_2 \leftarrow L_2 + c_2$;
    $A \leftarrow F \circ A_2 + G$;
    if $\deg(A) \le 1$ **then**
      $Results \leftarrow Results \cup \{(A_2, A + F(c_2))\}$;
    end
  end
end
return $Results$

computations for all known APN functions up to dimension $n = 10$. A complete list of these partitions is available online at https://boolean.h.uib.no/mediawiki. Here, we give a summary of the computed data.

In total, we have computed the partition induced by $\Sigma_k^F(0)$ for 21105 CCZ-inequivalent functions F. From these, we have obtained 19300 distinct partitions. Of these, the "Gold-like" partition (which splits the field into three partition classes, of size 1, 70, and 185, respectively) is the most frequently occurring, and is induced by 21 functions

	1	2	3	4	5	6	7	8	9	10	11	12
1	60	751	749	751	751	751	751	751	750	751	753	751
2	739	59	744	743	742	743	743	743	745	745	742	742
3	809	809	106	808	808	808	810	829	818	807	814	832
4	775	776	778	77	778	785	786	784	809	782	789	778
5	766	766	766	767	66	766	766	766	766	788	769	769
6	775	773	769	769	768	66	769	773	768	769	769	769
7	779	778	778	777	779	778	73	778	778	778	777	778
8	778	779	779	779	778	779	778	73	835	771	772	774
9	777	776	776	776	776	776	776	776	73	776	776	776
10	773	774	774	775	776	774	780	781	776	73	775	776
11	778	775	775	775	777	774	774	774	773	774	73	774
12	782	776	776	776	776	777	777	776	776	776	777	73
13	774	775	776	773	771	769	769	770	770	769	770	769
14	782	783	783	783	783	786	781	785	786	784	783	785
15	778	773	781	779	773	775	775	774	775	775	774	774
16	775	775	775	775	775	775	775	776	776	775	775	776
17	778	778	778	778	778	778	778	778	778	778	778	777
18	766	766	766	767	766	766	779	782	772	766	766	768
19	767	767	766	767	767	767	767	767	767	766	767	767
20	779	779	779	778	779	779	778	779	778	778	778	778
21	770	770	770	770	770	770	770	770	770	770	770	770
22	769	769	769	769	769	769	769	769	769	768	769	769
23	753	753	753	754	754	753	753	754	754	753	754	753

	13	14	15	16	17	18	19	20	21	22	23	
1	751	751	752	752	751	752	751	751	751	752	916	
2	741	743	743	741	742	743	743	743	743	743	909	
3	812	810	813	815	809	809	809	809	809	809	971	
4	779	779	779	780	776	775	776	776	776	776	941	
5	773	772	770	772	769	770	769	769	772	771	942	
6	772	770	772	771	771	917	786	791	814	797	941	
7	777	777	776	779	778	778	779	778	776	779	972	
8	823	775	833	772	772	772	771	771	772	771	937	
9	776	775	776	783	793	780	776	778	774	774	939	
10	775	776	776	776	776	774	775	776	775	775	942	
11	778	775	775	775	775	775	775	775	775	775	941	
12	776	776	778	776	776	776	776	776	776	776	952	
13	72	770	769	770	769	769	769	780	781	787	940	
14	789	75	781	789	781	785	785	784	781	782	949	
15	775	774	73	773	773	775	774	777	773	777	942	
16	776	777	773	72	773	773	773	775	773	773	943	
17	777	777	777	778	73	777	778	777	779	775	942	
18	766	765	770	766	766	63	765	763	766	764	931	
19	767	767	767	767	767	769	68	767	767	775	936	
20	778	778	778	779	779	778	779	67	780	774	940	
21	770	769	770	770	770	769	770	770	63	770	937	
22	769	769	769	769	769	768	769	781	769	65	934	
23	753	753	753	753	753	753	753	753	752	753	918	

TABLE II: Computation time for reconstructing the inner permutation for $n = 8$

including, of course, the Gold function x^3. The number of partitions that occur only once is 18103; and the remaining partitions occur between two and eleven times.

Most of the partitions contain a large number of classes: indeed, only the "Gold-like" partition described above has three classes, while all other observed partitions have at least 6 classes; the vast majority of functions induce a partition having between 12 and 16 classes, while the largest number of classes, 22, is achieved by only two functions. We recall that a large number of classes intuitively corresponds to a small number of linear permutations respecting the corresponding partition, and consequently to a faster test for EA-equivalence.

In the case of $n = 10$, we only observe the "Gold-like" partition for all the ten known representatives from the infinite families. However, among the five new functions given in the dataset accompanying [1], we find three that have different (and pairwise distinct) spectra.

For odd dimensions ($n = 7$ and $n = 9$), we also compute the partitions induced by the known APN representatives, but these always yield a trivial partition of $\mathbb{F}_{2^n}$ into a zero and non-zero elements (even when we take into account the newly discovered APN classes from [1]).

VI. Conclusion

We have introduced a family of invariants under EA-equivalence, and have shown how their values can be efficiently computed using the Walsh transform. We have experimentally observed that over $\mathbb{F}_{2^n}$ with even n, these invariants can be used to partition quadratic APN functions into small subclasses, thereby significantly facilitating their classification up to EA- and CCZ-equivalence. We have demonstrated how the values of these invariants can be used to restrict the values of the outer permutation A_1 in the relation $A_1 \circ F \circ A_2 + A = G$ for two given (n, m)-functions F and G, and have ran experiments in order to measure how much this approach reduces the search space. We have described how a variation of the same invariants can be used to restrict the values of the images of $\mathbb{F}_{2^n}$ under the inner permutation, A_2, and have combined the above into a computational test for deciding the EA-equivalence of any two (n, m)-functions F and G. Although slower than the standard test for CCZ-equivalence via the permutation equivalence of linear codes, our approach has the advantage that it is easily implementable on any programming language, and can be separated into a multitude of small, independent steps with concrete output, the majority of which can be naturally parallelized and run in different processes or on different computers. Furthermore, this is, to the best of our knowledge, the first efficient algorithm for directly testing the EA-equivalence of two given functions.

One direction for future work would be to investigate the invariants described in Section II more closely, and see whether they can be modified in order to provide more efficient restrictions. In the same vein, it would be interesting to investigate the functions for which our experimental results show a large number of choices for the outer permutation A_1 following the restriction described in Section III, and to see whether some of these choices can be ruled out using some other criterion; this would directly impact the efficiency of the entire EA-equivalence test for these functions.

So far, we have implemented the algorithms described in Section III and IV in the *Magma* programming language [5] due to the ease of implementation. As pointed out above, our approach is quite simple, and does not depend on anything more complicated than computing linear combinations of binary vectors, and so it should be readily implementable in any general-purpose programming language. We expect that a careful implementation in an efficient language would further reduce the computational time needed for testing EA-equivalence, and make the method even more useful in practice.

Acknowledgements

This research is supported by the Trond Mohn foundation. The author would like to thank the anonymous reviewers for their careful proofreading and helpful remarks.

References

[1] Christof Beierle and Gregor Leander. “New Instances of Quadratic APN Functions.” arXiv preprint arXiv:2009.07204 (2020).

[2] Thomas Beth and Cunsheng Ding. “On almost perfect nonlinear permutations.” Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.

[3] Eli Biham and Adi Shamir. “Differential cryptanalysis of DES-like cryptosystems.” Journal of CRYPTOLOGY 4.1 (1991): 3-72.

[4] Alex Biryukov, Christophe De Cannière, An Braeken and Bart Preneel. “A toolbox for cryptanalysis: Linear and affine equivalence algorithms.” International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2003.
[5] Wieb Bosma, John Cannon and Catherine Playoust. “The Magma algebra system I: The user language.” Journal of Symbolic Computation 24.3-4 (1997): 235-265.
[6] Marcus Brinkmann and Gregor Leander. “On the classification of APN functions up to dimension five.” Designs, Codes and Cryptography 49.1-3 (2008): 273-288.
[7] K. Browning, J. Dillon, R. Kibler and M. McQuistan. “APN polynomials and related codes.” Special volume of Journal of Combinatorics, Information and System Sciences 34 (2009): 135-159.
[8] Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Nikolay Kaleyski. “On the distance between APN functions.” IEEE Transactions on Information Theory (2020).
[9] Lilya Budaghyan, Claude Carlet, and Alexander Pott. “New classes of almost bent and almost perfect nonlinear polynomials.” IEEE Transactions on Information Theory 52.3 (2006): 1141-1152.
[10] Lilya Budaghyan and Oleksandr Kazymyrov. “Verification of restricted EA-equivalence for vectorial boolean functions.” International Workshop on the Arithmetic of Finite Fields. Springer, Berlin, Heidelberg, 2012.
[11] Claude Carlet, Pascale Charpin, and Victor Zinoviev. “Codes, bent functions and permutations suitable for DES-like cryptosystems.” Designs, Codes and Cryptography 15.2 (1998): 125-156.
[12] Itai Dinur, and Adi Shamir. “Breaking Grain-128 with dynamic cube attacks.” International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2011.
[13] Joan Daemen and Vincent Rijmen. “The design of Rijndael: AES-the advanced encryption standard.” Springer Science & Business Media, 2013.
[14] Ulrich Dempwolff. “CCZ equivalence of power functions.” Designs, Codes and Cryptography 86.3 (2018): 665-692.
[15] Hans Dobbertin. “Almost perfect nonlinear power functions on GF (2/sup n/): the Welch case.” IEEE Transactions on Information Theory 45.4 (1999): 1271-1275.
[16] Hans Dobbertin. “Almost perfect nonlinear power functions on GF (2n): the Niho case.” Information and Computation 151.1-2 (1999): 57-72.
[17] Hans Dobbertin. “Almost perfect nonlinear power functions on GF (2 n): a new case for n divisible by 5.” Finite Fields and Applications. Springer, Berlin, Heidelberg, 2001. 113-121.
[18] Yves Edel and Alexander Pott. “A new almost perfect nonlinear function which is not quadratic.” Adv. in Math. of Comm. 3.1 (2009): 59-81.
[19] Yves Edel and Alexander Pott. “On the equivalence of nonlinear functions.” Enhancibng cryptographic primitives with techniques from error correcting codes. Vol. 23. NATO Sci. Peace Secur. Ser. D. Inf. Commun. Secur. Amsterdam: IOS (2009): 87-103.
[20] Robert Gold. “Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.).” IEEE transactions on Information Theory 14.1 (1968): 154-156.
[21] Heeralal Janwa and Richard M. Wilson. “Hyperplane sections of Fermat varieties in P 3 in char. 2 and some applications to cyclic codes.” International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. Springer, Berlin, Heidelberg, 1993.
[22] Tadao Kasami. “The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes.” Information and Control 18.4 (1971): 369-394.
[23] Lars R. Knudsen. “Truncated and higher order differentials.” International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1994.
[24] Mitsuru Matsui. “Linear cryptanalysis method for DES cipher.” Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.
[25] Kaisa Nyberg. “Differentially uniform mappings for cryptography.” Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.
[26] Ferruh Özbudak, Ahmet Sınak, and Oğuz Yayla. “On verification of restricted extended affine equivalence of vectorial boolean functions.” International Workshop on the Arithmetic of Finite Fields. Springer, Cham, 2014.
[27] Satoshi Yoshiara. “Equivalences of quadratic APN functions.” Journal of Algebraic Combinatorics 35.3 (2012): 461-475.
[28] Yuyin Yu, Mingsheng Wang and Yongqiang Li. “A Matrix Approach for Constructing Quadratic APN Functions.”, Cryptology ePrint Archive: Report 2013/731.

Paper VI

Generalization of a Class of APN Binomials to Gold-Like Functions

Diana Davidova, Nikolay S. Kaleyski
Lecture Notes in Computer Science, **vol. 12542, pp. 195-206**

Generalization of a class of APN binomials to Gold-like functions

Diana Davidova and Nikolay Kaleyski

Department of Informatics, University of Bergen

Abstract

In 2008 Budaghyan, Carlet and Leander generalized a known instance of an APN function over the finite field $\mathbb{F}_{2^{12}}$ and constructed two new infinite families of APN binomials over the finite field $\mathbb{F}_{2^n}$, one for n divisible by 3, and one for n divisible by 4. By relaxing conditions, the family of APN binomials for n divisible by 3 was generalized to a family of differentially 2^t-uniform functions in 2012 by Bracken, Tan and Tan; in this sense, the binomials behave in the same way as the Gold functions. In this paper, we show that when relaxing conditions on the APN binomials for n divisible by 4, they also behave in the same way as the Gold function x^{2^s+1} (with s and n not necessarily coprime). As a counterexample, we also show that a family of APN quadrinomials obtained as a generalization of a known APN instance over $\mathbb{F}_{2^{10}}$ cannot be generalized to functions with 2^t-to-1 derivatives by relaxing conditions in a similar way.

I. Introduction

Let n, m be natural numbers. A *vectorial Boolean* (n, m)*-function*, or simply an (n, m)*-function*, or vectorial Boolean function, is a mapping from the n-dimensional vector space $\mathbb{F}_2^n$ over the finite field $\mathbb{F}_2 = \{0, 1\}$ to the m-dimensional vector space $\mathbb{F}_2^m$. Since the extension field $\mathbb{F}_{2^n}$ can be identified with an n-dimensional vector space over $\mathbb{F}_2$, (n, m)-functions can be seen as functions between the Galois fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$. Vectorial Boolean functions have many applications in mathematics and computer science. In cryptography, they are the basic building blocks of block ciphers, and the choice of functions directly influences the security of the cipher. In order to construct cryptographically secure ciphers, it is necessary to understand what properties such functions need to possess in order to resist various types of cryptanalytic attacks, and to find methods for constructing functions having these desirable properties. In our work, we mostly concentrate on the case when $n = m$, i.e. when the numbers of input and output bits are the same. A comprehensive survey on (n, m)-functions can be found in [4], [8].

One of the most powerful attacks against block ciphers is differential cryptanalysis, introduced by Biham and Shamir [1]. The attack is based on studying how the difference in two inputs to a function affects the difference in the corresponding outputs. The resistance to differential attacks of an (n, m)-function is measured by a property called its differential uniformity. The lower the differential uniformity, the more resistant the cryptosystem is to differential attacks. The class of almost perfect nonlinear (APN) functions is defined as the class of (n, n)-functions having the best possible differential uniformity, and thus provides optimal security against differential cryptanalysis.

Another powerful attack against block ciphers is linear cryptanalysis, introduced by Matsui [12]. The property of a function which measures the resistance to this kind of attack is called nonlinearity. The nonlinearity $\mathcal{NL}(F)$ of an (n, m)-function F is

defined to be the minimum Hamming distance between any component of F and any affine $(n,1)$-function. An upper bound on the nonlinearity of any (n,n)-function can be derived, and the class of almost bent (AB) functions is defined as the class of those functions that meet this bound with equality and therefore provide the best possible resistance to linear attacks.

Recall that the Gold functions are APN power functions over $\mathbb{F}_{2^n}$ of the form x^{2^s+1} for some natural number s satisfying $\gcd(s,n)=1$. Relaxing the condition to $\gcd(s,n)=t$ for some positive integer t, the functions of the form $F(x)=x^{2^s+1}$ become differentially 2^t-uniform, with all their derivatives $D_aF(x)=F(x)+F(a+x)$ for $a\neq 0$ being 2^t-to-1 functions. These functions are permutations if and only if $n/\gcd(s,n)=n/t$ is odd [13], and are (2^t+1)–to–1 functions otherwise. Their nonlinearity is $2^{n-1}-2^{(n+t)/2}$ when n/t is odd, and $2^{n-1}-2^{(n+2t)/2}$ otherwise.

In 2008, two infinite families of (n, n)-APN binomials inequivalent to power functions were introduced in [5] for values of n divisible by 3 or by 4 as generalizations of a known sporadic APN instance over $\mathbb{F}_{2^{12}}$ [11]. These were the first known infinite families of APN functions that are inequivalent to power functions. It was later shown in 2012 that the family of APN binomials for n divisible by 3 can be generalized to functions with 2^t-to-1 derivatives (for some positive integer t) with nonlinearity equal to $2^{n-1}-2^{(n+t)/2}$ for $n+t$ even, and $2^{n-1}-2^{(n+t-1)/2}$ for $n+t$ odd by relaxing conditions [3]. Thus, the APN binomials for n divisible by 3 behave in the same way as the Gold functions from the point of view of differential uniformity, nonlinearity and properties of the image set.

In this paper we show that the second class of APN binomials from [5] (for n divisible by 4) also behaves in the same way as the Gold functions in this respect. We note that all the constructed functions (much like the APN binomials) are quadratic, and are therefore not directly suitable for cryptographic use in practice. Nonetheless, the vast majority of known APN functions are given by a quadratic representation, but contain representatives of higher algebraic degrees in their CCZ-equivalence class. We also consider the family of APN quadrinomials constructed by generalizing a known APN instance over $\mathbb{F}_{2^{10}}$ [7] and computationally verify that they provide a counterexample to this approach, in the sense that they cannot be generalized to functions with 2^t-to-1 derivatives by relaxing conditions in a similar way for any even dimension n in the range $6\leq n\leq 14$.

The paper is structured as follows. In Section II, we recall the basic definitions and results that we use throughout our work. In Section III, we compute the differential uniformity of the generalized families of binomials; an upper bound on their nonlinearity is then derived in Section IV. Section V, in which we computationally show that the APN quadrinomials constructed in [7] cannot be generalized to 2^t-uniform functions over $\mathbb{F}_{2^n}$ with $6\leq n\leq 14$, concludes the paper.

II. Preliminaries

Let n be a positive integer. Then $\mathbb{F}_{2^n}$ denotes the finite field with 2^n elements, and $\mathbb{F}_{2^n}^*$ denotes its multiplicative group. For any positive integer k dividing n, the trace function Tr_k^n is the mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ defined by $\mathrm{Tr}_k^n(x)=\sum_{i=0}^{\frac{n}{k}-1}x^{2^{ik}}$. For $k=1$, the function $\mathrm{Tr}_1^n:\mathbb{F}_{2^n}\to\mathbb{F}_2$ is called the *absolute trace* over $\mathbb{F}_{2^n}$ and is denoted simply by $\mathrm{Tr}_n(x)$, or by $\mathrm{Tr}(x)$ if the dimension n is clear from context.

Let n and m be positive integers. An (n,m)-*function* is any function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. For any (n,m)-function F and for any $a \in \mathbb{F}_{2^n}$, the function $D_aF(x) = F(x+a) + F(x)$ is called the *derivative of* F *in the direction* a. Let $\delta_F(a,b)$ denote the number of solutions of the equation $D_aF(x) = b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$. The multiset $\{\delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}\}$ is called the *differential spectrum* of F. The *differential uniformity* of F is the largest value in its differential spectrum. We say that F is *differentially* δ*-uniform* if its differential uniformity is at most δ. The differential uniformity of any (n,m)-function is clearly always even, since if $x \in \mathbb{F}_{2^n}$ is a solution to $D_aF(x) = b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$, then so is $x+a$. The lowest possible differential uniformity of any function is thus 2. A function with differential uniformity equal to 2 is called *almost perfect nonlinear (APN)*. Since a low differential uniformity corresponds to a strong resistance to differential cryptanalysis, APN functions provide optimal security against this type of attack.

A *component function* of an (n,m)-function F is any function of the form $x \mapsto \mathrm{Tr}_m(cF(x))$ for $c \in \mathbb{F}_{2^m}^*$. The component functions are clearly $(n,1)$-functions. The nonlinearity $\mathcal{NL}(F)$ of F is the minimum Hamming distance between any component function of F and any affine $(n,1)$-function, i.e. any function $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfying $a(x) + a(y) + a(z) = a(x+y+z)$ for all $x,y,z \in \mathbb{F}_{2^n}$. Recall that the Hamming distance between two $(n,1)$-functions f and g is the number of inputs $x \in \mathbb{F}_{2^n}$ for which $f(x) \neq g(x)$.

An important tool for analyzing any (n,m)-function F is the so-called Walsh transform. The *Walsh transform of* F is the function $W_F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^n} \to \mathbb{Z}$ defined as $W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(aF(x)) + Tr_n(bx)}$.

The nonlinearity of an (n,m)-function F can be expressed as $\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^n}} |W_F(a,b)|$. The nonlinearity of any (n,n)-function is bounded from above by $2^{n-1} - 2^{(n-1)/2}$[10]. Functions attaining this bound are called *almost bent (AB)*. Clearly, AB functions exist only for odd values of n; when n is even, functions with nonlinearity $2^{n-1} - 2^{n/2}$ are known, and it is conjectured that this value is optimal in the even case. Nonlinearity measures the resistance to linear cryptanalysis; the higher the nonlinearity, the better. Thus, AB functions provide optimal security against linear cryptanalysis when n is odd. Furthermore, all AB functions are necessarily APN [10], so that AB functions are optimal with respect to differential cryptanalysis as well.

Due to the huge number of (n,m)-functions for non-trivial values of n and m, they are typically classified up to some notion of equivalence. The most general known equivalence relation which preserves differential uniformity (and hence APN-ness) is Carlet-Charpin-Zinoviev (or CCZ) equivalence [6], [9]. We say that two (n,m)-functions F and F' are *CCZ-equivalent* if there is an affine permutation $\mathcal{A}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ that maps the graph $\mathcal{G}(F) = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph $\mathcal{G}(F')$ of F'. A special case of CCZ-equivalence is extended affine (or EA) equivalence. We say that F and F' are *EA-equivalent* if there are affine permutations A_1 and A_2 of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively, and an affine (n,m)-function A such that $F' = A_1 \circ F \circ A_2 + A$.

In [5], Budaghyan, Carlet and Leander introduced the following two infinite families of APN binomials:

1) For $n = 3k$:

$$F_3(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}}, \tag{1}$$

where s and k are positive integers such that $s \leq 4k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, $i = sk \mod 3$, $m = 3-i$ and w is a primitive element of the field $\mathbb{F}_{2^n}$.

2) For $n = 4k$:

$$F_4(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}}, \tag{2}$$

where s and k are positive integers such that $s \leq 4k-1$, $\gcd(k,2) = \gcd(s,2k) = 1$, $i = sk \mod 4$, $m = 4-i$ and w is a primitive element of the field $\mathbb{F}_{2^n}$.

The first class of APN binomials (for n divisible by 3) are permutations if and only if k is odd.

As we show below, if the condition of k being odd is omitted, the binomials for n divisible by 4 are EA-equivalent to the Gold functions. Indeed, let k be even. Then $i = sk \mod 4$ is also even. If $i = 2$, then

$$F(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}} = x^{2^s+1} + w^{2^k-1}x^{2^{2k}+2^{2k+s}} = x^{2^s+1} + w^{2^k-1}x^{2^{2k}(1+2^s)} = x^{2^s+1} + w^{2^k-1}(x^{2^s+1})^{2^{2k}}$$

which is EA-equivalent to x^{2^s+1} since $x \mapsto x + w^{2^k-1}x^{2^{2k}}$ is a linear permutation. Indeed, if $x + w^{2^k-1}x^{2^{2k}} = y + w^{2^k-1}y^{2^{2k}}$ and $x \neq y$, then we must have $w^{1-2^k} = (x+y)^{2^{2k}-1}$ which is impossible since $2^{2k}-1$ is a multiple of 5 under the hypothesis, whereas $2^k - 1$ is not.

In the same manner, if $i = 0$, we get

$$F(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}} = x^{2^s+1} + w^{2^k-1}x^{1+2^s} = x^{2^s+1}(1 + w^{2^k-1}).$$

The complete Walsh spectra of the functions F_3 and F_4 were determined in [2].

As previously mentioned, relaxing the conditions allows the functions F_3 to be generalized to a family of 2^t-differentially uniform functions in the same way as the Gold functions [3]. In this paper, we show how the family F_4 can be generalized to functions with 2^t-to-1 derivatives in a similar way. Further, we provide a counterexample to the question of whether this construction can be used to generalize any family of quadratic APN functions to a family of 2^t-uniform functions: for the family of quadrinomials from [7], we computationally verify that relaxing conditions does not lead to functions with 2^t-to-1 derivatives for $t > 1$ over $\mathbb{F}_{2^n}$ for any $6 \leq n \leq 14$.

For background on APN functions and cryptographic Boolean functions, we refer the reader to [4] or [8].

III. Differential uniformity

In the following theorem, we show that by relaxing the condition $\gcd(s,2k) = 1$ in (2) to $\gcd(s,2k) = t$ for some positive integer t, we obtain functions over $\mathbb{F}_{2^{4k}}$ all of whose derivatives are 2^t-to-1 functions.

Theorem 1. *Let s, k, t be positive integers and let $n = 4k$. Let $\gcd(s, 2k) = t$, $2 \nmid k$, $i = sk \mod 4$, $m = 4 - i$, and w be a primitive element of $\mathbb{F}_{2^n}$. Then all derivatives $D_a F$ for $a \in \mathbb{F}_{2^n}^*$ of the function*

$$F(x) = wx^{2^s+1} + w^{2^k} x^{2^{ik}+2^{mk+s}} \tag{3}$$

are 2^t-to-1 functions. In particular, F is differentially 2^t-uniform.

Proof. We first show that for i even, F is EA-equivalent to x^{2^s+1}. To see this, consider two cases depending on the value of i. First, suppose $i = 2$. Then

$$F(x) = wx^{2^s+1} + w^{2^k} x^{2^{2k}+2^{2k+s}} = wx^{2^s+1} + w^{2^k}(x^{2^s+1})^{2^{2k}}$$

which is EA-equivalent to x^{2^s+1} since $x \mapsto wx + w^{2^k} x^{2^{2k}}$ is a linear permutation. Indeed, suppose that $wx + w^{2^k} x^{2^{2k}} = wy + w^{2^k} y^{2^{2k}}$ for some two distinct elements $x, y \in \mathbb{F}_{2^n}$; then $(x + y)^{2^{2k}-1} = w^{1-2^k}$ which is a contradiction since the exponent on the left-hand side is a multiple of three, while the one on the right-hand side is not. Finally, note that the derivatives of x^{2^s+1} are all 2^t-to-1 functions since $\gcd(s, 4k) = \gcd(s, 2k) = t$.

If $i = 0$, then

$$F(x) = wx^{2^s+1} + w^{2^k} x^{1+2^{4k+s}} = wx^{2^s+1} + w^{2^k} x^{1+2^s} = x^{2^s+1}(w + w^{2^k}),$$

which is EA-equivalent to x^{2^s+1} (as w is a primitive element, we have $w + w^{2^k} \neq 0$), and hence all of its derivatives are 2^t-to-1 under the conditions on s, t and k.

We now consider the case of i odd. Both possibilities for i produce functions in the same EA-equivalence class. For $i = 1$, the function (3) takes the form

$$F(x) = wx^{2^s+1} + w^{2^k} x^{2^k+2^{3k+s}}. \tag{4}$$

Consider the function F' defined by

$$F'(x) = F(x)^{2^{3k}} = (wx^{2^s+1} + w^{2^k} x^{2^k+2^{3k+s}})^{2^{3k}} = wx^{2^{2k+s}+1} + w^{2^{3k}} x^{2^{3k}(2^s+1)}.$$

Clearly, F' is EA-equivalent to F. From the condition $ks = 1 \mod 4$ we get $k \mod 4 = s \mod 4$, i.e. $2k + s = 3s \mod 4$, hence $(2k + s)k = 3sk = 3 \mod 4$. Thus, denoting $2k + s$ by s', we get $F'(x) = wx^{2^{s'}+1} + w^{2^{-k}} x^{2^{3k}+2^{k+s'}}$, which is precisely the function from (3) for $i = 3$.

It is thus enough to prove the theorem for $i = 3$, i.e. for the function $F(x) = wx^{2^s+1} + w^{2^k} x^{2^{3k}+2^{k+s}}$.

The derivatives of F are 2^t-to-1 functions if and only if the equation $F(x) + F(x + v) = u$ has either 0 or 2^t solutions for any $u, v \in \mathbb{F}_2^n, v \neq 0$. The left-hand side of this equality takes the form

$$\begin{aligned}
&F(x) + F(x+v) = \\
&wx^{2^s+1} + w^{2^k} x^{2^{3k}+2^{k+s}} + w(x+v)^{2^s+1} + w^{2^k}(x+v)^{2^{3k}+2^{k+s}} = \\
&wx^{2^s+1} + w^{2^k} x^{2^{3k}+2^{k+s}} + wx^{2^s+1} + wv^{2^s+1} + wx^{2^s} v + wxv^{2^s} + w^{2^k} x^{2^{3k}+2^{k+s}} + \\
&w^{2^k} v^{2^{3k}+2^{k+s}} + w^{2^k} x^{2^{3k}} v^{2^{k+s}} + w^{2^k} v^{2^{3k}} x^{2^{k+s}} = \\
&wv^{2^s+1} + wx^{2^s} v + wxv^{2^s} + w^{2^k} v^{2^{3k}+2^{k+s}} + w^{2^k} x^{2^{3k}} v^{2^{k+s}} + w^{2^k} v^{2^{3k}} x^{2^{k+s}} = \\
&w^{2^k} v^{2^{3k}+2^{k+s}} \left(\left(\frac{x}{v}\right)^{2^{3k}} + \left(\frac{x}{v}\right)^{2^{k+s}} \right) + wv^{2^s+1} \left(\left(\frac{x}{v}\right)^{2^s} + \left(\frac{x}{v}\right) \right) + wv^{2^s+1} + \\
&w^{2^k} v^{2^{3k}+2^{k+s}}.
\end{aligned}$$

Dividing the last expression by wv^{2^s+1} and substituting vx for x, we get a linear expression in x:

$$a(x^{2^{3k}} + x^{2^{k+s}}) + (x^{2^s} + x) + 1 + a,$$

where $a = w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)}$. So, $F(x) + F(x+v) = u$ has 0 or 2^t solutions if and only if the kernel of the linear map

$$\Delta_a(x) = a(x^{2^{3k}} + x^{2^{k+s}}) + (x^{2^s} + x)$$

has 2^t elements. Consider the equation $\Delta_a(x) = 0$. We use Dobbertin's multivariate method and follow the computations from Theorem 2 of [5]. Let $b = a^{2^k}$ and $c = b^{2^k}$. We get that

$$\Delta_a(x) = 0 \text{ if and only if } ab(bc+1)^{2^s+1}(x^{2^{2s}} + x^{2^s}) = 0,$$

assuming that $P(a) = c(ab+1)^{2^s+1} + a^{2^s}(bc+1)^{2^s+1} \neq 0$.

We now show that $bc + 1 \neq 0$. Clearly, $bc + 1 = 0$ if and only if $ab + 1 = 0$. Suppose $ab = 1$, i.e. $a^{2^k+1} = 1$. From

$$(2^{3k} + 2^{k+s} - (2^s + 1))(2^k + 1) = (2^{2k} - 1)(2^k + 2^s) \mod (2^{4k} - 1)$$

we get

$$1 = a^{2^k+1} = (w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)})^{2^k+1} = w^{2^{2k}-1}v^{(2^{2k}-1)(2^k+2^s)} = (wv^{2^k+2^s})^{2^{2k}-1},$$

hence $wv^{2^k+2^s}$ is a $(2^{2k}+1)$-st power of an element from $\mathbb{F}_{2^n}$. On the other hand, from $ks = 3 \mod 4$ and $2 \nmid k$ we have that k and s are odd, and $k \neq s \mod 4$, which means that $k - s = 2p$ for some odd p. Thus, $2^k + 2^s = 2^s(2^{k-s} + 1) = 2^s(2^{2p} + 1)$. Since p is odd, we have $5 \mid 2^{2p} + 1$, and therefore $u^{2^k+2^s}$ is the fifth power of an element of the field, while $wu^{2^k+2^s}$ is not. Thus $wu^{2^k+2^s}$ is also not a $(2^{2k}+1)$-st power. Hence, we get a contradiction, and so we must have $ab + 1 \neq 0$ and hence $bc + 1 \neq 0$. Therefore, we have

$$\Delta_a(x) = 0 \text{ if and only if } x^{2^{2s}} + x^{2^s} = 0$$

when $P(a) \neq 0$.

By the statement of Theorem 1, k is odd and $sk = 3 \mod 4$, so that s is also odd, and from $\gcd(s, 2k) = t$ it follows that $\gcd(s, 4k) = t$. Therefore the equation $x^{2^{2s}} + x^{2^s} = 0$, which is equivalent to $x^{2^s} = 1$, has exactly $2^{\gcd(s,4k)} = 2^t$ solutions.

So we only have to show that $P(a) = c(ab+1)^{2^s+1} + a^{2^s}(bc+1)^{2^s+1}$ does not vanish.

Assume $P(a) = 0$, i.e.

$$\frac{c}{a^{2^s}} = \left(\frac{bc+1}{ab+1}\right)^{2^s+1}.$$

We have that $\frac{c}{a^{2^s}}$ is the third power of an element of the field since $3 \mid 2^s + 1, 2^n - 1$ (since s is odd and n is even). On the other hand,

$$\frac{c}{a^{2^s}} = a^{2^{2k}-2^s} = a^{2^s(2^{2k-s}-1)} = (w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)})^{2^s(2^{2k-s}-1)} = w^{(2^k-1)2^s(2^{2k-s}-1)}v^{(2^{3k}+2^{k+s}-(2^s+1))2^s(2^{2k-s}-1)}$$

and $2^{3k} + 2^{k+s} - (2^s + 1) = 2^s(2^{3k-s} - 1) + (2^{k+s} - 1)$ is divisible by 3 because $3 \mid 2^{3k-s} - 1$ and $3 \mid 2^{k+s} - 1$ due to k and s being odd. But since k and $2k - s$ are odd, we have $3 \nmid 2^k - 1$ and $3 \nmid 2^{2k-s} - 1$, which means that $w^{(2^k-1)2^s(2^{2k-s}-1)}$ is not a third power, therefore $\frac{c}{a^{2^s}}$ is not a third power either, and we get a contradiction. □

As the following proposition illustrates, the binomials from (3) also behave in the same way as the Gold functions from the point of view of bijectivity.

Proposition 1. *A function of the form* (3) *is a permutation if and only if it is EA-equivalent to a 2^t-differentially uniform permutation of the form x^{2^s+1} for some positive integer s.*

Proof. Recall that the power function x^{2^s+1} over $\mathbb{F}_{2^n}$ is 2^t-uniform for some positive integer t if and only if $\gcd(s, n) = t$, and it is a permutation if and only if n/t is odd.

Let $F(x) = wx^{2^s+1} + w^{2^k}x^{2^{ik}+2^{mk+s}}$ be a function satisfying the conditions of Theorem 1. If F is a permutation, then $4k/\gcd(s, 4k)$ is odd. Indeed, assume that F is a permutation and $4k/\gcd(s, 4k)$ is even. Since k is odd, we have that $\gcd(s, 4k)$ should be odd or $\gcd(s, 4k) = 2 \mod 4$. If $\gcd(s, 4k)$ is odd, then so is s, and therefore $3 \mid 2^s + 1$. Since $i = (sk \mod 4)$ and s, k are odd, then i is an odd number, and hence $(m - i)k + s$ is also odd; hence $3 \mid 2^{ik}(1 + 2^{(m-i)k+s}) = 2^{ik} + 2^{mk+s}$. Thus, for any $\gamma \in \mathbb{F}_{2^2}$, we have $F(\gamma x) = F(x)$. On the other hand, if $\gcd(s, 4k) = 2 \mod 4$, then s is even, and therefore i is also even due to $i = sk \mod 4$. Hence, as we discussed in the proof of Theorem 1, F is EA-equivalent to x^{2^s+1} which is not a permutation since $4k/\gcd(s, 4k)$ is even. Therefore $4k/\gcd(s, 4k)$ is necessarily odd if F is a permutation. However, when $4k/\gcd(4k, s)$ is odd, $\gcd(4k, s)$ is divisible by 4, and therefore s is also divisible by 4 since k is odd. This means that F is EA-equivalent to a 2^t-differentially uniform permutation of the form x^{2^l+1} for some positive integer l. □

IV. Magnitude of the Walsh coefficients

In following theorem, we compute an upper bound on the absolute values of the Walsh coefficients of the functions from (3). In the proof we make use of the following result.

Lemma 1 ([14])**.** *Let n, l, d be positive integers such that $\gcd(n, s) = 1$ and let $G(x) = \sum_{i=0}^{d} a_i x^{li} \in \mathbb{F}_{2^n}[x]$. Then the equation $G(x) = 0$ has at most 2^d solutions.*

We are now ready to present the main result of this section.

Theorem 2. *Let s, k, t be positive integers and let $n = 4k$. Let $\gcd(s, 2k) = t$, $2 \nmid k$, $i = sk \mod 4$, $m = 4 - i$ and let w be a primitive element of $\mathbb{F}_{2^n}$. Then the Walsh coefficients of the function F from* (3) *satisfy*

$$|W_F(a, b)| \leq 2^{2k+t}$$

for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

Proof. For simplicity, instead of $F(x) = wx^{2^s+1} + w^{2^k}x^{2^{ik}+2^{mk+s}}$, we consider the EA-equivalent function $F'(x) = x^{2^s+1} + \alpha x^{2^{ik}+2^{mk+s}}$, where $\alpha = w^{2^k-1}$.

We are going to prove the theorem for $i = 3$ since as we already observed in the proof of Theorem 1, if i is even, the function $F(x)$ is EA-equivalent to a Gold-like

differentially 2^t-uniform function; and if i is odd, the functions that we obtain for $i = 1$ and for $i = 3$ are EA-equivalent.

We have

$$W^2_{F'}(a,b) = \sum_x \sum_y (-1)^{\mathrm{Tr}(ax+ay+bF'(x)+bF'(y))}.$$

Substituting $x + y$ for y, we get

$$W^2_{F'}(a,b) = \sum_x \sum_y (-1)^{\mathrm{Tr}(ax+a(x+y)+bF'(x)+bF'(x+y))}.$$

The exponent from the previous expression by straightforward calculations becomes

$$\begin{aligned}
&\mathrm{Tr}(ax + a(x+y) + bF'(x) + bF'(x+y)) = \\
&\mathrm{Tr}(ay + b(x^{2^s+1} + \alpha x^{2^{3k}+2^{k+s}} + (x+y)^{2^s+1} + \alpha(x+y)^{2^{3k}+2^{k+s}})) = \\
&\mathrm{Tr}(ay + by^{2^s+1} + b\alpha y^{2^{k+s}+2^{3k}}) + \mathrm{Tr}(bx^{2^s}y + bxy^{2^s} + b\alpha x^{2^{3k}}y^{2^{k+s}} + b\alpha y^{2^{3k}}x^{2^{k+s}}) = \\
&\mathrm{Tr}(ay + by^{2^s+1} + b\alpha y^{2^{k+s}+2^{3k}}) + \mathrm{Tr}(x\mathcal{L}(y)),
\end{aligned}$$

where $\mathcal{L}(y) = (by)^{2^{-s}} + by^{2^s} + (b\alpha)^{2^{-3k}}y^{2^{s-2k}} + (b\alpha)^{2^{3k-s}}y^{2^{2k-s}} = (by)^{2^{-s}} + by^{2^s} + (b\alpha)^{2^{2k}}y^{2^{s+2k}} + (b\alpha)^{2^{3k-s}}y^{2^{2k-s}}$ is a linear function.

Thus

$$W^2_{F'}(a,b) = 2^n \sum_{\{y|\mathcal{L}(y)=0\}} (-1)^{\mathrm{Tr}(ay+by^{2^s+1}+b\alpha y^{2^{k+s}+2^{3k}})}.$$

The next step is to show that the cardinality of the kernel of $\mathcal{L}(y)$ is at most 2^{2t}, where $t = \gcd(2k, s)$. Following the computations of [2], we have

$$b^{2^{-s+2k}}\mathcal{L}(y) + (b\alpha)^{2^{3k-s}}\mathcal{L}^{2^{2k}}(y) = 0 \text{ and } b^{2^{2k}}\mathcal{L}(y) + (b\alpha)^{2^k}\mathcal{L}^{2^{2k}}(y) = 0,$$

from where we get

$$Ay^{2^s} + By^{2^{-s}} + Cy^{2^{s+2k}} = 0, \tag{5}$$

$$B^{2^s}y^{2^s} + A^{2^{2k}}y^{2^{-s}} + Cy^{2^{-s+2k}} = 0, \tag{6}$$

where

$$\begin{aligned}
A &= b^{2^{-s+2k}+1} + (b\alpha)^{2^{-k}+2^{3k-s}} \neq 0, \\
B &= b^{2^{-s}+2^{-s+2k}} + (b\alpha)^{2^{k-s}+2^{3k-s}}, \text{ and} \\
C &= b^{2^{-s+2k}+2^k}\alpha^{2^k} + b^{2^{2k}+2^{3k-s}}\alpha^{2^{3k-s}} \neq 0,
\end{aligned}$$

with $B = 0$ if and only if B^{2^s-1} is a cube.

Assume that $B \neq 0$, i.e. B^{2^s-1} is not a cube. Then from (5) and (6) we get

$$B^{2^{2s}}C^{2^{-s}}y^{2^{2s}} + C^{2^{-s}}A^{2^{2k+s}}y + B^{2^{-s}}C^{2^s}y^{2^{-2s}} + A^{2^{-s}}C^{2^s}y = 0.$$

Denote the last expression by $G(y)$. For some $v \neq 0$ in the kernel of $G(y)$, consider the expression $G_v(y) = yG(y) + vG(v) + (y+v)G(y+v)$, i.e.

$$C^{2^s}B^{2^{-s}}(y^{2^{-2s}}v + v^{2^{-2s}}y) + C^{2^{-s}}B^{2^{2s}}(y^{2^{2s}}v + v^{2^{2s}}y).$$

Note that the kernel of $\mathcal{L}(y)$ is contained in that of $G_v(y)$. Then from $G_v(y) = 0$ we get

$$C^{2^{-s}-2^s} B^{2^{2s-1}} (y^{2^{-2s}} v + v^{2^{-2s}} y)^{2^{2s}-1} = B^{2^s-1}.$$

If $y^{2^{-2s}} v + v^{2^{-2s}} y = 0$, i.e. $yv^{-1} = (yv^{-1})^{2^{2s}}$, then $yv^{-1} \in \mathbb{F}_{\gcd(2s,4k)} = \mathbb{F}_{2^{2t}}$ and therefore $\mathcal{L}(y) = 0$ has exactly 2^{2t} solutions. Otherwise, if $y^{2^{-2s}} v + v^{2^{-2s}} y$ does not vanish, then the right-hand side of the previous equation is not a cube by our assumption, while the left-hand side is. Hence, $\mathcal{L}(y) = 0$ has exactly 2^{2t} solutions, where $t = \gcd(2k, s)$.

Suppose now that $B = 0$. Following the computations of [2], the equation $\mathcal{L}(y) = 0$ becomes

$$(b + (bw)^{2^k} v^{2^{2k+s}-2^s}) y^{2^s} + (b^{2^{-s}} + (bw)^{2^{3k-s}} v^{2^{2k-s}-2^{-s}}) y^{2^{-s}} = 0.$$

If both coefficients (in front of y^{2^s} and in front of $y^{2^{-s}}$) in the above equation are nonzero, then raising both sides to the power 2^s, we get

$$(b + (bw)^{2^k} v^{2^{2k+s}-2^s})^{2^s} y^{2^{2s}} + (b^{2^{-s}} + (bw)^{2^{3k-s}} v^{2^{2k-s}-2^{-s}})^{2^s} y = 0.$$

Note that $2s = 2t\frac{s}{t}$ and $\gcd(\frac{s}{t}, 4k) = 1$. Then, applying Lemma 1, we get that $\mathcal{L}(y) = 0$ has at most 2^{2t} solutions. If exactly one of the coefficients is not zero, then the equation will have exactly one solution, namely $y = 0$. If both coefficients are equal to zero, then raising them to the power of 2^s and of 2^{-s}, and adding these powers together, we get $v^{2^{2k}-1} = b^{2^{3k}-2^{k-s}} w^{-2^{k-s}} = b^{1-2^{3k}} w^{-2^{3k}}$ which implies $C = 0$, a contradiction.

Thus, the kernel of $\mathcal{L}(y)$ consists of at most 2^{2t} elements, where $t = \gcd(2k, s)$ and therefore $|W_F^2(a, b)| \leq 2^n 2^{2t}$ and $|W_F(a, b)| \leq 2^{2k+t}$. □

The next corollary immediately follows from Theorem 2.

Corollary 1. *Let s, k, t be positive integers and let $n = 4k$. Let $\gcd(s, 2k) = t$, $2 \nmid k$, $i = sk \mod 4$, $m = 4-i$ and let w be a primitive element of $\mathbb{F}_{2^n}$. Then the nonlinearity of the function F from* (3) *satisfies*

$$\mathcal{NL}(F) \geq 2^{n-1} - 2^{2k+t-1}.$$

V. A COUNTEREXAMPLE: GENERALIZING A FAMILY OF APN QUADRINOMIALS TO 2^t-UNIFORM FUNCTIONS

As discussed above, both families of APN binomials from [5] can be generalized to functions all of whose derivatives are 2^t-to-1 by relaxing conditions; furthermore, the two families are obtained as generalizations of a previously unclassified sporadic APN instance over $\mathbb{F}_{2^{12}}$. Another sporadic APN instance, this time over $\mathbb{F}_{2^{10}}$, was recently also generalized into an infinite family [7]. This immediately raises the question of whether the same approach, i.e. relaxing conditions in order to obtain functions with 2^t-to-1 derivatives, could be applied to the latter family. In this section, we summarize our experimental results, which suggest that this is impossible.

The functions in the infinite family from [7] are defined over $\mathbb{F}_{2^n}$ with $n = 2m$ with m odd such that $3 \nmid m$, and have the form

$$F(x) = x^3 + \beta(x^{2^i+1})^{2^k} + \beta^2(x^3)^{2^m} + (x^{2^i+1})^{2^{m+k}}, \tag{7}$$

where k is a non-negative integer, and β is a primitive element of $\mathbb{F}_{2^2}$. It is shown that the function in (7) is APN for $i = m-2$ and $i = (m-2)^{-1} \mod n$, as well as for $i = m$ and $i = m-1$ (however, the last two values yield functions that are trivially EA-equivalent to known ones).

We computationally go through all functions of the form

$$F(x) = x^{2^j+1} + \beta(x^{2^i+1})^{2^k} + \beta^2(x^{2^j+1})^{2^m} + (x^{2^i+1})^{2^{m+k}} \tag{8}$$

with $0 \leq i, j \leq n-1$ for all values of $n = 2m$ with $6 \leq n \leq 14$, disregarding the conditions of $3 \nmid m$ and of m being odd. For each such function, we test whether all of its derivatives are 2^t-to-1 functions for some positive integer t. We restrict ourselves to the cases $k = 0$ and $k = 1$, as the APN functions constructed for $k \in \{0, 1\}$ appear to exhaust all CCZ-equivalence classes [7].

Besides the already known APN functions, for $k = 0$, we only encounter functions with 2^t-to-1 derivatives when $j = i$, i.e. when all exponents are in the same cyclotomic coset. In the case of $k = 1$, the only exceptions are for $n = 12$ where each pair (j, i) with $2 \leq j, i \leq 12$ and i, j even yields a 2^2-to-1, i.e. 4-to-1 function. However, since we do not observe other such non-trivial functions for other dimensions n, this does not suggest that (7) can be generalized to 2^t-functions in general.

These computational results constitute convincing evidence that the quadrinomials of the form (7) cannot be generalized to 2^t-to-1 functions in the same way as the binomials from [5].

VI. Conclusion

The APN binomial $x^3+\alpha x^{258}$ over $\mathbb{F}_{2^{12}}$ was generalized in 2008 to two infinite APN families over $\mathbb{F}_{2^n}$, one for $3 \mid n$, and one for $4 \mid n$. The family for $3 \mid n$ was generalized to a family of functions with 2^t-to-1 derivatives in 2012 [3] by relaxing conditions. We have shown that the same approach can be applied to the family for $4 \mid n$, and have computed the differential uniformity of the resulting functions. We have also given an upper bound on their nonlinearity, and have shown that this construction cannot be applied to any infinite family of quadratic APN functions by computationally verifying that the quadrinomial family from [7] constitutes a counterexample.

Acknowledgment

This research was supported by the Trond Mohn foundation (TMS).

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", J. Cryptol., vol. 4, no. 1, 1991, pp. 3–72.
[2] C. Bracken, C. Byrne, N. Markin, and G. Mcguire, "Fourier spectra of binomial APN functions", SIAM J, Discrete Math., vol. 23, no. 2, 2009, pp. 596–608.
[3] C. Bracken, C. Tan, and Y. Tan, "Binomial differentially 4 uniform permutations with hight nonlinearity", Finite Fields and Their Applications, 18, 2012, pp. 537–546.
[4] L. Budaghyan. "Construction and Analysis of Cryptographic Functions". Springer Verlag, 2015.

[5] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions", IEEE Transactions on Information Theory, vol. 54, 9, 2008, pp. 4218-4229.
[6] L. Budaghyan, C. Carlet, and A. Pott,"New classes of almost bent and almost perfect nonlinear functions", IEEE Trans. Inform. Theory, vol.52, no.3, 2006, pp.1141–1152.
[7] L. Budaghyan, T. Helleseth, and N. Kaleyski, "A new family of APN quadrinomials", IEEE Trans. Inform. Theory, 2020, early access article.
[8] C. Carlet. "Vectorial (multi-output) Boolean Functions for Cryptography". Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear soon. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html
[9] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptography", Design, Codes and Cryptography, vol.15, no.2, 1998, pp.125–156.
[10] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", Advances in Cryptology, Eurocrypt'94, Lecture Notes in Comput.Sci., vol, 950, 1995, pp. 356–365.
[11] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping", IEEE Trans. Inf. Theory, vol. 52, no.2, 2006, pp. 744–747.
[12] M.Matsui, "Linear cryptanalysis methods for DES cipher", Advances in Cryptology, Eurocrypt'93, Lecture Notes in Comput.Sci., vol, 765, 1993,pp. 386–397.
[13] K. Nyberg, "Differentially uniform mappings for cryptography", Eurocrypt'93, Lecture Notes in Comput.Sci., vol, 765, 1994, pp. 55-64.
[14] H. M. Trachtenberg, "On the Cross–Correlation Functions of Maximal Linear Sequences" , Ph.D. dissertation, University of Southern California, Los Angeles, 1970.

Paper VII

Partially APN Boolean functions and classes of functions that are not APN infinitely often

Lilya Budaghyan, Nikolay S. Kaleyski, Soonhak Kwon, Constanza S. Riera, Pantelimon Stanica
Cryptography and Communications, **vol. 12, pp.527-545** (2020)

Partially APN Boolean functions and classes of functions that are not APN infinitely often

Lilya Budaghyan[1], Nikolay S. Kaleyski[1], Soonhak Kwon[2], Constanza Riera[3], and Pantelimon Stănică[4]

[1]*Department of informatics, University of Bergen*
[2]*Department of Mathematics, Sungkyunkwan University*
[3]*Department of Computing, Mathematics, and Physics, Western Norway University of Applied Sciences*
[4]*Department of Applied Mathematics, Naval Postgraduate School*

Abstract

In this paper we define a notion of partial APNness and find various characterizations and constructions of classes of functions satisfying this condition. We connect this notion to the known conjecture that APN functions modified at a point cannot remain APN. In the second part of the paper, we find conditions for some transformations not to be partially APN, and in the process, we find classes of functions that are never APN for infinitely many extensions of the prime field $\mathbb{F}_2$, extending some earlier results of Leander and Rodier.

I. Introduction

The objects of this study are Boolean functions and some of their differential properties. We will introduce here only some needed notions, and the reader can consult [2], [5], [6], [9], [13], [16] for more on Boolean functions.

Let n be a positive integer and $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements, and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. Further, let $\mathbb{F}_2^m$ denote the m-dimensional vector space over $\mathbb{F}_2$. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables. The cardinality of a set S is denoted by $\#S$. For $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer-valued function $\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)}$, $u \in \mathbb{F}_{2^n}$, where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, given by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. This transform satisfies Parseval's relation $\sum_{a \in \mathbb{F}_{2^n}} \mathcal{W}_f(a)^2 = 2^{2n}$.

Given a Boolean function f, the derivative of f with respect to $a \in \mathbb{F}_{2^n}$ is the Boolean function $D_a f(x) = f(x + a) + f(x)$, for all $x \in \mathbb{F}_{2^n}$.

For positive integers n and m, any map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a vectorial Boolean function, or (n, m)-function. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field with the vector space) of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, $a_i \in \mathbb{F}_{2^n}$. The algebraic degree of F is then the largest Hamming weight of the exponents i with $a_i \neq 0$. For an (n, m)-function F, we define the Walsh transform $\mathcal{W}_F(a, b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x))+\mathrm{Tr}_1^n(ax)}, \text{ where } a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}.$$

For an (n,n)-function F, and $a,b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a,b) = \#\{x \in \mathbb{F}_{2^n} : F(x+a)+F(x) = b\}$. We call the quantity $\Delta_F = \max\{\Delta_F(a,b) : a,b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F \leq \delta$, then we say that F is differentially δ-uniform. If $\delta = 2$, then F is called an *almost perfect nonlinear* (*APN*) function. There are many useful characterizations and properties of APN functions, some of which are stated below (see [3], [6], [7], [15]).

Lemma 1. *Let F be an (n,n)-function. The following hold:*

(i) we have $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^4(a,b) \geq 2^{3n+1}(3\cdot 2^{n-1}-1)$, *with equality if and only if F is APN;*

(ii) if $F(0)=0$ and F is APN, then $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1)$;

(iii) (Rodier Condition) F is APN if and only if all the points x,y,z satisfying $F(x)+F(y)+F(z)+F(x+y+z)=0$, belong to the curve $(x+y)(x+z)(y+z)=0$.

We next introduce the notion of a partial APN function. Let $x_0 \in \mathbb{F}_{2^n}$. We call an (n,n)-function F a (*partial*) *x_0-APN function*, or simply x_0-APN function, if all the points u,v satisfying $F(x_0)+F(u)+F(v)+F(x_0+u+v)=0$, belong to the curve $(x_0+u)(x_0+v)(u+v)=0$. Certainly, an APN function is an x_0-APN for any point x_0.

A function F is called *weakly APN* if for any $a \neq 0$ the function $F(x+a)+F(x)$ takes at least $2^{n-2}+1$ different values (see [2]). Note that the notion of partial APN function differs from the notion of weakly APN function. For example, it can be checked that $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ with n even is weakly APN but not x_0-APN, for $x_0 \in \mathbb{F}_{2^n}$. On the other hand, $F(x) = x^7$ over $\mathbb{F}_{2^{11}}$ is 0-APN but not weakly APN.

Our proposal for the partial APN concept comes from a study of the conjecture in [3], which claims that for $n \geq 3$ an APN function modified at a point cannot remain APN. While this work has some overlap with [3], our ultimate goal is to investigate the partial APN concept.

II. Boolean functions modified at a point

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and consider an arbitrary point $x_0 \in \mathbb{F}_{2^n}$ and some nonzero $\epsilon \in \mathbb{F}_{2^n}^*$. Denote $y_0 = F(x_0)$ and $y_1 = y_0 + \epsilon$. Then the function F' over $\mathbb{F}_{2^n}$ defined by

$$F'(x) = \begin{cases} F(x) & \text{if } x \neq x_0 \\ y_1 & \text{if } x = x_0 \end{cases} \tag{1}$$

is called a *(single point) (x_0,y_1)-modification of F*.

It is rather easy to show that there are single point modifications of an APN function F that are not APN.

Proposition 2. *If an (n,n)-function F is APN for $n>1$, then for any $x_0 \in \mathbb{F}_{2^n}$ there exists $\epsilon \in \mathbb{F}_{2^n}^*$ such that the $(x_0, F(x_0)+\epsilon)$-modification of F is not APN.*

Proof. Suppose F is APN and $x_0 \in \mathbb{F}_{2^n}$ is given. Take $y,z \in \mathbb{F}_{2^n}$ such that x_0, y and z are distinct and let F' be the $(x_0, F(y)+F(z)+F(x_0+y+z))$ modification of F. Then we have $F'(x_0) \neq F(x_0)$ since F is APN and $F'(x_0)+F'(y)+F'(z)+F'(x_0+y+z) = 0$ so that F' cannot be APN. □

Next, we find some necessary and sufficient conditions for an (x_0, y_1)-modification of a given function to be partially APN.

Lemma 3. *Let F be an (n,n)-function and F' be an (x_0,y_1)-modification of F for $x_0, y_1 \in \mathbb{F}_{2^n}$ and $y_1 \neq y_0 = F(x_0)$. Then, with $\epsilon = y_0 + y_1$,*

$$\mathcal{W}_{F'}(a,b) = \mathcal{W}_F(a,b) - (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)}(1-(-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}).$$

Proof. We have

$$\begin{aligned}\mathcal{W}_{F'}(a,b) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF'(x)+ax)} = \sum_{x\neq x_0} (-1)^{\mathrm{Tr}_1^n(bF(x)+ax)} + (-1)^{\mathrm{Tr}_1^n(by_1+ax_0)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(x)+ax)} + (-1)^{\mathrm{Tr}_1^n(ax_0+by_1)} - (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)},\end{aligned}$$

which justifies our claim. □

For any given elements $a, b \in \mathbb{F}_{2^n}$ let us denote $E_F(a,b) = (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} D_F(b)$ where $D_F(b) = 1-(-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}$. Note that $E_F(a,b)$ depends on x_0, y_0 and y_1.

Lemma 4. *Let F be an (n,n)-function and let $x_0, y_1 \in \mathbb{F}_{2^n}$ with $y_1 \neq y_0 = F(x_0)$ and $\epsilon = y_0 + y_1$. Then for any integer $m \geq 1$ and any elements $a, b \in \mathbb{F}_{2^n}$, we have*

(i) $E_F^{2m}(a,b) = 2^{2m-1} D_F(b)$, *and*

(ii) $E_F^{2m+1}(a,b) = 2^{2m} E_F(a,b)$.

In the following we make use of the Kronecker function $\delta_0(z) = \begin{cases} 1 & \text{if } z = 0 \\ 0 & \text{if } z \neq 0. \end{cases}$

Theorem 5. *Let F be an (n,n)-function and F' be its (x_0,y_1)-modification for some $x_0, y_1 \in \mathbb{F}_{2^n}$ with $y_1 \neq y_0 = F(x_0)$. Then the following hold:*

(i) $\dfrac{1}{4}\displaystyle\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) = \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) - (3\cdot 2^{3n} - 2^{2n+1})$;

(ii) $\displaystyle\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 3\cdot 2^{2n+1}$
$\cdot\,(\delta_0(F(0)) - \delta_0(y_1 - y_0 + F(0))) + 2^{2n+2}\delta_0(x_0)\,(\delta_0(y_0) - \delta_0(y_1))\,.$

Proof. We show (i) first. Taking fourth powers in the identity $\mathcal{W}_{F'}(a,b) = \mathcal{W}_F(a,b) - E_F(a,b)$ of Lemma 3 and applying Lemma 4, we get

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) \\ &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(4\mathcal{W}_F^3(a,b)E_F(a,b) - 6\mathcal{W}_F^2(a,b)E_F^2(a,b) + 4\mathcal{W}_F(a,b)E_F^3(a,b) - E_F^4(a,b)\right) \\ &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(4\mathcal{W}_F^3(a,b)E_F(a,b) - 12\mathcal{W}_F^2(a,b)D_F(b) + 16\mathcal{W}_F(a,b)E_F(a,b) - 8D_F(b)\right).\end{aligned}$$

Thus,

$$\begin{aligned}&\frac{1}{4}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) \\ &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b)E_F(a,b) - 3\mathcal{W}_F^2(a,b)D_F(b) + 4\mathcal{W}_F(a,b)E_F(a,b) - 2D_F(b)\right).\end{aligned}$$

We now observe that $\sum_{a,b\in\mathbb{F}_{2^n}} D_F(b) = 2^n \sum_{b\in\mathbb{F}_{2^n}} D_F(b) = 2^n \sum_{b\in\mathbb{F}_{2^n}} (1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}) = 2^{2n}$, since $\sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0$ when $\epsilon \neq 0$. Further, by Parseval's identity we get $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b) D_F(b) = \sum_{b\in\mathbb{F}_{2^n}} D_F(b) \sum_{a\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b) = 2^{2n} \sum_{b\in\mathbb{F}_{2^n}} D_F(b) = 2^{3n}$. Finally, we use the inverse Walsh-Hadamard transform to obtain

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F(a,b)E_F(a,b) &= \sum_{a,b,u\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+y_0)+a(u+x_0))} D_F(b) \\ &= \sum_{b,u\in\mathbb{F}_{2^n}} \left(D_F(b)(-1)^{\mathrm{Tr}_1^n(b(F(u)+y_0))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+x_0))} \right) \\ &= 2^n \sum_{b\in\mathbb{F}_{2^n}} \left(D_F(b)(-1)^{\mathrm{Tr}_1^n(b(F(x_0)+y_0))} \right) = 2^n \sum_{b\in\mathbb{F}_{2^n}} D_F(b) = 2^{2n}.\end{aligned}$$

Combining the above results, we obtain

$$\frac{1}{4} \sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b) \right) = \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) - (3\cdot 2^{3n} - 2^{2n+1}),$$

and our first claim is shown.

By a similar argument as in part (i), we obtain

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b) \right) \\ &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(3\mathcal{W}_F^2(a,b)E_F(a,b) - 3\mathcal{W}_F(a,b)E_F^2(a,b) + E_F^3(a,b) \right) \qquad (2) \\ &= 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 6\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F(a,b)D_F(b) + 4\sum_{a,b\in\mathbb{F}_{2^n}} E_F(a,b).\end{aligned}$$

Furthermore, with $\epsilon = y_1 - y_0$, we compute

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F(a,b)D_F(b) \\ &= \sum_{b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right) \sum_{u\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(u))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(au)} \\ &= 2^n \sum_{b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right) (-1)^{\mathrm{Tr}_1^n(bF(0))} \\ &= 2^n \left(\sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(0))} - \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(y_1-y_0+F(0)))} \right) \\ &= 2^{2n} \left(\delta_0(F(0)) - \delta_0(y_1-y_0+F(0)) \right),\end{aligned}$$

and

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} \left(1-(-1)^{\mathrm{Tr}_1^n(b(y_1-y_0))}\right) \\ &= 2^{2n}\delta_0(x_0)\left(\delta_0(y_0)-\delta_0(y_1)\right).\end{aligned}$$

Using these identities in (2), we obtain

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right)$$
$$= 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 3\cdot 2^{2n+1}\left(\delta_0(F(0)) - \delta_0(y_1 - y_0 + F(0))\right)$$
$$+ 2^{2n+2}\delta_0(x_0)\left(\delta_0(y_0) - \delta_0(y_1)\right),$$

and the theorem is shown. □

Corollary 6. *Let F be an (n,n)-function satisfying $F(0)=0$, and $x_0 \in \mathbb{F}_{2^n}$, $\epsilon \in \mathbb{F}_{2^n}^*$. Let further F' be its $(x_0, F(x_0)+\epsilon)$-modification. Then we have, with $y_1 = F(x_0)+\epsilon$:*
(a) if $x_0 = y_0 = 0$ then $y_1 \neq 0$ and

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 2^{2n+1};$$

(b) if $x_0 \neq 0$ then

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 3\cdot 2^{2n+1}.$$

Proof. Follows easily from Theorem 5 (ii). □

Corollary 7. *Let F be an APN (n,n)-function satisfying $F(0)=0$. Let $x_0 = 0 = y_0$, and let F' be the $(0,\epsilon)$-modification of F. Then, F' is APN if and only if*

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0.$$

Proof. By Lemma 1, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^4(a,b) = 2^{3n+1}(3\cdot 2^{n-1}-1)$, and $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1)$. Also, by the same lemma, F' is APN if and only if $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^4(a,b) = 2^{3n+1}(3\cdot 2^{n-1}-1)$. This, together with Theorem 5 (i), implies that F' is APN if and only if

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) = 3\cdot 2^{3n} - 2^{2n+1}.$$

On the other hand, since $x_0 = 0 = y_0$, $E_F(a,b) = D_F(a,b) = 1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}$, and

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) = \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)}$$
$$= 2^{2n+1}(3\cdot 2^{n-1}-1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)}.$$

This, together with the previous corollary, gives the sufficient and necessary condition $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0$. □

Theorem 8. *Let F be an (n,n)-function and F' be its (x_0,y_1)-modification. For any $x,y\in\mathbb{F}_{2^n}$, let*

$$\begin{aligned} T_{x,y} &= \{(u,v)\in\mathbb{F}_{2^n}^2 : (u+x)(v+x)(u+v)\neq 0, F(u)+F(v)+F(u+v+x)+y=0\},\\ S_{x,y} &= \{u\in\mathbb{F}_{2^n} : F(u)+F(u+x)+y=0\}. \end{aligned}$$

Then:

$$(i)\quad \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) = 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0} - \#T_{x_0,y_1}\right);$$

$$(ii)\quad \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) = 2^{2n}\left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right).$$

Proof. To show (i), we write

$$\begin{aligned} \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right)\\ &\quad\cdot \sum_{u,v,w\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w)+y_0))}(-1)^{\mathrm{Tr}_1^n(a(u+v+w+x_0))}\\ &= \sum_{b,u,v,w\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right)(-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w)+y_0))}\\ &\quad\cdot \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+w+x_0))}\\ &= 2^n \sum_{b,u,v\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right)(-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(u+v+x_0)+y_0))}\\ &= 2^n \sum_{u,v\in\mathbb{F}_{2^n}} \left(\sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(u+v+x_0)+y_0))} \right. \qquad (3)\\ &\quad \left. - \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(u+v+x_0)+y_1))} \right). \qquad (4) \end{aligned}$$

Now, the inner sums in (3) and (4) will be zero unless one of the exponents is zero, that is, unless $F(u)+F(v)+F(u+v+x_0)+F(x_0)=0$ or $F(u)+F(v)+F(u+v+x_0)+y_1=0$.

Since there are $3\cdot 2^n-2$ pairs (u,v) satisfying $(u+x_0)(v+x_0)(u+v)=0$, the above equation becomes

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) = 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0} - \#T_{x_0,y_1}\right),$$

and the first claim is proven. To show (ii) we write

$$\begin{aligned} \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(\sum_{u,v\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+x_0)+b(F(u)+F(v)+y_0))} \right.\\ &\quad \left. - \sum_{u,v\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+x_0)+b(F(u)+F(v)+y_1))} \right) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{b\in\mathbb{F}_{2^n}} \sum_{u,v\in\mathbb{F}_{2^n}} \left((-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+y_0))} - (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+y_1))}\right) \\
&\qquad\qquad \cdot \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+x_0))} \\
&= 2^n \sum_{u\in\mathbb{F}_{2^n}} \sum_{b\in\mathbb{F}_{2^n}} \left((-1)^{\mathrm{Tr}_1^n(b(F(u)+F(u+x_0)+y_0))} - (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(u+x_0)+y_1))}\right) \\
&= 2^{2n}\left(|S_{x_0,y_0}| - |S_{x_0,y_1}|\right),
\end{aligned}
$$

and the theorem is proven. □

Note that in the above theorem we in fact showed that

$$
\begin{aligned}
\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} &= 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0}\right), \\
\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_1)} &= 2^{2n}\left(\#T_{x_0,y_1}\right).
\end{aligned}
$$

That is, for an (n,n)-function F and its one point modification F' at x_0, Theorem 8 gives

$$
\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) \\
&\quad= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_1)} \\
&\quad= 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0}\right) - 2^{2n}\left(\#T_{x_0,y_1}\right). \qquad (5)
\end{aligned}
$$

By Theorem 5, we get

$$
\begin{aligned}
\frac{1}{4}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) &= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) - 2^{2n}(3\cdot 2^n - 2) \\
&= 2^{2n}(\#T_{x_0,y_0} - \#T_{x_0,y_1}),
\end{aligned}
$$

where the last equality comes from the equation (5).

Therefore, we obtain the following equivalence:

$$
\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) = 0 \iff \#T_{x_0,y_0} = \#T_{x_0,y_1}. \qquad (6)
$$

The definition of x_0-APN implies that F' is x_0-APN if and only if $(u+x_0)(v+x_0)(u+v) \neq 0 \implies F'(u)+F'(v)+y_1+F'(u+v+x_0) \neq 0$. However, when $(u+x_0)(v+x_0)(u+v) \neq 0$, one has $F'(u)+F'(v)+y_1+F'(u+v+x_0) = F(u)+F(v)+y_1+F(u+v+x_0)$. Therefore, F' is x_0-APN if and only if $(u+x_0)(v+x_0)(u+v) \neq 0 \implies F(u)+F(v)+y_1+F(u+v+x_0) \neq 0$. In other words, F' is x_0-APN if and only if T_{x_0,y_1} is the empty set.

Now, the set T_{x_0,y_0} with $y_0 = F(x_0)$ is empty if and only if F is x_0-APN. By (6) and Lemma 1 we have:

Theorem 9. *If F is APN and its (x_0,y_1)-modification F' with $y_1 \neq F(x_0)$ is x_0-APN, then F' is APN.*

Note that this can also be directly derived from the definition of one point modification. Indeed, suppose to the contrary, that F' is x_0-APN but it is not APN. Then for some $a \neq 0$ and some b the equation $F'(x+a)+F'(x)=b$ has more than 2 solutions. Let x_1, x_2, x_3 be three distinct solutions to this equation. We consider two cases. If $\{x_1,x_2,x_3\} \cap \{x_0, x_0+a\} = \emptyset$ then $F'(x_i+a)+F'(x_i) = F(x_i+a)+F(x_i)$ for $i \in \{1,2,3\}$ and this contradicts F being APN. If $\{x_1,x_2,x_3\} \cap \{x_0, x_0+a\} \neq \emptyset$, then it contradicts F' being x_0-APN.

In light of Theorem 9, it follows that the conjecture from [3] can be strengthened as follows:

Conjecture 10. *An (x_0, y_1)-modification of an APN function with $y_1 \neq F(x_0)$ is not x_0-APN.*

One way of showing that this is true would be to show $\{F(x_0)+F(u)+F(v)+F(x_0+u+v) : u,v \in \mathbb{F}_{2^n}\} = \mathbb{F}_{2^n}$. Indeed, suppose that F' is an (x_0,y_1)-modification of F with $y_1 \neq y_0 = F(x_0)$ and that F' is not APN. This is true if and only if the equation $F'(x_0)+F'(u)+F'(v)+F'(x_0+u+v)=0$ is satisfied by a pair of elements $u,v \in \mathbb{F}_{2^n}$ with $(u+x_0)(v+x_0)(u+v) \neq 0$. Writing $\epsilon = y_0+y_1$, this is equivalent to $F(x_0)+F(u)+F(v)+F(x_0+u+v)=\epsilon$ or, in other words, $\epsilon \in \{F(x_0)+F(u)+F(v)+F(x_0+u+v) : u,v \in \mathbb{F}_{2^n}\}$. Thus, the difference ϵ between $F(x_0)$ and $F'(x_0)$ must not be expressible as $D_aF(x_0)+D_aF(y)$ in order for F' to be x_0-APN.

Corollary 11. *Let F be an (n,n)-function and let F' be its (x_0,y_1)-modification for $x_0, y_0 \in \mathbb{F}_{2^n}$ with $y_1 \neq y_0 = F(x_0)$. Then,*

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\cdot 2^{2n}\left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right)$$
$$- 3\cdot 2^{2n+1}\left(\delta_0(F(0)) - \delta_0(y_1-y_0+F(0))\right) + 2^{2n+2}\delta_0(x_0)\left(\delta_0(y_0)-\delta_0(y_1)\right).$$

Furthermore,

(a) *If $F(0)=0\neq x_0$, then,* $\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\cdot 2^{2n}\left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right) - 3\cdot 2^{2n+1}$;

(b) *If $F(0)=0=x_0$, then* $\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\cdot 2^{2n}\left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right) - 2^{2n+1} = 2^{2n+1}(3\cdot 2^{n-1}-1)$;

(c) *If F is APN and $F(0)=0\neq x_0$, then* $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1) + 3\cdot 2^{2n}\#S_{x_0,y_1}$;

(d) *If F is APN and $F(0)=0=x_0$, then* $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 0$.

Proof. The main claim, item (a) and the first equation in (b) follow easily from Theorem 5 (ii) and Theorem 8 (ii). For the second equation of (b), we suppose $F(0)=0=x_0$. Then, $S_{x_0,y_0} = \{u \in \mathbb{F}_{2^n} | F(u)+F(u)+F(0)=0\} = \mathbb{F}_{2^n}$, so $\#S_{x_0,y_0} = 2^n$. Also, $S_{x_0,y_1} = \{u \in \mathbb{F}_{2^n} | F(u)+F(u)+F'(0)=0\} = \emptyset$, so $\#S_{x_0,y_1}=0$.

To show (c), we assume that F is APN with $F(0)=0\neq x_0$. Then, $S_{x_0,y_0} = \{u \in \mathbb{F}_{2^n} | F(u)+F(u+x_0)+F(x_0)=0\} = \{0,x_0\}$. By Lemma 1, we get $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1)$. From this and from the main claim of this corollary, we have

$$2^{2n+1}(3\cdot 2^{n-1}-1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 3\cdot 2^{2n}\left(2-\#S_{x_0,y_1}\right) - 3\cdot 2^{2n+1},$$

and so,

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^3_{F'}(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1) + 3\cdot 2^{2n}\#S_{x_0,y_1}.$$

To show (d), we now suppose that F is APN and $F(0)=0=x_0$. Then, by Lemma 1 and point (b) of this corollary,

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}^3_F(a,b) - \mathcal{W}^3_{F'}(a,b)\right) &= 2^{2n+1}(3\cdot 2^{n-1}-1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^3_{F'}(a,b)\\ &= 2^{2n+1}(3\cdot 2^{n-1}-1),\end{aligned}$$

which implies that $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^3_{F'}(a,b) = 0$, and the claim is shown. □

Note that Corollary 7 can also be deduced from Theorem 8. Furthermore, we can deduce the following corollary:

Corollary 12. *Let F be an (n,n)-function. Let $x_0 = 0 = y_0$, and F' be the $(0,\epsilon)$-modification of F for some $\epsilon\in\mathbb{F}_{2^n}^*$. Then, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^2_F(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0$.*

Proof. Using the notation of Theorem 8, $S_{0,0}=\mathbb{F}_2^n$, while $S_{0,\epsilon}=\emptyset$. Then, by Theorem 8, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^2_F(a,b)E_F(a,b) = 2^{3n}$. On the other hand,

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^2_F(a,b)D_F(b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^2_F(a,b) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^2_F(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\\ &= 2^{3n} - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^2_F(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)},\end{aligned}$$

which shows the corollary. □

III. A CHARACTERIZATION OF PARTIAL APN FUNCTIONS

We now provide a necessary and sufficient condition for a function to be x_0-APN. As a consequence of our theorem we can obtain the APN conditions of Lemma 1.

Theorem 13. *Let F be an (n,n)-function and $x_0\in\mathbb{F}_{2^n}$. Then F is x_0-APN if and only if*

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^3_F(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+bF(x_0))} = 2^{2n+1}(3\cdot 2^{n-1}-1).$$

Proof. We have

$$\begin{aligned}&\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}^3_F(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+bF(x_0))}\\ &= \sum_{a,b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(ax_0+bF(x_0))} \sum_{u,v,w\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w))+a(u+v+w))}\\ &= \sum_{b,u,v,w\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w)+F(x_0)))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+w+x_0))}\\ &= 2^n \sum_{b,u,v\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(x_0)+F(u+v+x_0)))}\end{aligned}$$

$$= 2^n \sum_{u,v\in\mathbb{F}_{2^n}} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(x_0)+F(u+v+x_0)))}$$
$$= 2^{2n}\#\{(u,v)\in\mathbb{F}_{2^n}^2 : F(u)+F(v)+F(x_0)+F(u+v+x_0)=0\}$$
$$= 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0}\right).$$

Since T_{x_0,y_0} is empty if and only if F is x_0-APN, the claim follows. □

IV. Monomial partial APN functions

For a monomial $F(x)=x^m$, the polynomial $G(x,y,z)=F(x)+F(y)+F(z)+F(x+y+z)$ is a symmetric homogeneous polynomial of degree m, and so, $G(kx,ky,kz)=k^mG(x,y,z)$ for all $k\in\mathbb{F}_{2^n}$. Using this property, we show that a monomial F is APN if and only if F is partial APN on a subspace of dimension 1 (that is, it is partial APN at 0 and some $x_0\neq 0$).

Proposition 14. *Let $F(x)=x^m$ over $\mathbb{F}_{2^n}$. Then:*

(*i*) *If $x_0\neq 0$, then F is x_0-APN if and only if F is x_1-APN for all $x_1\in\mathbb{F}_{2^n}^*$;*
(*ii*) *F is APN if and only if F is 0-APN and x_1-APN for some $x_1\in\mathbb{F}_{2^n}^*$.*

Proof. Certainly, (*ii*) is a consequence of (*i*). For a proof of the first claim, note that F is x_0-APN if and only if $G(x_0,y,z)\neq 0$ for all y,z with $(y+x_0)(z+x_0)(y+z)\neq 0$. Using the homogeneous property of G, $0\neq G(x_0,y,z)=G(kx_0,ky,kz)$ for any $k\neq 0$, so the condition can be written as $G(x_1,y,z)\neq 0$ for all $x_1\neq 0$ and y,z with $(y+x_1)(z+x_1)(y+z)\neq 0$. □

Charpin and Kyureghyan [8] also considered a partial APN concept on (n,n)-functions: we say that F satisfies the property (p_a), $a\in\mathbb{F}_{2^n}^*$, if the equation $F(x)+F(x+a)=b$ has either 0 or 2 solutions for every $b\in\mathbb{F}_{2^n}$. They showed that a mapping F is APN if and only if F satisfies (p_a) for all nonzero a belonging to a hyperplane. It is not clear if such a result is true for our notion of partial APNness. From the result above, we see that a similar result is true for monomials, i.e. F is APN if and only if it is partial APN for a subspace of dimension 1. Moreover, when F is a monomial, the property (p_1) implies the property (p_a) for any $a\neq 0$. Therefore our result on 0-APN has some analogy with the property (p_1), but 0-APN is a more general condition than the property (p_1), as the following examples will show.

We let $\binom{a}{b}_2$ denote the residue modulo 2 of the binomial coefficient $\binom{a}{b}$. We next investigate and explicitly construct many classes of Boolean functions that are 0-APN (but not necessarily APN).

Theorem 15. *Let $\mathbb{F}_{2^n}$ be the extension field of $\mathbb{F}_2$ corresponding to the primitive polynomial f of degree n and let g be one of the (primitive) roots of f. Then:*

(*i*) *if $F(x)=x^m$ over $\mathbb{F}_{2^n}$, then F is 0-APN if and only if for $1\leq i\leq 2^n-1$, the minimal polynomial $P_{g^i}(X)=\prod_{j\in C_i}(X-g^j)$ of g^i, where $C_i=\{(i\cdot 2^j) \pmod{2^n-1} : j=0,1,\ldots\}$ is the unique cyclotomic coset of i modulo 2^n-1, does not divide $\sum_{k=1}^{mi-1}\binom{mi}{k}_2 x^{mi-k-1}$;*
(*ii*) *if $F(x)=x^{2^d-1}$ over $\mathbb{F}_{2^n}$, then F is 0-APN if and only if $\gcd(d-1,n)=1$;*
(*iii*) *if $F(x)=x^{2^d+1}$ over $\mathbb{F}_{2^n}$, then F is 0-APN if and only if $\gcd(d,n)=1$.*

Proof. If $F(x)=x^m$, then F is 0-APN if and only if the Rodier equation

$$F(y)+F(z)+F(y+z)=y^m+z^m+(y+z)^m=0,$$

has no solution $y, z \in \mathbb{F}_{2^n}^*$ with $y \neq z$. Given two distinct elements $y, z \in \mathbb{F}_{2^n}^*$, let $z = y\alpha$, where $\alpha \neq 0, 1$. Then, the equation above becomes

$$y^m \left(1 + \alpha^m + (1+\alpha)^m\right) = 0,$$

implying $1 + \alpha^m + (1+\alpha)^m = 0$. Then, if there exists $\alpha \neq 0, 1$ satisfying the previous equation, then there exists $1 \leq i \leq 2^n - 1$ such that

$$\frac{1 + x^{im} + (1+x^i)^m}{x} = \sum_{k=1}^{mi-1} \binom{mi}{k}_2 x^{mi-k-1}$$

vanishes at g, that is, $1 + g^{i\,m} + \left(1 + g^i\right)^m = 0$. Then it will vanish at g^{2^ℓ}, for all ℓ, since $1 + g^{i\,m\,2^\ell} + \left(1 + g^{i\,2^\ell}\right)^m = \left(1 + g^{i\,m} + \left(1 + g^i\right)\right)^{2^\ell} = 0$. Thus, the minimal polynomial $P_{g^i}(X) = \prod_{j \in C_i} (X - g^j)$ of g^i divides $\sum_{k=1}^{mi-1} \binom{mi}{k}_2 x^{mi-k-1}$. The converse is certainly true, and the first claim is shown.

To test whether $F = x^{2^d-1}$ is 0-APN, one needs to check the (in)solvability of the Rodier equation

$$\begin{aligned} 0 &= F(y) + F(z) + F(y+z) \\ &= y^{2^d-1} + z^{2^d-1} + (y+z)^{2^d-1} \\ &= \frac{zy^{2^d-1} + yz^{2^d-1}}{y+z} = \frac{(\alpha^{2^d-1} + \alpha) z^{2^d}}{z(\alpha+1)}, \end{aligned}$$

where $y = z\alpha, \alpha \neq 0, 1$. Therefore, when (and only when) $\gcd(2^d - 2, 2^n - 1) = 1$, there is no $\alpha \neq 0, 1$ satisfying the above equation, that is, x^{2^d-1} is 0-APN. The condition $\gcd(d-1, n) = 1$ follows form the known identity $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$, since $1 = \gcd(2^d - 2, 2^n - 1) = \gcd(2^{d-1} - 1, 2^n - 1) = 2^{\gcd(d-1,n)} - 1$.

In the same way, we consider $F(x) = x^{2^d+1}$ over $\mathbb{F}_{2^n}$. To test whether F is 0-APN, one needs to check the solvability of the Rodier equation

$$\begin{aligned} 0 &= F(y) + F(z) + F(y+z) \\ &= y^{2^d+1} + z^{2^d+1} + (y+z)^{2^d+1} \\ &= zy^{2^d} + yz^{2^d} = (\alpha^{2^d} + \alpha) z^{2^d+1}, \end{aligned}$$

where $y = z\alpha, \alpha \neq 0, 1$. Therefore, when (and only when) $1 = \gcd(2^d - 1, 2^n - 1) = 2^{\gcd(d,n)} - 1$, that is, for $\gcd(d, n) = 1$, there is no $\alpha \neq 0, 1$ satisfying the above equation, so x^{2^d+1} is 0-APN. □

Example 16. Table I lists the exponents i for which x^i is 0-APN but not APN over $\mathbb{F}_{2^n}$. Only one representative from every cyclotomic coset is given. There are no functions of this type for $n \leq 5$. We also verified that there are no power functions $F(x) = x^i$ over $\mathbb{F}_{2^n}$, $n \leq 15$, which are 1-APN but not 0-APN, suggesting that perhaps 1-APN-ness implies 0-APN-ness for power functions. This is not true in general: we found over six million polynomials over $\mathbb{F}_{2^3}$ that are 1-APN but not APN, for example, $x^7 + x^6$. Out of these, 64 have coefficients in $\mathbb{F}_2$: 48 of them have the differential spectrum $\{0^{31}, 2^{22}, 4^3\}$, while the remaining 16 have the spectrum $\{0^{42}, 2^7, 6^7\}$. We also found 6944 polynomials of this type over $\mathbb{F}_{2^4}$ with coefficients in $\mathbb{F}_2$, for example, $x^{12} + x^7$.

n	Exponents i	Δ_F
6	27	12
7	7,21,31,55	6
	19,47	4
8	15,45	14
	21,111	4
	51	50
	63	6
9	7,21,35,61,83,91,111,117,119,175	6
	41,187	8
	45,125	4
10	15,27,45,75,111,117,147,189,207,255	6
	21,69,87,237,375	4
	51	8
	93	92
	105,351	10
	231,363	12

TABLE I: Power functions $F(x) = x^i$ over $\mathbb{F}_{2^n}$ that are 0-APN but not APN

V. Classes of never 0-APN (hence never APN) for infinitely many extensions of $\mathbb{F}_2$

Building up on some of their earlier work on the function $x^3 + \mathrm{Tr}_1^n(x^9)$, which is APN on $\mathbb{F}_{2^n}$, for all dimensions n, Budaghyan et al. [4] generalized this class to $L_1(x^3) + L_2(x^9)$, where L_1, L_2 are linear functions on $\mathbb{F}_{2^n}$, and found conditions under which this function is APN.

In a series of papers, Rodier and his collaborators [1], [10], [11], [14], [15] concentrated on finding classes of functions that are never APN for infinitely many extensions of the prime field $\mathbb{F}_2$. Here we present classes of functions that are never 0-APN (and hence never APN) for infinitely many extensions of $\mathbb{F}_2$, and in the process even extend some of the existing results.

Theorem 17. *Let L be a linear polynomial on $\mathbb{F}_{2^n}$, g be a primitive element of $\mathbb{F}_{2^n}$ and $d \geq 1$ be a positive integer. Furthermore, let F and G be defined over $\mathbb{F}_{2^n}$ by $F(x) = L\left(x^{2^d+1}\right) + \mathrm{Tr}_1^n(x^3)$ and $G(x) = L\left(x^{2^{d+1}+2^d+1}\right) + \mathrm{Tr}_1^n(x^3)$. If $\gcd(d, n) > 1$, then neither F nor G is 0-APN.*

In general, $L(x^m) + \mathrm{Tr}_1^n(x^3)$ is not 0-APN if there exists some $1 \leq i \leq 2^n - 1$, such that $P_{g^i}(X) = \prod_{j \in C_i}(X - g^j)$ divides $\sum_{k=1}^{mi-1} \binom{mi}{k}_2 x^{mi-k-1}$, where $C_i = \{(i \cdot 2^j) \pmod{2^n - 1} \mid j = 0, 1, \ldots\}$ is the unique cyclotomic coset of i modulo $2^n - 1$.

Proof. The function F is 0-APN if and only if there are no solutions $x, y \in \mathbb{F}_{2^n}^*$, $x \neq y$ of the equation

$$\begin{aligned} 0 &= F(x) + F(y) + F(x+y) \\ &= L\left(x^{2^d+1} + y^{2^d+1} + (x+y)^{2^d+1}\right) + \mathrm{Tr}_1^n\left(x^3 + y^3 + (x+y)^3\right) \\ &= L\left(x^{2^d} y + x\, y^{2^d}\right) + \mathrm{Tr}_1^n(x^2 y + x y^2). \end{aligned}$$

Writing $y = \alpha x$, this is equivalent to the equation

$$L\left(x^{2^d+1}(\alpha + \alpha^{2^d})\right) = \mathrm{Tr}_1^n\left(x^3(\alpha + \alpha^2)\right)$$

having no solution for $\alpha \neq 0, 1$. Now, if $m = \gcd(d, n) > 1$, we take $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \subseteq \mathbb{F}_{2^d} \cap \mathbb{F}_{2^n}$. Then $\alpha^{2^d} + \alpha = 0$, and for $x = 1$ we have $\mathrm{Tr}_1^n(x^3(\alpha + \alpha^2)) = 0$, since it is known that $\mathrm{Tr}_1^n(u) = 0$ if and only if $u = b^2 + b$ (in characteristic 2), which renders nontrivial solutions to the above equation. The first claim is shown.

We now concentrate on $G(x)$. Once again we want to show that the Rodier equation

$$G(x) + G(y) + G(x + y) = 0$$

has no solutions $x, y \in \mathbb{F}_{2^n}^*$ with $x \neq y$. Similarly to the case for F above and writing $y = \alpha x$, we can easily see that this is equivalent to the equation

$$L\left(x^{2^{d+1}+2^d+1}(\alpha + \alpha^{2^d})(1 + \alpha^{2^d} + \alpha^{2^{d+1}})\right) = \mathrm{Tr}_1^n\left(x^3(\alpha + \alpha^2)\right) \tag{7}$$

having no solutions with $\alpha \neq 0, 1$. So, denoting $m = \gcd(d, n) > 1$, we can take $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \subseteq \mathbb{F}_{2^d} \cap \mathbb{F}_{2^n}$. Then we have $\alpha + \alpha^{2^d} = 0$ so that this α along with $x = 1$ constitute a solution to (7) implying that G is not 0-APN.

The last claim can be argued as in the proof of Theorem 15(i). □

Remark 18. We have computationally checked that if $n = 5$, then $x^9 + \mathrm{Tr}_1^n(x^3)$ is 0-APN, and potentially there may be some other cases.

These classes of functions can be further generalized so as to encompass even more functions that are not 0-APN.

Theorem 19. *Let L_1 and L_2 be linear functions over $\mathbb{F}_{2^n}$. If $\gcd(d, r, n) > 1$, then $L_1(x^{2^d+1}) + L_2(x^{2^r+1})$ is not 0-APN.*

Furthermore, if L_1 is the identity and L_2 is the absolute trace, then $x^{2^d+1} + \mathrm{Tr}_1^n(x^{2^r+1})$ is not 0-APN if $\gcd(d, n) > 1$ and $\gcd(2^r + 1, 2^n - 1) = 1$, or $\gcd(d, r, n) > 1$.

Finally, $L_1\left(x^{2^{d+1}+2^d+1}\right) + L_2\left(x^{2^{s+1}+2^s+1}\right)$ is not 0-APN if $\gcd(d, s, n) > 1$.

Proof. We consider first the function $L_1(x^{2^d+1}) + L_2(x^{2^r+1})$. As before, we investigate the solvability of the equation

$$L_1\left(x^{2^d+1}(\alpha + \alpha^{2^d})\right) = L_2\left(x^{2^r+1}(\alpha + \alpha^{2^r})\right) \tag{8}$$

where $y = \alpha x$ for $x \neq 0$ and $\alpha \neq 0, 1$. Denoting $m = \gcd(d, r, n) > 1$, we can take $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \subseteq \mathbb{F}_{2^d} \cap \mathbb{F}_{2^r}$. Then $\alpha^{2^d} + \alpha = \alpha^{2^r} + \alpha = 0$, so that (8) has nontrivial solutions and thus the considered function is not 0-APN.

In the particular case when L_1 is the identity and L_2 is the trace function, it is sufficient to show that the function $x^{2^d+1} + \mathrm{Tr}_1^n(x^{2^r+1})$ is not 0-APN if $\gcd(d, n) > 1$ and $\gcd(2^r + 1, 2^n - 1) = 1$ since the other case follows from the previously proven statement. The relevant Rodier equation is

$$x^{2^d+1}(\alpha + \alpha^{2^d}) = \mathrm{Tr}_1^n\left(x^{2^r+1}(\alpha + \alpha^{2^r})\right).$$

Denoting $m = \gcd(d, n) > 1$, we can find $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$ for which the left hand side vanishes. Now we argue that regardless of the value of α, there exists an element x such that $x^{2^r+1}(\alpha + \alpha^{2^r}) = \beta^2 + \beta$ for some β. If $\alpha + \alpha^{2^r} = 0$, we are done since x can take any value. If $\alpha + \alpha^{2^r} \neq 0$, taking $\beta = \alpha + \alpha^{2^r}$, if $\beta + 1 \neq 0$, or any other nonzero element β of the finite field such that $\beta + 1 \neq 0$, the above claim is implied by the existence of solutions x such that $x^{2^r+1} = \frac{\beta^2+\beta}{\alpha+\alpha^{2^r}}$. This in turn follows from the fact

that $\gcd(2^r+1, 2^n-1) = 1$ and thus every element of $\mathbb{F}_{2^n}$ has a 2^r+1-st root (see e.g. [12]).
To show the last claim, we again examine the relevant Rodier equation which in this case (by applying the same approach as above) takes the form

$$L_1\left(\left(\alpha+\alpha^{2^d}\right)\left(1+\alpha^{2^d}+\alpha^{2^{d+1}}\right)\right) = L_2\left(\left(\alpha+\alpha^{2^s}\right)\left(1+\alpha^{2^s}+\alpha^{2^{s+1}}\right)\right).$$

Denoting $m = \gcd(d, s, n) > 1$, we can find $\alpha \in \mathbb{F}_{2^m}\backslash\mathbb{F}_2$, so that , $\alpha+\alpha^{2^d} = \alpha+\alpha^{2^s} = 0$. The Rodier equation thus has nontrivial solutions and the function in question is not 0-APN. □

Recall the following result (obtained using a combination of theoretical and computational arguments) of Leander and Rodier [11].

Theorem 20 (Leander-Rodier, 2011)**.** *If $n \geq 2$ and d is a nonzero integer which is not a power of 2, then the function*

$$F(x) = x^{2^n-2} + \beta\, x^d$$

over $\mathbb{F}_{2^n}$ is not APN for $d \leq 29$ and any $\beta \in \mathbb{F}_{2^n}^*$.

Below we find more classes of functions that are not 0-APN for infinitely many extensions $\mathbb{F}_{2^n}$. In the process, we extend the previous result of Leander and Rodier.

Theorem 21. *Let $a > b$ be positive integers. Assuming that one of x^a and x^b are 0-APN on $\mathbb{F}_{2^n}$ and $\gcd(a-b, 2^n-1) = 1$, the polynomial $x^a + \beta\, x^b$ is not 0-APN for any $\beta \in \mathbb{F}_{2^n}^*$. Let $c > d$ be positive integers. In particular,*

(i) if $\gcd(c-1, n) = \gcd(c-d, n) = 1$, or $\gcd(d-1, n) = \gcd(c-d, n) = 1$, then the polynomial $x^{2^c-1} + \beta\, x^{2^d-1}$ is not 0-APN;

(ii) if $\gcd(c, n) = \gcd(c-d, n) = 1$, or $\gcd(d, n) = \gcd(c-d, n) = 1$, then the polynomial $x^{2^c+1} + \beta\, x^{2^d+1}$ is not 0-APN;

(iii) if $\gcd(c, n) = \gcd(2^{c-1} - 2^{d-1} + 1, 2^n-1) = 1$, or $\gcd(d-1, n) = \gcd(2^{c-1} - 2^{d-1} + 1, 2^n-1) = 1$, then the polynomial $x^{2^c+1} + \beta\, x^{2^d-1}$ is not 0-APN;

(iv) if $\gcd(c-1, n) = \gcd(2^{c-1} - 2^{d-1} - 1, 2^n-1) = 1$, or $\gcd(d, n) = \gcd(2^{c-1} - 2^{d-1} - 1, 2^n-1) = 1$, then the polynomial $x^{2^c-1} + \beta\, x^{2^d+1}$ is not 0-APN.

Proof. Let $F(x) = x^a + \beta\, x^b$ $(a > b)$. Then F is 0-APN if and only if $0 = F(y) + F(z) + F(y+z)$ has no solutions y, z with $yz(y+z) \neq 0$. The relevant Rodier equation takes the form

$$0 = F(y) + F(z) + F(y+z) = y^a + \beta\, y^b + z^a + \beta z^b + (y+z)^a + \beta(y+z)^b$$

which, writing $y = z\alpha$ with $\alpha \neq 0, 1$, becomes

$$0 = z^a\left(\alpha^a + 1 + (\alpha+1)^a\right) + \beta z^b\left(\alpha^b + 1 + (\alpha+1)^b\right).$$

Note that the polynomial x^m is 0-APN if and only $x^m + 1 + (x+1)^m$ has no root $x \neq 0, 1$, and such m can be classified by Theorem 15 (i). Assume that at least one of x^a and x^b are 0-APN. Then one can always find $\alpha \in \mathbb{F}_{2^n}$ such that

$$\alpha^a + 1 + (\alpha+1)^a \neq 0 \neq \alpha^b + 1 + (\alpha+1)^b.$$

For example, when x^a is 0-APN, one can choose any $\alpha \neq 0, 1$ outside the roots of $x^b + 1 + (x+1)^b = 0$. Therefore one has

$$z^{a-b} = \beta \frac{\alpha^b + 1 + (\alpha+1)^b}{\alpha^a + 1 + (\alpha+1)^a}.$$

When $\gcd(a-b, 2^n-1) = 1$, the above equation always has a unique solution z for any $\alpha \neq 0, 1$, and one has $y = z\alpha \neq z$, since $\alpha \neq 1$.

We now show the other claims. When $a = 2^c - 1$ and $b = 2^d - 1$, with $\gcd(c-1, n) = 1$ or $\gcd(d-1, n)$, then by Theorem 15, one of x^a or x^b is 0-APN. One has $a - b = 2^d(2^{c-d} - 1)$ and $\gcd(a-b, 2^n-1) = \gcd(2^{c-d} - 1, 2^n - 1) = 2^{\gcd(c-d,n)} - 1$, which becomes one if and only if $\gcd(c-d, n) = 1$. Therefore, when $\gcd(c-d, n) = 1$ the polynomial $x^{2^c-1} + \beta\, x^{2^d-1}$ is not 0-APN by the first part of the proof.

When $a = 2^c + 1$ and $b = 2^d + 1$ with $\gcd(c, n) = 1$ or $\gcd(d, n) = 1$, then by Theorem 15, one of x^a or x^b is 0-APN. One has $a - b = 2^d(2^{c-d} - 1)$ and $\gcd(a - b, 2^n - 1) = \gcd(2^{c-d} - 1, 2^n - 1) = 2^{\gcd(c-d,n)} - 1$ which becomes one if and only if $\gcd(c-d, n) = 1$. Therefore, when $\gcd(c-d, n) = 1$, the polynomial $x^{2^c+1} + \beta\, x^{2^d+1}$ is not 0-APN.

When $a = 2^c + 1$ and $b = 2^d - 1$ with $\gcd(c, n) = 1$ or $\gcd(d-1, n) = 1$, then by Theorem 15, one of x^a or x^b is 0-APN. One has $a - b = 2^c - 2^d + 2$ and $\gcd(a-b, 2^n - 1) = \gcd(2^{c-1} - 2^{d-1} + 1, 2^n - 1)$. Therefore, when $\gcd(2^{c-1} - 2^{d-1} + 1, 2^n - 1) = 1$, the polynomial $x^{2^c+1} + \beta\, x^{2^d-1}$ is not 0-APN.

Lastly, when $a = 2^c - 1$ and $b = 2^d + 1$ with $\gcd(c-1, n) = 1$ or $\gcd(d, n) = 1$, then by Theorem 15, one of x^a or x^b is 0-APN. One has $a - b = 2^c - 2^d - 2$ and $\gcd(a-b, 2^n - 1) = \gcd(2^{c-1} - 2^{d-1} - 1, 2^n - 1)$. Therefore, when $\gcd(2^{c-1} - 2^{d-1} - 1, 2^n - 1) = 1$ the polynomial $x^{2^c-1} + \beta\, x^{2^d+1}$ is not 0-APN. □

From the above examples, one can find many binomials which are not 0-APN for infinitely many extensions of the prime field $\mathbb{F}_2$. For example, both $x^7 + x^3$ and $x^5 + x^3$ are not 0-APN for all finite fields $\mathbb{F}_{2^n}$ when $n > 2$. We can easily generalize (for any odd n) Leander and Rodier's result of Theorem 20 [11] in our next corollary.

Corollary 22. *Assume that n is odd and d is a positive integer with $\gcd(d+1, 2^n-1) = 1$. Then $x^{2^n-2} + \beta\, x^d$ is not 0-APN for any $\beta \in \mathbb{F}_{2^n}^*$.*

Proof. Observe that x^{2^n-2} is APN for n odd. By the previous theorem $x^{2^n-2} + \beta\, x^d$ is not APN if $1 = \gcd(2^n - 2 - d, 2^n - 1) = \gcd(2^n - 1, d+1)$ and the proof is done. □

REFERENCES

[1] Y. Aubry, G. McGuire, F. Rodier, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, 23–31, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[2] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[3] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, B. Sun, *On upper bounds for algebraic degrees of APN functions*, IEEE Trans. Inf. Theory 64:6 (2018), 4399–4411.

[4] L. Budaghyan, C. Carlet, G. Leander, *On a construction of quadratic APN functions*, Proc. of IEEE Information Theory workshop ITW'09, Oct. 2009, pp. 374–378.

[5] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[6] C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.

[7] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Adva. in Crypt.–EUROCRYPT'94, LNCS 950, pp. 356–365, 1995.

[8] P. Charpin, G. M. Kyureghyan, *On sets determining the differential spectrum of mappings*, Internat. J. Inf. Coding Theory 4(2-3) (2017), 170–184.
[9] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.
[10] E. Férard, R. Oyono, F. Rodier, *Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents*, Arithmetic, geometry, cryptography and coding theory, 27–36, Contemp. Math., 574, Amer. Math. Soc., Providence, RI, 2012.
[11] G. Leander, F. Rodier, *Bounds on the degree of APN polynomials: the case of* $x^{-1} + g(x)$, Des. Codes Cryptogr. 59(1-3)(2011), 207–222.
[12] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge university press, 1994.
[13] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.
[14] F. Rodier, *Functions of degree* $4e$ *that are not APN infinitely often*, Cryptogr. Commun. 3:4 (2011), 227–240.
[15] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M. Tsfasman eds., Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169–181, 2009.
[16] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.

Paper VIII

Partially APN functions with APN-like polynomial representations

Lilya Budaghyan, Nikolay S. Kaleyski, Constanza S. Riera, Pantelimon Stanica
Designs, Codes and Cryptography, **vol. 88, pp. 1159-1177** (2020)

Partially APN functions with APN-like polynomial representations

Lilya Budaghyan[1], Nikolay S. Kaleyski[1], Constanza Riera[2], and Pantelimon Stănică[3]

[1]*Department of informatics, University of Bergen*
[2]*Department of Computing, Mathematics, and Physics, Western Norway University of Applied Sciences*
[3]*Department of Applied Mathematics, Naval Postgraduate School*

Abstract

In this paper we investigate several families of monomial functions with APN-like exponents that are not APN, but are partially 0-APN for infinitely many extensions of the binary field $\mathbb{F}_2$. We also investigate the differential uniformity of some binomial partial APN functions. Furthermore, the partial APN-ness for some classes of multinomial functions is investigated. We show also that the size of the pAPN spectrum is preserved under CCZ-equivalence.

I. Introduction

The objects of this study are functions over the field with 2^n elements and some of their differential properties. For more on these objects the reader can consult [3], [7], [8], [12]. We will introduce here only some needed notions.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements for some positive integer n. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables and denote the set of all such functions by $\mathcal{B}_n$. For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer valued function

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)},$$

where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Given a Boolean function f, the derivative of f in direction $a \in \mathbb{F}_{2^n}$ is the Boolean function D_aF defined by $D_af(x) = f(x + a) + f(x)$.

A vectorial Boolean function (often called an (n, m)-function) is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for some positive integers m and n. When $m = n$, it can be represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field with the vector space), namely

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i,\ a_i \in \mathbb{F}_{2^n}.$$

Any positive integer $k \leq 2^n - 1$ can be represented as a sum $k = \sum_{i=0}^{n-1} k_i \cdot 2^i$, with $a_i \in \{0, 1\}$. The *2-weight* of k is then $wt(k) = \sum_{i=0}^{n-1} k_i$, i.e. the number of powers of two that add up to k. The *algebraic degree* of the function is then the largest 2-weight of an exponent i with $a_i \neq 0$.

In general, for an (n, m)-function F, we define the Walsh transform $W_F(a, b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is,

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x)) + \mathrm{Tr}_1^n(ax)}.$$

For an (n, n)-function F, and $a, b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} \,|\, F(x + a) + F(x) = b\}|$. We call the quantity $\Delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F \leq \delta$, then we say that F is *differentially δ-uniform*. If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function. There are several equivalent characterizations of APN-ness, and we state some below.

Lemma I.1. *([8], [10], [17]) Let F be an (n, n)-function.*

(i) *The following inequality is always true:*

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^4(a, b) \geq 2^{3n+1}(3 \cdot 2^{n-1} - 1),$$

with equality if and only if F is APN.

(ii) *If, in addition, F is APN and satisfies $F(0) = 0$, then*

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^3(a, b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1).$$

(iii) *(Rodier Condition) F is APN if and only if all the points x, y, z satisfying*

$$F(x) + F(y) + F(z) + F(x + y + z) = 0,$$

belong to $(x + y)(x + z)(y + z) = 0$.

We introduced in [6] a notion of partial APN-ness in our attempt to resolve a conjecture on the upper bound on the algebraic degree of APN functions [5].

Definition I.2. *For a fixed $x_0 \in \mathbb{F}_{2^n}$, we call an (n, n)-function a (*partial*) x_0-*APN function *(which we typically refer to as simply x_0-APN, partially APN or pAPN for short) if all points, x, y, satisfying*

$$F(x_0) + F(x) + F(y) + F(x_0 + x + y) = 0 \tag{1}$$

belong to the curve

$$(x_0 + x)(x_0 + y)(x + y) = 0. \tag{2}$$

We refer to the set of points x_0 for which F is x_0-APN as the pAPN spectrum *of F.*

Certainly, a function is APN if and only if it is x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$. We refer to equation (1) as the *Rodier equation*.

An alternative way to express the fact that a given function F is x_0-APN is to say that, for any $a \neq 0$, the equation $F(x + a) + F(x) = F(x_0 + a) + F(x_0)$ has only two solutions x, namely x_0 and $x_0 + a$.

The remainder of the paper is organized as follows. In the next section, we show that the size of the pAPN spectrum is preserved under CCZ-equivalence. In Section III, we observe a connection between the pAPN-ness of a vectorial Boolean function and its associated Boolean code. Next, in Section IV, we theoretically and experimentally investigate the partial APN-ness of monomial functions. We consider

monomial functions which are known to be APN under certain conditions, and find conditions under which they are partially APN. In Section V, we show that the binomial $F(x) = x^{2^n-1} + x^{2^n-2}$ over $\mathbb{F}_{2^n}$ is 1-APN but not 0-APN for $n \geq 3$. In Section VI we derive some conditions under which a polynomial of the form $F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q}$ for $q = 2^k, 2^k + 1$ with $1 \leq k \leq n-1$ is (not) partially APN (this class of polynomials was suggested by Dillon as containing potential APN or differentially 4-uniform functions). Since every APN function is 0-APN as well, some of the results from Sections IV, V and VI can be seen as non-existence results for APN functions.

II. The size of the pAPN spectrum is preserved under CCZ-equivalence

We first recall that two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ are *CCZ-equivalent* [9] if there exists an affine permutation $\mathcal{A}$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ such that $\{(x, G(x)), x \in \mathbb{F}_{2^n}\} = \mathcal{A}(\{(x, F(x)), x \in \mathbb{F}_{2^n}\})$. As in [9], we use the natural identification of the elements in $\mathbb{F}_{2^n}$ with the elements in $\mathbb{F}_2^n$, and denote by x both an element in $\mathbb{F}_{2^n}$ and the corresponding element in $\mathbb{F}_2^n$.

Theorem II.1. *The size of the pAPN spectrum is preserved under CCZ-equivalence. More precisely, if F and G are two CCZ-equivalent (n,n)-functions and $\mathcal{A}$ is the corresponding CCZ-isomorphism, and denoting the respective pAPN spectra of F, G by S_F, S_G, if $x_0 \in S_F$, and $(\tilde{x}_0, G(\tilde{x}_0)) = \mathcal{A}(x_0, F(x_0))$, we have that $\tilde{x}_0 \in S_G$.*

Proof. We first decompose the affine permutation as an affine block-matrix, $\mathcal{A}\mathbf{u} = \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \mathbf{u} + \begin{pmatrix} c \\ d \end{pmatrix}$, for an input vector $\mathbf{u}$, where $\mathcal{A}_{11}, \mathcal{A}_{21}, \mathcal{A}_{12}, \mathcal{A}_{22}$ are matrices in $\mathbb{F}_{2^n}$, and $\begin{pmatrix} c \\ d \end{pmatrix}$ is a column vector in $\mathbb{F}_{2^{2n}}$.

We assume that F is x_0-APN, and we want to show that G is $\tilde{x}_0$-APN, where $\tilde{x}_0 = \mathcal{A}_{11}x_0 + \mathcal{A}_{12}F(x_0) + c$. For that, we consider the Rodier equation of G at $\tilde{x}_0$, namely

$$G(\tilde{x}_0) + G(\tilde{x}) + G(\tilde{y}) + G(\tilde{x}_0 + \tilde{x} + \tilde{y}) = 0. \tag{3}$$

To simplify notation, we let $\tilde{z} = \tilde{x}_0 + \tilde{x} + \tilde{y}$. We know that there exist x_0, x, y, z such that

$$\begin{aligned} &\tilde{x}_0 = \mathcal{A}_{11}x_0 + \mathcal{A}_{12}F(x_0) + c, \quad \tilde{x} = \mathcal{A}_{11}x + \mathcal{A}_{12}F(x) + c, \\ &\tilde{y} = \mathcal{A}_{11}y + \mathcal{A}_{12}F(y) + c, \quad \tilde{z} = \mathcal{A}_{11}z + \mathcal{A}_{12}F(z) + c, \\ &G(\tilde{x}_0) = \mathcal{A}_{21}x_0 + \mathcal{A}_{22}F(x_0) + d, \quad G(\tilde{x}) = \mathcal{A}_{21}x + \mathcal{A}_{22}F(x) + d, \\ &G(\tilde{y}) = \mathcal{A}_{21}y + \mathcal{A}_{22}F(y) + d, \quad G(\tilde{z}) = \mathcal{A}_{21}z + \mathcal{A}_{22}F(z) + d. \end{aligned} \tag{4}$$

Observe that if $\tilde{x}_0 + \tilde{x} + \tilde{y} + \tilde{z} = 0$, then

$$\mathcal{A}_{12}\left(F(x_0) + F(x) + F(y) + F(z)\right) = \mathcal{A}_{11}\left(x_0 + x + y + z\right).$$

Similarly, The Rodier equation (3) for G at $\tilde{x}_0$ becomes

$$\mathcal{A}_{22}\left(F(x_0) + F(x) + F(y) + F(z)\right) = \mathcal{A}_{21}\left(x_0 + x + y + z\right).$$

We can write the previous identities in matrix form, namely

$$\mathcal{A}\left(\begin{pmatrix} x_0 \\ F(x_0) \end{pmatrix} + \begin{pmatrix} x \\ F(x) \end{pmatrix} + \begin{pmatrix} y \\ F(y) \end{pmatrix} + \begin{pmatrix} z \\ F(z) \end{pmatrix}\right) = 0,$$

to which we can apply $\mathcal{A}^{-1}$, obtaining

$$x_0 + x + y + z = 0 \text{ and } F(x_0) + F(x) + F(y) + F(z) = 0. \tag{5}$$

Now, since $z = x_0 + x + y$ and F is x_0-APN, then equation (5) has only the trivial solutions on $(x_0 + x)(x_0 + y)(x + y) = 0$. Therefore, $(\tilde{x}_0 + \tilde{x})(\tilde{x}_0 + \tilde{y})(\tilde{x} + \tilde{y}) = 0$, and the result is shown. □

III. The Boolean code of a pAPN function

In [9], a result was shown on the minimal distance of the Boolean code associated to a Boolean function. We give a brief overview of that result here (only for the (n, n)-functions relevant to this paper). For an (n, n)-function, $F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j$, with $F(0) = 0$, let $\mathcal{C}_F$ be the $[2^n - 1, k, d]$ linear code defined by the generator matrix

$$\mathcal{G}_F = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{2^n-2}) \end{pmatrix},$$

where each entry is regarded as a binary vector. The codewords are then of the form $(\mathrm{Tr}_1^n(ax) + \mathrm{Tr}_1^n(bF(x)))_{x \in \mathbb{F}_{2^n}}$, where $a, b \in \mathbb{F}_{2^n}$.

It was shown in [9, Theorem 5] (see also [11]) that the code $\mathcal{C}_F$ has minimal distance $3 \leq d \leq 5$, and $d = 5$ if and only if F is APN. It is easy to see that if F is a monomial then $\mathcal{C}_F$ is cyclic (and the 0-APN property is equivalent to the code having minimal distance 4). One might venture the claim that perhaps the pAPN functions that are not APN may have constant minimal distance 4. However, we can find examples of pAPN (but not APN) functions both with $d = 3$ and with $d = 4$. For example, for $F(x) = x^3 + \mathrm{Tr}_1^5(x^7)$, which is $0, 1$-APN on $\mathbb{F}_{2^5}$, one can check that the minimal distance is $d = 4$, while for $F(x) = x^3 + x^{127}$, which is pAPN for 64 values on $\mathbb{F}_{2^7}$, the minimal distance is $d = 3$.

IV. Partial x_0-APN monomials

In [6], a list of exponents i for which x^i is 0-APN but not APN over $\mathbb{F}_{2^n}$ was computed. This list is given as Table I in this paper. We observe that the function x^{21} appears for various dimensions, which raises the natural question of whether this is merely a coincidence or is the consequence of a more general rule. As our first result, we show that the latter is true.

Proposition IV.1. *The function $F(x) = x^{21}$ is 0-APN if and only if n is not a multiple of 6.*

Proof. Let $F(x) = x^{21}$, and $x_0 = 0$. Then the conditions expressed by (1) and (2) state that the equality

$$x^{21} + y^{21} + (x + y)^{21} = 0 \tag{6}$$

implies

$$xy(x + y) = 0.$$

Assuming $y \neq 0$ and dividing both sides of (6) by y^{21}, we get

$$a^{21} + (a + 1)^{21} + 1 = 0$$

n	Exponents i	Δ_F
1-5	-	-
6	27	12
7	7,21,31,55	6
	19,47	4
8	15,45	14
	21,111	4
	51	50
	63	6
9	7,21,35,61,63,83,91,111,117,119,175	6
	41,187	8
	45,125	4
10	15, 27, 45, 75, 111, 117, 147, 189, 207, 255	6
	21, 69, 87, 237, 375	4
	51	8
	93	92
	105, 351	10
	231, 363, 495	42
	447	12
11	79, 109, 183, 251, 367, 463, 695, 703	4
	7, 11, 15, 21, 29, 31, 37, 47, 49, 51, 53, 55, 67, 71, 73, 75, 81, 83, 85, 99, 101, 103, 111 113, 121, 125, 127, 137, 139, 149, 153, 155, 157, 159, 167, 171, 173, 179, 181, 185, 187, 189, 191, 201, 203, 205, 213, 215, 217, 219, 221, 223, 229, 247, 255, 293, 295, 301, 307, 309, 311, 317, 319, 331, 333, 335, 339, 341, 343, 347, 351, 359, 371, 373, 375, 379, 381, 383, 423, 427, 443, 469, 471, 475, 477, 479, 491, 493, 495, 507, 511, 687, 727, 731, 735, 751, 763, 767, 879, 887, 959, 991	6
	19, 25, 27, 39, 41, 45, 61, 77, 87, 91, 105, 119, 123, 141, 147, 163, 165, 175, 199, 211, 233, 235, 237, 239, 349, 363, 415, 429, 431, 439, 501, 503, 699, 895	8
	59, 93, 169, 243, 303, 509	10
	245, 447	16
	23, 69, 115, 207, 253, 299, 437, 759	22
	89, 445	88

TABLE I: Power functions $F(x) = x^i$ over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 10$ that are 0-APN but not APN

where $a = x/y$. This simplifies to

$$a^{19} + a^{16} + a^{15} + a^4 + a^3 + 1 = 0,$$

which can be written as

$$(a+1)(a^6 + a^3 + 1)(a^6 + a^4 + a^3 + a + 1)(a^6 + a^5 + a^3 + a^2 + 1) = 0. \quad (7)$$

Note that $F(x) = x^{21}$ is 0-APN if and only if $a = 1$ is the only root of the polynomial on the left-hand side of (7).

It can be easily verified that each of the three polynomials of degree six is irreducible over $\mathbb{F}_2$. We now use [16, Theorem 3.46], which states that if a degree ℓ polynomial f is irreducible over $\mathbb{F}_q$ and $n \in \mathbb{N}$, then f factors into d irreducible polynomials in $\mathbb{F}_{q^n}[x]$ of the same degree ℓ/d, where $d = gcd(\ell, n)$. Therefore, the polynomial from (7) has multiple roots if and only if the dimension n of $\mathbb{F}_{2^n}$ is a multiple of six. □

The experimentally computed differential properties of x^{21} for dimensions $n \leq 15$ are given in Table II. The differential spectrum is the multiset $\{\Delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$, with the multiplicity of a given value in this multiset given as a superscript after the value; e.g. the differential spectrum of x^{21} for $n = 2$ contains the value 0 six times and the value 2 six times.

Dimension	Differential uniformity	Differential spectrum
1	2	$0^1, 2^1$
2	6	$0^6, 2^6$
3	6	$0^{42}, 2^7, 6^7$
4	2	$0^{120}, 2^{120}$
5	2	$0^{496}2^{496}$
6	20	$0^{3780}, 12^{126}, 20^{126}$
7	6	$0^{9906}, 2^{5461}, 6^{889}$
8	4	$0^{38760}, 2^{20400}, 4^{6120}$
9	6	$0^{159432}, 2^{78694}, 4^{18396}, 6^{5110}$
10	4	$0^{585156}, 2^{401016}, 4^{61380}$
11	6	$0^{2523951}, 2^{1285516}, 4^{337755}, 6^{45034}$
12	20	$0^{9541350}, 2^{6183450}, 4^{1031940}, 14^{8190}, 20^{8190}$
13	6	$0^{41323595}, 2^{19175131}, 4^{5430633}, 6^{1171313}$
14	8	$0^{163338510}, 2^{80538828}, 4^{20642580}, 6^{3211068}, 8^{688086}$
15	8	$0^{649474707}, 2^{327866602}, 4^{82081335}, 6^{12320392}, 8^{1966020}$

TABLE II: Differential uniformity and differential spectrum of x^{21} over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 15$

The approach described above can easily be generalized to any power function $F(x) = x^\ell$: the polynomial $x^\ell+1+(x+1)^\ell$ can be expressed as the product $p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$ of powers of $\mathbb{F}_2$-irreducible polynomials $p_1, p_2, \dots, p_k$. If at least one of these polynomials has degree at least 2, then F is 0-APN over infinitely many fields $\mathbb{F}_{2^n}$, and is not 0-APN over infinitely many fields. More precisely, F is not 0-APN over $\mathbb{F}_{2^n}$ if n is a multiple of the degree of some p_i with $\deg(p_i) \geq 2$ (since this polynomial will split into a product of linear terms by [16, Theorem 3.46]), and is 0-APN if n is not divisible by the least common multiple of all of those degrees.

We can also try to characterize those power functions $F(x) = x^\ell$ which are 0-APN over any finite field, regardless of its dimension. By the above discussion, the polynomial $F(x)+F(y)+F(x+y)$ in this case can only have two irreducible factors, viz. x and $(x+1)$. Suppose we have the decomposition

$$x^\ell + 1 + (x+1)^\ell = x^\alpha(x+1)^\beta.$$

Let k be defined via $(x+1)^\ell = x^\ell + x^k + \dots + x^{l-k} + 1$. Then we have

$$x^k + \dots + x^{l-k} = x^{\alpha+\beta} + \dots + x^\alpha$$

so that we get $k = \alpha + \beta$ and $l - k = \alpha$, which imply $l = 2\alpha + \beta$.

Theorem IV.2. *Suppose $x^\ell + 1 + (x+1)^\ell$ can be written as*

$$x^\ell + 1 + (x+1)^\ell = x^\alpha(x+1)^\beta$$

for some $\alpha, \beta \in \mathcal{N}$. Then $\alpha = \beta = \ell/3$, and $\ell = 3 \cdot 2^k$ for some $k > 0$. Furthermore, $F(x) = x^\ell$ with $l = 3 \cdot 2^k$ are the only power functions which are 0-APN over any finite binary field. All other power functions are 0-APN and not 0-APN over infinitely many finite binary fields.

Proof. First, we observe that the derivative of $x^\ell + 1 + (x+1)^\ell$ in direction 1 is zero; thus, if $x^\ell + 1 + (x+1)^\ell$ can be written as $x^\alpha(x+1)^\beta$, then

$$x^\alpha(x+1)^\beta + (x+1)^\alpha x^\beta = 0$$

for all $x \in \mathbb{F}_{2^n}$. Suppose $\alpha > \beta$ and $x \neq 0, 1$. Dividing both sides by $x^\beta(x+1)^\beta$, we obtain

$$x^{\alpha-\beta} + (x+1)^{\alpha-\beta} = 0.$$

The polynomial on the left-hand side of this equation then has precisely $2^n - 2$ roots (since 0 and 1 evaluate to non-zero values), hence it can be written in the form $\Pi_{i=1}^{2^n-2}(x+\gamma_i)$ for some $\gamma_i \in \mathbb{F}_{2^n}$. Thus, the degree of $x^{\alpha-\beta} + (x+1)^{\alpha-\beta}$ is $2^n - 2$ and hence $\alpha - \beta > 2^n - 2$. Assuming $\alpha, \beta \leq 2^n$, this implies $\alpha = 2^n - 1$ and $\beta = 0$, so that we have

$$x^\ell + 1 + (x+1)^\ell = x^{2^n-1}.$$

This then implies $\ell > 2^n - 1$.

Thus, assuming $\ell < 2^n$, we must necessarily have $\alpha = \beta$ if $x^\ell + 1 + (x+1)^\ell = x^\alpha(x+1)^\beta$, i.e.

$$x^\ell + 1 + (x+1)^\ell = (x(x+1))^\alpha$$

for some $\alpha \in \mathbb{N}$.

We now prove that $x^\ell + 1 + (x+1)^\ell$ can be written in the form $(x(x+1))^\alpha$ if and only if $\ell = 3 \cdot 2^k$ for some $k \in \mathbb{N}$. First, observe that we can restrict ourselves to the case of ℓ odd, since if we have $\ell = 2\ell'$, then

$$(x(x+1))^\alpha = x^\ell + 1 + (x+1)^\ell = (x^{l'} + 1 + (x+1)^{l'})^2$$

implies $x^{\ell'} + 1 + (x+1)^{\ell'} = (x(x+1))^{\alpha/2}$. Thus, let $\ell = 2m+1$ for $m \in \mathbb{N}$. Note that the binomial coefficients $\binom{2m+1}{1} = \binom{2m+1}{2m} = 2m+1$ are always odd, so that x^{2m} is the term with largest and x is the term with smallest exponent in $x^\ell + 1 + (x+1)^\ell$. Suppose $\alpha > 1$. Then the term with smallest exponent in $(x(x+1))^\alpha$ is x^α which contradicts x being the term with smallest exponent. Thus $a = 1$, and $x^\ell + 1 + (x+1)^\ell = x(x+1)$. It is now easy to see that this implies $\ell = 3$. Hence, the exponents ℓ for which $x^\ell + 1 + (x+1)^\ell$ is of the form $(x(x+1))^\alpha$ are precisely those of the form $\ell = 3 \cdot 2^k$, and $a = 2^k$. Finally, from the above discussion, we have that the exponents $\ell = 3 \cdot 2^k$ are precisely those for which x^ℓ is 0-APN over all finite fields $\mathbb{F}_{2^n}$, regardless of the dimension n. □

a) :

Remark IV.3. *The same approach can be used for a polynomial function F as well, however it is not possible to restrict the choice of (x, y) to pairs of the type $(x, 1)$ in general so that we would have to factorize $F(x) + F(y) + F(x+y)$ for all possible values of y in order to obtain a necessary and sufficient condition for F to be 0-APN. Selecting some concrete y, e.g. $y = 1$, would however allow us to obtain a necessary condition for the 0-APN-ness of F.*

It is also interesting whether a characterization of 1-APN-ness as the one discussed in this section can be obtained for e.g. $F(x) = x^{21}$. In this case, we consider the polynomial $x^{21} + y^{21} + (x+y+1)^{21} + 1$ which can be written as

$$\left(\frac{x}{y+1}\right)^{20} + \left(\frac{x}{y+1}\right)^{17} + \left(\frac{x}{y+1}\right)^{16} + \left(\frac{x}{y+1}\right)^{5} + \left(\frac{x}{y+1}\right)^{4} + \left(\frac{x}{y+1}\right) + \frac{y}{(y+1)^{17}} + \frac{y^4}{(y+1)^5} + \frac{y^{16}}{(y+1)^{20}} = 0.$$

This seems more difficult to handle than the 0-APN-ness by this method, however.

We showed in [6] that the Gold function $f_1(x) = x^{2^t+1}$ is 0-APN if and only if $\gcd(n, t) = 1$, which is known to be also equivalent to f_1 being APN. One would

wonder (as we suggested in [6] for monomial functions) if perhaps under $\gcd(n,t) \neq 1$, the Gold function is 1-APN. We shall see below that in reality, the Gold function is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$, under $\gcd(n,t) \neq 1$. Note that the derivatives of the Gold functions are known to be 2^d-to-1 maps for some natural d, so that such a function is either APN, or not x_0-APN for any x_0. We now state and prove our main theorem in this section.

Theorem IV.4. *The following are true:*

- (i) *Let $f_1(x) = x^{2^t+1}$ be the Gold function on $\mathbb{F}_{2^n}$ (known to be APN for $\gcd(t,n) = 1$). If $\gcd(n,t) = d > 1$, then f_1 is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$.*
- (ii) *Let $f_2(x) = x^{2^r-2^t+1}$, $r > s$, be the generalization of the Kasami function $x \mapsto x^{2^{2t}-2^t+1}$ on $\mathbb{F}_{2^n}$ (known to be APN for $\gcd(t,n) = 1$). Then, f_2 is 0-APN if and only if $\gcd(t,n) = \gcd(r-t,n) = d = 1$. Moreover, if $\gcd(t,r-t,n) > 1$, then f_2 is not ζ^k-APN, where ζ is a (2^n-1)-primitive root of unity, and $k \equiv 0 \pmod{\frac{2^n-1}{2^d-1}}$.*
- (iii) *Let $f_3(x) = x^{2^r+2^t-1}$, $r > t$, be the generalization of the Niho function $x \mapsto x^{2^{2t}+2^t-1}$ on $\mathbb{F}_{2^n}$ (known to be APN for $n = 2r+1$, $2t = r$; or, $n = 2t+1$ and $2r = 3t+1$). Then, f_3 is 0-APN if and only if $\gcd(r,n) = \gcd(t,n) = 1$. Note that, for $t = 2$, this includes $f(x) = x^{2^r+3}$, the Welch function (known to be APN for $n = 2r+1$). Then, f is 0-APN if and only of n is odd and $\gcd(r,n) = 1$. If $t = 1$, this case includes the Gold function f_1, as well, but only for $x_0 = 0$.*
- (iv) *Let $f_4(x) = x^{2^{2t}+2^t+1}$ be the Bracken-Leander function on $\mathbb{F}_{2^n}$ (we do not necessarily impose the condition $n = 4t$). If t is odd, then f_4 is not 0-APN on any $\mathbb{F}_{2^n}$ when n is even. If $n = 4t$ and t even, then f is 0-APN.*
- (v) *Let $f_5(x) = x^{2^n-2^s}$ (which coincides with the inverse function x^{-1} extended by $0^{-1} = 0$ for $s = 1$). Then, f_5 is 0-APN if and only if $\gcd(n, s+1) = 1$.*

Remark IV.5. *Note that the case (iv) includes the function $F(x) = x^{21}$. In that particular case, however, we were able to prove a stronger result than the one contained in (iv) above.*

Proof. We proved in [6] that f_1 is 0-APN if and only if $\gcd(n,t) = 1$. We will show next that f_1 is not x_0-APN under $\gcd(n,t) = d > 1$, for any $x_0 \neq 0$. Let ζ be a (2^n-1)-primitive root of unity, and write $x_0 = \zeta^k$, for some $0 \leq k \leq 2^n-2$. Recall that $\gcd(2^t-1, 2^n-1) = 2^d-1$. The Rodier equation (1) for f_1 at x_0 becomes

$$\begin{aligned} 0 &= \zeta^{k(2^t+1)} + x^{2^t+1} + y^{2^t+1} + (x+y+\zeta^k)^{2^t+1} \\ &= \zeta^{k(2^t+1)} + x^{2^t+1} + y^{2^t+1} + (\zeta^{k2^t} + x^{2^t} + y^{2^t})(\zeta^k + x + y) \\ &= xy^{2^t} + yx^{2^t} + (x+y)\zeta^{k2^t} + \zeta^k(x+y)^{2^t}, \end{aligned}$$

which is equivalent (using $y = ax$, and assuming $xy \neq 0$) to

$$x^{2^t} a(a^{2^t-1}+1) + x^{2^t-1}\zeta^k(a^{2^t}+1) + (a+1)\zeta^{k2^t} = 0.$$

Now, let $a \in \mathbb{F}_{2^d} \setminus \mathbb{F}_2$, and so, $a^{2^t-1} = \left(a^{2^d-1}\right)^{\frac{2^t-1}{2^d-1}} = 1$. Further, $a^{2^t}+1 = a+1$, and so, dividing by $(a+1)\zeta^k$, the previous equation becomes $x^{2^t-1} = \zeta^{k(2^t-1)}$, which certainly holds if we take $x = \zeta^{k+\frac{2^n-1}{2^d-1}} \neq \zeta^k$. Therefore, f_1 is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$, under $\gcd(n,t) > 1$.

Now, let $f_2(x) = x^{2^r-2^t+1}$ be the generalization of the Kasami function. Multiplying the Rodier equation for f_2 at 0 by $(x+y)^{2^t}$, we get

$$\begin{aligned} 0 &= (x+y)^{2^t}\left(x^{2^r-2^t+1} + y^{2^r-2^t+1} + (x+y)^{2^r-2^t+1}\right) \\ &= \left(x^{2^t} + y^{2^t}\right)\left(x^{2^r-2^t+1} + y^{2^r-2^t+1}\right) + (x+y)^{2^r}(x+y) \\ &= x^{2^r-2^t+1}y^{2^t} + y^{2^r-2^t+1}x^{2^t} + x^{2^r}y + xy^{2^r}. \end{aligned}$$

Label $y = ax$. Then, assuming $xy \neq 0$, $a \neq 0, 1$, the equation above becomes

$$\begin{aligned} 0 &= a^{2^r} + a^{2^t} + a^{2^r-2^t+1} + a \\ &= a^{2^t}(a^{2^r-2^t} + 1) + a(a^{2^r-2^t} + 1) \\ &= (a^{2^t} + a)(a^{2^t(2^{r-t}-1)} + 1) \\ &= a(a^{2^t-1} + 1)(a^{2^{r-t}-1} + 1)^{2^t} = 0. \end{aligned}$$

If we assume that $a \neq 1$ satisfies $a^{2^t-1}+1 = 0$, then $\gcd(2^t-1, 2^n-1) = 2^{\gcd(t,n)}-1 > 1$, and so $\gcd(t,n) > 1$. Similarly, if $a^{2^{r-t}-1} + 1 = 0$, $a \neq 1$, then $\gcd(2^{r-t}-1, 2^n-1) = 2^{\gcd(r-t,n)} - 1 > 1$, that is, $\gcd(r-t,n) > 1$.

We conclude that the above equation has no solutions outside of $a = 0, 1$ if and only if $\gcd(t,n) = \gcd(r-t,n) = 1$.

Next, let $\gcd(t, r-t, n) = d > 1$. Multiplying the Rodier equation of f_2 at ζ^k by $(x+y+\zeta^k)^{2^t}$, we get

$$\begin{aligned} &(x+y+\zeta^k)^{2^t}\left(x^{2^r-2^t+1} + y^{2^r-2^t+1} + \zeta^{k(2^r-2^t+1)}\right) + (x+y+\zeta^k)^{2^r}(x+y+\zeta^k) \\ = \;& x^{2^t}y^{2^r-2^t+1} + y^{2^t}x^{2^r-2^t+1} + y^{2^t}\zeta^{k(2^r-2^t+1)} + x^{2^t}\zeta^{k(2^r-2^t+1)} \\ &+\zeta^{k2^t}(x^{2^r-2^t+1} + y^{2^r-2^t+1}) + yx^{2^r} + xy^{2^r} + \zeta^k(x^{2^r} + y^{2^r}) + \zeta^{k2^r}(x+y), \end{aligned}$$

and using $\zeta^{k(2^t-1)} = \zeta^{k(2^r-1)} = 1$ (both identities can be shown by observing that $k = m \cdot \frac{2^n-1}{2^d-1}$ for some integer m and so, both $k(2^t-1)$ and $k(2^r-1)$ are multiples of 2^n-1), along with the substitution $y = ax$, we get

$$\begin{aligned} &x^{2^r+1}(a^{2^r} + a^{2^r-2^t+1} + a^{2^t} + a) + x^{2^r}\zeta^k(a^{2^r} + 1) \\ &+x^{2^t}\zeta^k(a^{2^t} + 1) + x^{2^r-2^t+1}\zeta^k(a^{2^r-2^t+1} + 1) + x(1+a)\zeta^k = 0. \end{aligned}$$

Taking $a \in \mathbb{F}_{2^d} \setminus \mathbb{F}_2$, and so, $a^{2^d-1} = 1$, which implies $a^{2^t-1} = 1$, and observing that the first term above is zero, we get

$$x^{2^r}\zeta^k(a+1) + x^{2^t}\zeta^k(a+1) + x^{2^r-2^t+1}\zeta^k(a+1) + x\zeta^k(a+1) = 0,$$

that is,

$$x^{2^r} + x^{2^t} + x^{2^r-2^t+1} + x = x(x^{2^t-1} + 1)(x^{2^{r-t}-1} + 1)^{2^t} = 0,$$

which has nontrivial solutions if $\gcd(t,n) > 1$.

For $f_3(x) = x^{2^r+2^t-1}$, the Rodier equation at 0 is

$$0 = x^{2^r+2^t-1} + y^{2^r+2^t-1} + (x+y)^{2^r+2^t-1},$$

which multiplied by $x+y$ gives

$$\begin{aligned} 0 &= x^{2^r+2^t} + y^{2^r+2^t} + yx^{2^r+2^t-1} + xy^{2^r+2^t-1} + (x^{2^r} + y^{2^r})(x^{2^t} + y^{2^t}) \\ &= xy^{2^r+2^t-1} + yx^{2^r+2^t-1} + x^{2^r}y^{2^t} + y^{2^r}x^{2^t}. \end{aligned}$$

Writing $y = xa$, the above equation becomes (assuming $x \neq 0$)

$$\begin{aligned} 0 &= a^{2^r+2^t-1} + a^{2^r} + a^{2^t} + a \\ &= a(a^{2^r-1}+1)(a^{2^t-1}+1). \end{aligned}$$

Thus, f is 0-APN if and only if $\gcd(r,n) = \gcd(t,n) = 1$.

The Rodier equation (1) for $f_4(x) = x^{2^{2t}+2^t+1}$ at 0 becomes

$$\begin{aligned} 0 &= x^{2^{2t}+2^t+1} + y^{2^{2t}+2^t+1} + (x+y)^{2^{2t}+2^t+1} \\ &= x^{2^{2t}+2^t+1} + y^{2^{2t}+2^t+1} + (x+y)^{2^{2t}}(x+y)^{2^t}(x+y) \\ &= x^{2^{2t}+1}y^{2^t} + x^{2^{2t}}y^{2^t+1} + x^{2^t+1}y^{2^{2t}} + x^{2^t}y^{2^{2t}+1} + x^{2^{2t}+2^t}y + xy^{2^{2t}+2^t}. \end{aligned}$$

Taking $y = ax$, $a \neq 0, 1$, and dividing by $x^{2^{2t}+2^t+1} \neq 0$, we obtain

$$0 = a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a, \tag{8}$$

or, equivalently,

$$0 = (a^{2^t+1} + a^{2^t} + a)^{2^t} + a(a^{2^t} + a + 1)^{2^t}. \tag{9}$$

If t is odd and n is even, then $3 \mid \gcd(2^{t-1}-1, 2^n-1) = 2^{\gcd(t-1,n)} - 1$ and so, we can choose $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Then $a \neq 0, 1$ and $a^2 + a + 1 = 0$. Further, $a^{2^t} + a + 1 = 0$ (since $a^{2^{t-1}} = a$) and the equation above becomes

$$(a(a+1) + (a+1) + a)^{2^t} = (a^2 + a + 1)^{2^t} = 0,$$

which certainly holds, and so, f_4 is not 0-APN.

Assume now that $n = 4t$ for t even (hence $\gcd(t-1,n) = 1$ and $\gcd(2t-1,n) = 1$). As in [2], we apply the relative trace $\mathrm{Tr}_t^{4t}(x) = x + x^{2^t} + x^{2^{2t}} + x^{2^{3t}}$ to equation (8) and obtain

$$\begin{aligned} 0 &= \mathrm{Tr}_t^{4t}\left(a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a\right) \\ &= a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a \\ &\quad + a^{2^{3t}+2^{2t}} + a^{2^{3t}+2^t} + a^{2^{3t}} + a^{2^{2t}+2^t} + a^{2^{2t}} + a^{2^t} \\ &\quad + a^{2^{4t}+2^{3t}} + a^{2^{4t}+2^{2t}} + a^{2^{4t}} + a^{2^{3t}+2^{2t}} + a^{2^{3t}} + a^{2^{2t}} \\ &\quad + a^{2^{5t}+2^{4t}} + a^{2^{5t}+2^{3t}} + a^{2^{5t}} + a^{2^{4t}+2^{3t}} + a^{2^{4t}} + a^{2^{3t}} \\ &= a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a \\ &\quad + a^{2^{3t}+2^{2t}} + a^{2^{3t}+2^t} + a^{2^{3t}} + a^{2^{2t}+2^t} + a^{2^{2t}} + a^{2^t} \\ &\quad + a^{2^{3t}+1} + a^{2^{2t}+1} + a + a^{2^{3t}+2^{2t}} + a^{2^{3t}} + a^{2^{2t}} \\ &\quad + a^{2^t+1} + a^{2^{3t}+2^t} + a^{2^t} + a^{2^{3t}+1} + a + a^{2^{3t}} \\ &= a + a^{2^t} + a^{2^{2t}} + a^{2^{3t}}, \end{aligned} \tag{10}$$

since $a^{2^{4t}} = a$. Adding the first and second powers of (10) to (8) renders

$$a^2 + a^{2^{3t}+1} + a^{2^{2t}+2^t} + a^{2^{3t}} = 0. \tag{11}$$

Raising this last equation to 2^{2t} we get

$$a^{2^{2t+1}} + a^{2^{5t}+2^{2t}} + a^{2^{4t}+2^{3t}} + a^{2^{5t}} = a^{2^{2t+1}} + a^{2^{2t}+2^t} + a^{2^{3t}+1} + a^{2^t} = 0,$$

which added to (11) gives

$$a^{2^{3t}} + a^{2^{2t+1}} + a^{2^t} + a^2 = 0.$$

Using (10), we obtain

$$a^{2^{2t+1}} + a^{2^{2t}} + a^2 + a = 0,$$

implying

$$(a + a^{2^{2t}})^2 + a + a^{2^{2t}} = (a^{2^{2t}} + a)(a^{2^{2t}} + a + 1) = 0,$$

which has solutions if and only if $a+a^{2^{2t}} = 0$, or $1+a+a^{2^{2t}} = 0$. Substituting $a^{2^{2t}} = a$ into (8) renders

$$a^{2^t+1} + a^2 + a + a^{2^t+1} + a^{2^t} + a = 0,$$

that is,

$$0 = a^{2^t} + a^2 = a^2(a^{2^t-2} + 1) = a^2(a^{2^{t-1}-1} + 1)^2,$$

and so $a^{2^{t-1}-1} = 1$,which is impossible under $\gcd(t-1, n) = 1$. If $a^{2^{2t}} = a + 1$, then (8) becomes $a^2 + a + 1 = 0$, which implies that $a^{2^{2t}} = a^2$. This is equivalent to $a^{2^{2t-1}-1} = 1$, which is impossible if $\gcd(2t-1, n) = 1$.

Lastly, the Rodier equation for $f_5(x) = x^{2^n-2^s}$ at 0 is

$$x^{2^n-2^s} + y^{2^n-2^s} + (x+y)^{2^n-2^s} = 0.$$

Suppose that $x, y \neq 0, 1$, and that $x \neq y$. Let $y = xa$, with $a \neq 0, 1$. Then, we can rewrite the equation as

$$x^{2^n-2^s}\left(1 + a^{2^n-2^s} + (1+a)^{2^n-2^s}\right) = 0.$$

Since $x \neq 0$, this implies that $1 + a^{2^n-2^s} + (1+a)^{2^n-2^s} = 0$. Multiplying by $(1+a)^{2^s}$, renders $a^{2^n-2^s} + a^{2^s} = a^{2^s}(a^{2^{n-s-1}-1} + 1)^{2^{s+1}} = 0$. This equation has solutions if and only if $\gcd(n, s+1) > 1$.

□

Remark IV.6. *We could have referred to (reversed) Dickson polynomials* [14] *in some of the arguments above, but we felt that in this case it would not bring further light to the proofs.*

As in Remark IV.5, it is not difficult to find specific values of exponents that are 0-APN for infinitely many extensions $\mathbb{F}_{2^n}$, but, in this paper, we prefer to give more general results. On the other hand, there are polynomials for which we can find general conditions not to be partial APN (and, consequently, not APN), and we provide such instances below.

Proposition IV.7. *Let $f_6(x) = x^{2^{2s+1}+2^{s+1}+2^s-1}$ be defined on $\mathbb{F}_{2^n}$, where $n \geq 4$ is even. Then f_6 is not 0-APN. Let $f_7(x) = x^{2^{4s}+2^{3s}+2^{2s}+2^s-1}$ be a Dobbertin-like function*[1]*. If s is odd and n is even on $\mathbb{F}_{2^n}$, then f_7 is not 0-APN. For n even, $f_8(x) = x^{2^{2t+1}+5}$ is never 0-APN.*

Proof. The Rodier equation for f_6 at $x_0 = 0$ is

$$x^{2^{2s+1}+2^{s+1}+2^s-1} + y^{2^{2s+1}+2^{s+1}+2^s-1} + (x+y)^{2^{2s+1}+2^{s+1}+2^s-1} = 0,$$

[1]Note that f_7 is known to be APN for $n = 5s$.

rendering, in the same way as before, for $y = ax$ (under $0 \neq x \neq y \neq 0$)

$$a^{2^s+2^{s+1}+2^{2s+1}-1} + a^{2^{s+1}+2^{2s+1}} + a^{2^s+2^{2s+1}} + a^{2^s+2^{s+1}} + a^{2^{2s+1}} + a^{2^{s+1}} + a^{2^s} + a = 0. \quad (12)$$

Since n is even, then we can take $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, and so $a^3 = 1$, implying $a^2 + a + 1 = 0$. For such an a, observe that $a^{2^{s+1}} = a^{2^s} + 1, a^{2^{2s+1}} = a^{2^{2s}} + 1$, and the previous expression becomes

$$\begin{aligned}
&a^{2^s-1}(a^{2^s}+1)(a^{2^{2s}}+1) + (a^{2^s}+1)(a^{2^{2s}}+1) + a^{2^s}(a^{2^{2s}}+1) \\
&\qquad + a^{2^s}(a^{2^s}+1) + a^{2^{2s}} + 1 + a^{2^s} + 1 + a^{2^s} + a \\
=&a^{2^{2s}+2^{s+1}-1} + a^{2^{2s}+2^s-1} + a^{2^{s+1}-1} + a^{2^s-1} + a^{2^{2s}+2^s} + a^{2^{2s}} \\
&\qquad + a^{2^s} + 1 + a^{2^{2s}+2^s} + a^{2^s} + a^{2^{s+1}} + a^{2^s} + a^{2^{2s}} + a + 1 \\
=&a^{2^{2s}-1}(a^{2^s}+1) + a^{2^{2s}+2^s-1} + a^{2^{s+1}-1} + a^{2^s-1} + a^{2^s} + a^{2^s} + 1 + 1 + a \\
=&a^{2^{2s}+2^s-1} + a^{2^{2s}-1} + a^{2^{2s}+2^s-1} + a^{2^{s+1}-1} + a^{2^s-1} + a \\
=&a^{2^{2s}-1} + a^{2^{s+1}-1} + a^{2^s-1} + a = a^{-1}\left(a^{2^{2s}} + a^{2^{s+1}} + a^{2^s} + a^2\right) \\
=&a^{-1}\left(a^{2^{2s}} + a^{2^s} + 1 + a^{2^s} + a^2\right) = a^{-1}\left(a^{2^{2s}} + a^2 + 1\right) = 0,
\end{aligned}$$

since $a^{2^{2s}} = a^{2^{2s-1}}+1 = a^{2^{2s-2}} = \cdots = a^{2^{2s-2s}} = a$, and so $a^{2^{2s}}+a^2+1 = a+a^2+1 = 0$.

Similarly, the Rodier equation for f_7 implies

$$\begin{aligned}
&a^{2^s+2^{2s}+2^{3s}+2^{4s}} + a^{1+2^{2s}+2^{3s}+2^{4s}} + a^{1+2^s+2^{3s}+2^{4s}} + a^{1+2^s+2^{2s}+2^{4s}} \\
&+ a^{1+2^s+2^{2s}+2^{3s}} + a^{1+2^{3s}+2^{4s}} + a^{1+2^{2s}+2^{4s}} + a^{1+2^s+2^{4s}} + a^{1+2^{2s}+2^{3s}} \\
&+ a^{1+2^s+2^{3s}} + a^{1+2^{2s}+2^s} + a^{1+2^{4s}} + a^{1+2^{3s}} + a^{1+2^{2s}} + a^{1+2^s} + a^2 = 0.
\end{aligned}$$

Using a similar method as in the first part of our proposition, with n even, and taking $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$ and s odd, one can show that the above expression is zero, and so, f_7 is not 0-APN.

The Rodier equation for f_8 is

$$x^{2^{2t+1}+5} + y^{2^{2t+1}+5} + (x+y)^{2^{2t+1}+5} = 0,$$

which, when $y = ax$, $a \neq 0, 1$, $x \neq 0$, becomes

$$\begin{aligned}
0 &= 1 + a^{2^{2t+1}+5} + (1 + a^{2^{2t+1}})(1+a)^5 \\
&= 1 + a^{2^{2t+1}+5} + \left(1 + a^{2^{2t+1}}\right)\left(1 + a + a^4 + a^5\right) \\
&= a + a^4 + a^5 + a^{2^{2t+1}} + a^{2^{2t+1}+1} + a^{2^{2t+1}+4}.
\end{aligned}$$

Since n is even, we can take $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, and so $a^3 = 1$, implying $a^2 + a + 1 = 0$. For such an a, observe that $a^4 = a, a^5 = a^2, a^{2^{2t+1}} = a^2, a^{2^{2t+1}+4} = a^{2^{2t+1}+1}$, and the previous expression becomes $a + a + a^2 + a^2 + a^{2^t+1} + a^{2^t+1} = 0$, implying that f_8 is not 0-APN. □

V. Binomial partial APN functions

It was observed in [6] that if a monomial is 0-APN and $0 \neq x_0$-APN for some $x_0 \in \mathbb{F}_{2^n}$, then it is APN. We also know that for any quadratic (n,n)-function F and for any $x_0 \in \mathbb{F}_{2^n}$, F is x_0-APN if and only if it is APN. Similarly, it was suggested and consequently shown in [6] that any partially 1-APN monomial function is APN. It is natural to wonder if such a statement is true for other types of functions. We give below an instance when such a claim fails.

Theorem V.1. *Let $F(x) = x^{2^n-1} + x^{2^n-2}$ be defined on $\mathbb{F}_{2^n}$. Then F is 1-APN, but not 0-APN, for all $n \geq 3$. Furthermore, F is differentially 4-uniform.*

Proof. Let $F(x) = x^{2^n-1}+x^{2^n-2}$, and $x_0 = 1$. Then, the Rodier condition (1) becomes

$$x^{2^n-1} + x^{2^n-2} + y^{2^n-1} + y^{2^n-2} + (x+y+1)^{2^n-1} + (x+y+1)^{2^n-2} = 0,$$

which is equivalent to (since $x^{2^n-1} = 1$, for $x \in \mathbb{F}_{2^n}^*$),

$$1 + x^{-1} + 1 + y^{-1} + 1 + (x+y+1)^{-1} = 0, \text{ assuming } xy(x+y+1) \neq 0.$$

Multiplying the previous equation by $xy(x+y+1)$, we obtain

$$\begin{aligned}
& y(x+y+1) + x(x+y+1) + xy(x+y+1) + xy = 0 \\
\iff & xy + y^2 + y + x^2 + xy + x + x^2y + xy^2 + xy + xy = 0 \\
\iff & x + y + x^2 + y^2 + x^2y + xy^2 = 0 \\
\iff & (x+y)(1 + x + y + xy) = 0 \\
\iff & (x+y)(1+x)(1+y) = 0
\end{aligned}$$

which proves the first claim.

To show that F is not 0-APN, let us consider the Rodier equation for $x_0 = 0$,

$$\begin{aligned}
& x^{2^n-1} + x^{2^n-2} + y^{2^n-1} + y^{2^n-2} + (x+y)^{2^n-1} + (x+y)^{2^n-2} = 0 \\
\iff & 1 + x^{-1} + 1 + y^{-1} + 1 + (x+y)^{-1} = 0 \qquad (13) \\
\iff & y(x+y) + x(x+y) + xy(x+y) + xy = 0 \\
\iff & xy + y^2 + x^2 + xy + x^2y + xy^2 + xy = 0 \\
\iff & (x+y)^2 + xy(x+y) + xy = 0 \\
\iff & 1 + \frac{xy}{x+y} + \frac{xy}{(x+y)^2} = 0. \qquad (14)
\end{aligned}$$

We will find $0 \neq x \neq y \neq 0$ to satisfy the previous equation. Let $t = x + y$. Then, the previous equation is equivalent to (under $xy \neq 0 \neq x + y = t$)

$$\begin{aligned}
& t^2 + x(x+t)(t+1) = 0, \text{ (observe that } t \neq 1) \\
\iff & x^2 + tx + \frac{t^2}{t+1} = 0 \\
\iff & \left(\frac{x}{t}\right)^2 + \frac{x}{t} + \frac{1}{t+1} = 0.
\end{aligned}$$

Labeling $z = \frac{x}{t}$, we obtain the equation

$$z^2 + z + \frac{1}{t+1} = 0.$$

We now use the fact that for $0 \neq v \in \mathbb{F}_{2^n}$ the equation $X^2 + X = v$ has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(v) = 0$ (see Berlekamp et al. [1]). Taking any of the $2^{n-1} - 1$ nontrivial values of $v \in \mathbb{F}_{2^n}^*$ for which $\mathrm{Tr}_1^n(v) = 0$, $t = 1 + v^{-1} \neq 0$ and z a solution of $X^2 + X = v$, we have that $x = tz, y = t(z + 1)$ will satisfy equation (14) and $0 \neq x \neq y \neq 0$, hence F is not 0-APN.

We next show that F is differentially 4-uniform. We first write the equation $D_aF(x) = b$, under $a \neq 0, b \in \mathbb{F}_{2^n}$, namely,

$$x^{2^n-1} + x^{2^n-2} + (x + a)^{2^n-1} + (x + a)^{2^n-2} = b, x \in \mathbb{F}_{2^n}. \tag{15}$$

Case 1. Let $b = 1 + a^{-1}$. We can see that $x = 0$, $x = a$ are solutions of (15). Further, if $x \neq 0, x \neq a$, then (15) becomes $x^{2^n-2} + (x + a)^{2^n-2} = b$, which is equivalent to $x^{-1} + (x + a)^{-1} = b = 1 + a^{-1}$, that is,

$$(a + 1)x^2 + (a^2 + a)x + a^2 = 0. \tag{16}$$

We can see that $a \neq 1$ and so, $a^2 + a \neq 0$, and therefore, by taking $y = xa^{-1}$, we obtain that (16) is equivalent to $y^2 + y = (a+1)^{-1}$, which, by [1] has solutions y (and thus x) if and only if $\mathrm{Tr}_1^n((a + 1)^{-1}) = 0$. There certainly exist $a \in \mathbb{F}_{2^n}$ satisfying this condition, in which case equation (16) has two more solutions, in addition to $0, a$.
Case 2. Let $b \neq 1 + a^{-1}$. Then $x \neq 0, a$ in (15) and so, the first and third terms are equal to 1, and (15) becomes

$$x^{-1} + (x + a)^{-1} = b, \tag{17}$$

that is, $bx^2 + abx + a = 0$, which has at most two solutions x (in general, the equation above may have four solutions if $b = a^{-1}$, namely $\{0, a, a\alpha, a\alpha^2\}$, where $\alpha \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, but we removed $0, a$ from the possibilities because of (15)). In fact, we know exactly when equation (17) has no solutions, namely, when $\mathrm{Tr}_1^n\left(\frac{1}{ab}\right) = 1$.

In conclusion, equation (15) has at most 4 solutions (with that bound attained), and therefore F is differentially 4-uniform. □

Remark V.2. *The non-0-APN-ness of the above function can also be derived from* [6, Thm. 5.5]*, but we prefer to give a self-contained argument above.*

VI. Partial APN functions based on Dillon's polynomial

Dillon [13] suggested investigating functions of the form

$$F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q}, q = 2^{n/2}, n \text{ even}, \tag{18}$$

over $\mathbb{F}_{2^n}$ as candidates for APN or differentially 4-uniform functions. An infinite family of APN functions of this type was constructed in [4]. In this section, we investigate several such functions for being partial APN functions, and consequently, APN functions (recall that we showed in [6] that for quadratic functions, pAPN property is equivalent to the APN property). The motivation for this section is to point out that any of the functions coming from F can be investigated quite easily for APN-ness using the not so restrictive concept of pAPN-ness.

First, we write the Rodier condition at $x_0 = 0$ for the function F above, which we generalize by taking $q = 2^k$ for some arbitrary $1 \leq k \leq n-1$. Now, letting $y = ax$, $a \neq 0, 1, x \neq 0$, we obtain

$$\begin{aligned} 0 =& Ax^3(a+a^2) + Bx^{2^k+1}\left(a+a^{2^k}\right) + Cx^{2^{k+1}+1}\left(a+a^{2^{k+1}}\right) \\ &+ Dx^{2^k+2}\left(a^2+a^{2^k}\right) + Ex^{2^{k+1}+2}\left(a^2+a^{2^{k+1}}\right) + Gx^{2^{k+1}+2^k}\left(a^{2^k}+a^{2^{k+1}}\right). \end{aligned} \tag{19}$$

We will not provide the proof of the next theorem (whose cases are perhaps known via APN-ness), but we will provide the proof of the last theorem of this section, since it is more complicated.

Theorem VI.1. *Let $1 \leq k \leq n-1$ and consider the function F from* (18)*. The following statements hold:*

- (i) *If $AB \neq 0$, $\gcd(k-1,n) = 1$, $k \geq 1$, the function $F_1(x) = Ax^3 + Bx^{2^k+1}$ is not 0-APN. Obviously, if $AC \neq 0$ and $\gcd(k,n) = 1$, then $F_2(x) = Ax^3 + Cx^{2^{k+1}+1}$ is not 0-APN.*
- (ii) *If $AD \neq 0$ and $\gcd(k,n) = 1$, $k > 1$, the function $F_3(x) = Ax^3 + Dx^{2^k+2}$ is not 0-APN. Furthermore, $H_3(x) = Ax^3 + Dx^4$ is 0-APN.*
- (iii) *If $AE \neq 0$ and $\gcd(k+1,n) = 1$, then $F_4(x) = Ax^3 + Ex^{2^{k+1}+2}$ is not 0-APN.*
- (iv) *If $AG \neq 0$ and $\frac{A}{G} \notin \mathbb{F}_{2^n}^{2^k-1}$, then $F_5(x) = Ax^3 + Gx^{3\cdot 2^k}$ is 0-APN; if $AG \neq 0$, $\frac{A}{G} \in \mathbb{F}_{2^n}^{2^k-1}$ and there exists z such that $\mathrm{Tr}_1^n((A/G)^{1/(2^k-1)}/z^3) = 0$, then F_5 is not 0-APN.*
- (v) *If $BC \neq 0$ and $k \geq 1$, then $F_6(x) = Bx^{2^k+1} + Cx^{2^{k+1}+1}$ is not 0-APN.*
- (vi) *If $BD \neq 0$, then $F_7(x) = Bx^{2^k+1} + Dx^{2^k+2}$ is not 0-APN.*
- (vii) *If $BE \neq 0$, then $F_8(x) = Bx^{2^k+1} + Ex^{2^{k+1}+2}$ is not 0-APN, if $\gcd(k,n) > 1$, or n is odd and $\gcd(k,n) = 1$.*
- $(viii)$ *If $BG \neq 0$ and $\gcd(k+1,n) = 1$, then $F_9(x) = Bx^{2^k+1} + Gx^{2^{k+1}+2^k}$ is not 0-APN.*
- (ix) *If $CD \neq 0$ and $\gcd(k,n) = 1$, then $F_{10}(x) = Cx^{2^{k+1}+1} + Dx^{2^k+2}$ is not 0-APN.*
- (x) *If $CE \neq 0$, then $F_{11}(x) = Cx^{2^{k+1}+1} + Ex^{2^{k+1}+2}$ is not 0-APN.*
- (xi) *If $CG \neq 0$, then $F_{12}(x) = Cx^{2^{k+1}+1} + Gx^{2^{k+1}+2^k}$ is not 0-APN.*
- (xii) *If $DE \neq 0$, then $F_{13}(x) = Dx^{2^k+2} + Ex^{2^{k+1}+2}$ is not 0-APN.*
- $(xiii)$ *If $DG \neq 0$, then $\gcd(k,n) = 1$, then $F_{14}(x) = Dx^{2^k+2} + Gx^{2^{k+1}+2^k}$ is not 0-APN.*
- (xiv) *If $EG \neq 0$, then $\gcd(k-1,n) = 1$, then $F_{15}(x) = Ex^{2^{k+1}+2} + Gx^{2^{k+1}+2^k}$ is not 0-APN.*

We can certainly go beyond binomials and we do so in the next theorem without attempting to be exhaustive.

Theorem VI.2. *Let $G \neq 0$, $\gcd(k,n) > 1$, n odd, and $A/G \in \mathbb{F}_{2^n}^{2^k-1}$. Then $F_{16}(x) = Ax^3 + Bx^{2^k+1} + Ex^{2^{k+1}+2} + Gx^{2^{k+1}+2^k}$ is not 0-APN.*

Proof. The Rodier equation (19) for F_{16} at $x_0 = 0$ is equivalent to

$$\begin{aligned} &x^3(a+a^2)\left(A + Gx^{3\cdot(2^k-1)}(a+a^2)^{2^k-1}\right) \\ &\quad + x^{2^k+1}a\left(1+a^{2^k-1}\right)\left(B + Ex^{2^k+1}\left(a+a^{2^k}\right)\right) = 0. \end{aligned}$$

If $\gcd(k,n) > 1$, then taking $a \neq 0, 1$ such that $a^{2^k-1} = 1$, the second term is zero. Furthermore $(a+a^2)^{2^k-1} = a^{2^k-1}(a+1)^{2^k-1} = \frac{(a+1)^{2^k}}{a+1} = \frac{a^{2^k}+1}{a+1} = \frac{a+1}{a+1} = 1$, and so the

first term becomes $x^3(a+a^2)\left(A+Gx^{3\cdot(2^k-1)}\right)$, which is zero for the unique solution x of $x^3=\left(\frac{A}{G}\right)^{1/(2^k-1)}$, which exists since n is odd (that is, $\gcd(3,2^n-1)=1$). □

We now take $q=2^{k+1}$ in Dillon's polynomial (18).

Theorem VI.3. *Let $1\le k\le n-1$. The following statements hold:*

(*i*) *If $AC\neq 0$, then the functions $H_1(x)=Ax^3+Cx^{2^{k+1}+3}$ (respectively, $H_2(x)=Ax^3+Cx^{2^k+3}$) is not 0-APN.*

(*ii*) *If $AG\neq 0$, then the functions $H_3(x)=Ax^3+Gx^{2^{k+1}+2^k+3}$ is not 0-APN if n is odd; if n is even, then H_3 is 0-APN if and only if $\left(\frac{A}{G}\right)^{2^{-k}}\notin\mathbb{F}_{2^2}^*$.*

(*iii*) *If $BC\neq 0$, and $\gcd(2^k+1,2^n-1)=1$, which happens if n is odd, or $n\equiv 2 \pmod 4$ and k is even, then $H_4(x)=Bx^{2^k+2}+Cx^{2^{k+1}+3}$ is not 0-APN.*

(*iv*) *If $BD\neq 0$, $H_5(x)=Bx^{2^k+2}+Dx^{2^k+3}$ is never 0-APN.*

(*v*) *If $BG\neq 0$, and $\gcd(2^{k+1}+1,2^n-1)=1$ (which happens if n is odd, or $n\equiv 2 \pmod 4$ and k is odd), then $H_6(x)=Bx^{2^k+2}+Gx^{2^{k+1}+2^k+2+1}$ is not 0-APN.*

(*vi*) *If $CDEG\neq 0$, then $H_7(x)=Cx^{2^{k+1}+3}+Dx^{2^k+3}$, $H_8(x)=Cx^{2^{k+1}+3}+Ex^{2^{k+1}+4}$, and $H_9(x)=Cx^{2^{k+1}+3}+Gx^{2^{k+1}+2^k+2+1}$ are never 0-APN.*

(*vii*) *If $DE\neq 0$, and $\gcd(2^k+1,2^n-1)=1$, which happens if n is odd, or $n\equiv 2 \pmod 4$ and k is even, then $H_{10}(x)=Dx^{2^k+3}+Ex^{2^{k+1}+4}$ is not 0-APN.*

(*viii*) *If $DG\neq 0$, then $H_{11}(x)=Dx^{2^k+3}+Gx^{2^{k+1}+2^k+2+1}$ is never 0-APN.*

(*ix*) *If $EG\neq 0$ and $gcd(k,n)=1$, then $H_{12}(x)=Ex^{2^{k+1}+4}+Gx^{2^{k+1}+2^k+2+1}$ is not 0-APN.*

Proof. Let $q=2^k+1$ in Dillon's polynomial (18); as before, letting $y=ax$, $x\neq 0$, $a\neq 0,1$, we obtain

$$\begin{aligned}
0 &= Ax^3(a+a^2)+Bx^{2^k+2}\left(a^2+a^{2^k}\right)\\
&+Cx^{2^{k+1}+3}\left(a+a^2+a^3+a^{2^{k+1}}+a^{2^{k+1}+1}+a^{2^{k+1}+2}\right)\\
&+Dx^{2^k+3}\left(a+a^2+a^3+a^{2^k}+a^{2^k+1}+a^{2^k+2}\right)\\
&+Ex^{2^{k+1}+2^2}\left(a^4+a^{2^{k+1}}\right)+Gx^{2^{k+1}+2^k+3}\left(a+a^2+a^3+a^{2^k}+a^{2^k+1}+a^{2^k+2}+a^{2^k+3}+\right.\\
&\left.+a^{2^{k+1}}+a^{2^{k+1}+1}+a^{2^{k+1}+2}+a^{2^{k+1}+3}+a^{2^{k+1}+2^k}+a^{2^{k+1}+2^k+1}+a^{2^{k+1}+2^k+2}\right)\\
&= Ax^3(a+a^2)+Bx^{2^k+2}\left(a^2+a^{2^k}\right)+Cx^{2^{k+1}+3}\left(a+a^2+a^3\right)\left(1+a^{2^{k+1}}\right)\\
&+Dx^{2^k+3}\left(a+a^2+a^3\right)\left(1+a^{2^k}\right)+Ex^{2^{k+1}+2^2}\left(a^4+a^{2^{k+1}}\right) \qquad (20)\\
&+Gx^{2^{k+1}+2^k+3}(1+a)^{2^k}\left((1+a)^{2^{k+1}+3}+(1+a)^{2^{k+1}}+(1+a)^{2^k}+1\right).
\end{aligned}$$

The coefficient of G was simplified in the following way:

$$\begin{aligned}
&\left(1+a^{2^k}\right)\left(\left(a+a^2+a^3\right)\left(1+a^{2^{k+1}}\right)+a^{2^k}\right)\\
=&(1+a)^{2^k}\left(\left(1+a+a^2+a^3\right)\left(1+a^{2^{k+1}}\right)+a^{2^k}+a^{2^{k+1}}+1\right)\\
=&(1+a)^{2^k}\left((1+a)^{2^{k+1}+3}+(1+a)^{2^{k+1}}+(1+a)^{2^k}+1\right)
\end{aligned}$$

We only consider combinations rendering non-quadratic functions. Let $AC \neq 0$, $H_1(x) = Ax^3 + Cx^{2^{k+1}+2+1}$ (similarly, for $AD \neq 0$, $H_2(x) = Ax^3 + Dx^{2^k+3}$). The Rodier equation (20) for H_1 at 0 is therefore

$$Ax^3(a+a^2) = Cx^{2^{k+1}+3}\left(a+a^2+a^3\right)\left(1+a^{2^{k+1}}\right),$$

that is $x^{2^{k+1}} = \frac{A}{C(1+a+a^2)(1+a)^{2^{k+1}-1}}$ (recall that $a \neq 0, 1$ and if a is a primitive third root of unity then the displayed equation above cannot hold for nontrivial solutions x). Since this last equation always has nontrivial solutions, the function H_1 cannot be 0-APN.

Next, $H_3(x) = Ax^3 + Gx^{2^{k+1}+2^k+2+1}$ whose Rodier equation at 0 is

$$Ax^3(a+a^2) = Gx^{2^{k+1}+2^k+3}(1+a)^{2^k}\left((1+a)^{2^{k+1}+3} + (1+a)^{2^{k+1}} + (1+a)^{2^k} + 1\right),$$

which is equivalent to (the expression in the parentheses on the right-hand side cannot be zero, otherwise there are no non-trivial solutions)

$$x^{3\cdot 2^k} = \frac{Ab(b+1)}{G\,b^{2^k}\left(b^{2^{k+1}+3} + b^{2^{k+1}} + b^{2^k} + 1\right)}, \tag{21}$$

where $b = a+1$. If n is odd, then equation (21) will always have nontrivial solutions. If n is even, taking 2^k-th roots on both sides, we obtain

$$u^3 = \left(\frac{A}{G}\right)^{2^{-k}}, \tag{22}$$

where

$$u = xb\left(\frac{b^{2^{k+1}+3} + b^{2^{k+1}} + b^{2^k} + 1}{b(b+1)}\right)^{2^{-k}}$$

is any of the 2^k roots. Certainly, the equation (22) has nontrivial solutions if and only if $\left(\frac{A}{G}\right)^{2^{-k}} \in \mathbb{F}_{2^2}^*$.

Next, take $BC \neq 0$, and $H_4(x) = Bx^{2^k+2} + Cx^{2^{k+1}+3}$. The Rodier equation at 0 is now

$$x^{2^k+1} = \frac{B\left(a^2+a^{2^k}\right)}{C\left(a+a^2+a^3\right)\left(1+a^{2^{k+1}}\right)}.$$

If $\gcd(2^k+1, 2^n-1) = 1$ (which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is even), then the equation above has nontrivial solutions (certainly, for a such that $a \notin \mathbb{F}_4^*$).

If $BD \neq 0$, then it is straightforward to check that the cubic $H_5(x) = Bx^{2^k+2} + Dx^{2^k+3}$ is never 0-APN, since its Rodier equation at 0 is equivalent to

$$x = \frac{B\left(a^2+a^{2^k}\right)}{D\left(a+a^2+a^3\right)\left(1+a^{2^k}\right)},$$

which obviously has nontrivial solutions.

If $BG \neq 0$, then the Rodier equation at 0 for $H_6(x) = Bx^{2^k+2} + Gx^{2^{k+1}+2^k+2+1}$ is (with $b = a + 1$)

$$x^{2^{k+1}+1} = \frac{B\left(b^2 + b^{2^k}\right)}{G\, b^{2^k}\left(b^{2^{k+1}+3} + b^{2^{k+1}} + b^{2^k} + 1\right)}.$$

If $\gcd(2^{k+1} + 1, 2^n - 1) = 1$ (which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is odd), then the equation above has nontrivial solutions (certainly, for a such that the denominator above is not zero, which can easily be achieved).

If $CD \neq 0$, the Rodier equation at 0 for the cubic $H_7(x) = Cx^{2^{k+1}+3} + Dx^{2^k+3}$ is

$$((1 + a)x)^{2^k} = \frac{D}{C}.$$

Since $\gcd(2^k, 2^n - 1) = 1$, the above equation always has nontrivial solutions. A similar straightforward analysis can be done, under $CEG \neq 0$, for the cubics $H_8(x) = Cx^{2^{k+1}+3} + Ex^{2^{k+1}+4}$ and $H_9(x) = Cx^{2^{k+1}+3} + Gx^{2^{k+1}+2^k+2+1}$.

If $DE \neq 0$, the Rodier equation at 0 for $H_{10}(x) = Dx^{2^k+3} + Ex^{2^{k+1}+4}$ renders

$$x^{2^k+1} = \frac{D(a + a^2 + a^3)(1 + a)^{2^k}}{E\left(a^4 + a^{2^{k+1}}\right)},$$

a similar equation as for H_4. If $DG \neq 0$, the Rodier equation at 0 for $H_{11}(x) = Dx^{2^k+3} + Gx^{2^{k+1}+2^k+2+1}$ is similar to the one of H_7.

If $EG \neq 0$, the Rodier equation for the quartic $H_{12}(x) = Ex^{2^{k+1}+4} + Gx^{2^{k+1}+2^k+2+1}$ is equivalent to (with $b = a + 1$)

$$x^{2^k-1} = \frac{E\left(b^4 + b^{2^{k+1}}\right)}{G\, b^{2^k}\left(b^{2^{k+1}+3} + b^{2^{k+1}} + b^{2^k} + 1\right)},$$

which has a nontrivial solution x if $\gcd(k, n) = 1$ (for any value of b for which the denominator does not vanish).

Thus, the theorem is shown. □

Certainly, there are other values of q, for which one can investigate the pAPN property of various combinations of terms in Dillon's polynomial. Furthermore, a fruitful direction for future work is to check and find conditions for pAPN-ness of other classes of multinomials, like the generalization proposed by Budaghyan and Carlet in [4], or perhaps, as a separate and quite interesting venue, to find classes of pAPN permutations.

References

[1] E. R. Berlekamp, H. Rumsey, G. Solomon, *On the solutions of algebraic equations over finite fields*, Information and Control 10 (1967), 553–564.

[2] C. Bracken, G. Leander, *A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree*, Finite Fields Appl. 16 (4) (2010), 231–242.

[3] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[4] L. Budaghyan, C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures*, IEEE Trans. Inform. Theory 54:5 (2008), 2354–2357.

[5] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, B. Sun, *On upper bounds for algebraic degrees of APN functions*, IEEE Trans. Inform. Theory 64:6 (2018), 4399–4411.

[6] L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera, P. Stănică, *Partially APN Boolean functions and classes of functions that are not APN infinitely often*, Cryptography and Communication, 2019; preliminary version as *Partially APN Boolean functions*, Proc. Sequences and Their Applications – SETA 2018, Hong Kong, 2018.

[7] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[8] C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.

[9] C. Carlet, P. Charpin, V. Zinoviev, *Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems*, Des. Codes Cryptogr. 15 (1998), 125–156.

[10] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Advances in Cryptology–EUROCRYPT'94, LNCS 950, pp. 356–365, 1995.

[11] P. Charpin, A. Tietäväinen, V. Zinoviev, *On binary cyclic codes with codewords of weight three and binary sequences with the trinomial property*, IEEE Trans. Inform. Theory 47:1 (2001), 421–425.

[12] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

[13] J. F. Dillon, *APN Polynomials and Related Codes*, Polynomials over Finite Fields and Applications, Banff International Research Station, Nov. 2006.

[14] X. Hou, G. L. Mullen, J. A. Sellers and J. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. 15 (2009), 748–773.

[15] D. R. Hughes, *Collineation groups and non-Desarguesian planes*, American J. Math 81 (1959), 921–938; *ibid.* 82, 113–119.

[16] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.

[17] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman eds., Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169–181, 2009.

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS

uib.no

ISBN: 9788230849026 (print)
9788230848784 (PDF)