A NOTE ON SOME ALGEBRAIC TRAPDOORS
FOR BLOCK CIPHERS

MARCO CALDERINI

Department of Informatics, University of Bergen, Norway

ABSTRACT. We provide sufficient conditions to guarantee that a translation based cipher is not vulnerable with respect to the partition-based trapdoor. This trapdoor has been introduced, recently, by Bannier et al. (2016) and it generalizes that introduced by Paterson in 1999. Moreover, we discuss the fact that studying the group generated by the round functions of a block cipher may not be sufficient to guarantee security against these trapdoors for the cipher.

1. **Introduction.** In the last years, since the work [11] of Coppersmith and Grossman, much attention has been devoted to the group generated by the round functions of a block cipher. In this context, Paterson [17] showed that the imprimitivity of the group can be exploited to construct a trapdoor. By a trapdoor we mean a hidden algebraic structure in the cipher design that would allow an attacker (with the knowledge of the trapdoor) to break it easily. In [9] Caranti, Dalla Volta and Sala introduced the definition of translation based cipher, which contains well-known ciphers like AES [12], SERPENT [1] and PRESENT [8]. For this class of ciphers, in [9] and [2], the authors provided cryptographic conditions on the S-Boxes and the mixing layer, in order to guarantee the primitivity of the group generated by the round functions of the cipher.

In a recent work [5], inspired by the partition cryptanalysis developed in [14], the authors introduce the partition-based trapdoor. This type of trapdoor generalizes that introduced by Paterson. Moreover, the authors give an example of a (toy) block cipher which is not vulnerable with respect to linear [16] and differential attacks [7], but that can be broken, easily, using the structure of the trapdoor. A more sophisticated way to use such a weakness is given in [6].

The principal aim of this work is to investigate an open question left by Paterson in his work [17], that is, if it might be possible to have the case where the round functions generate a primitive group but the subgroup generated by the ℓ-round cipher itself has a block structure. In particular, we want to find cryptographic properties that could avoid such a threat.

In this work, we give some conditions on the S-boxes and the mixing layer of a translation based cipher, in order to avoid the partition-based trapdoor. From this result, we are able to give a security proof for the group of encryption functions of a cipher with independent round-keys.

The paper is organized as follows. In Section 2, we recall some definitions and a series of properties and already known results. In Section 3, we show how we can avoid the partition-based trapdoor on a translation based cipher. Finally, in Section 4, we discuss the fact that studying the group generated by the round functions of a block cipher may not be sufficient to guarantee security against these trapdoors for the cipher, and we show that avoiding the partition-based trapdoor we can give some properties of the group generated by an ℓ-round cipher with independent round-keys. We report our conclusions and some final remarks in Section 5.

2. **Preliminaries and notation.** Let $\mathcal{C}$ be a block cipher acting on a message space $V = (\mathbb{F}_2)^d$, for some $d \geq 1$ (we suppose that V coincides with the ciphertext space). Let $\mathcal{K}$ be its key space. Then any key $k \in \mathcal{K}$ individuates a permutation τ_k on the space V and our cipher is given by the set

$$\mathcal{C} = \{\tau_k \mid k \in \mathcal{K}\}.$$

We are interested in determining the properties of the group $\Gamma(\mathcal{C}) = \langle \tau_k \mid k \in \mathcal{K} \rangle$. Unfortunately, the study of $\Gamma(\mathcal{C})$ is a difficult task, in general. Most modern block ciphers are iterated ciphers, i.e., obtained by a composition of several key-dependent permutations, called rounds. This allows to investigate an other permutation group related to $\mathcal{C}$. For an iterated block cipher $\mathcal{C}$ each τ_k is a composition of some permutations of V, say $\tau_{k,1}, ..., \tau_{k,\ell}$. For any round h, let

$$\Gamma_h(\mathcal{C}) = \langle \tau_{k,h} \mid k \in \mathcal{K} \rangle,$$

therefore, we can define the group containing $\Gamma(\mathcal{C})$ generated by the round functions

$$\Gamma_\infty(\mathcal{C}) = \langle \Gamma_h(\mathcal{C}) \mid h = 1, ..., \ell \rangle.$$

2.1. **Translation based ciphers.** Here we consider translation based ciphers, introduced in [9]. This class of iterated block ciphers includes some well-known ciphers, as for instance AES [12] and SERPENT [1].

We first fix the notation, in order to recall the definition of a translation based cipher $\mathcal{C}$. Let $m, b > 1$ and

$$V = V_1 \oplus \cdots \oplus V_b,$$

where each V_i is isomorphic to $(\mathbb{F}_2)^m$. We will denote by $\mathrm{Sym}(V)$ the symmetric group on V. Given $v \in V$, we write $\sigma_v \in \mathrm{Sym}(V)$ for the translation of V mapping x to $x + v$. We denote by $T(V)$ the group of all translations of V. We will write the action of $g \in \mathrm{Sym}(V)$ on an element $v \in V$ as vg.

For any $v \in V$, we will write $v = v_1 \oplus \cdots \oplus v_b$, where $v_i \in V_i$. Also, we consider the projections $\pi_i : V \to V_i$ mapping $v \mapsto v_i$.

Any $\gamma \in \mathrm{Sym}(V)$ that acts as $v\gamma = v_1\gamma_1 \oplus \cdots \oplus v_b\gamma_b$, for some $\gamma_i \in \mathrm{Sym}(V_i)$, is called *bricklayer transformation* (a "parallel map") and any γ_i's is a *brick*. Traditionally, the maps γ_i's are called S-boxes and γ a "parallel S-box". A linear map $\lambda : V \to V$ is traditionally said a "Mixing Layer" when used in composition with parallel maps. For any $I \subset \{1, ..., b\}$, with $I \neq \emptyset$ and $I \neq \{1, ..., b\}$, we define $\bigoplus_{i \in I} V_i$ a *wall*.

Definition 2.1. A linear map $\lambda \in \mathrm{GL}(V)$ is called a *proper mixing layer* if no wall is invariant under λ.

We can characterize translation-based block ciphers by the following:

Definition 2.2 ([9]). A block cipher $\mathcal{C} = \{\tau_k \mid k \in \mathcal{K}\}$ over $\mathbb{F}_2$ is called *translation based (tb)* if:

- it is the composition of a finite number of rounds, such that any round $\tau_{k,h}$ can be written as $\gamma_h \lambda_h \sigma_{k_h}$, where
  - γ_h is a round-dependent bricklayer transformation (but it does not depend on k) and $0\gamma_h = 0$,
  - λ_h is a round-dependent linear map (but it does not depend on k),
  - k_h is in V and depends on both k and the round (k_h is called a "round key"),
- for at least one round, called a "proper" round, we have (at the same time) that λ_h is proper and that the map $\Phi_h : \mathcal{K} \to V$ given by $k \mapsto k_h$ is surjective.

The assumption $0\gamma_h = 0$ is not restrictive. Indeed, we can always include $0\gamma_h$ in the round key addition of the previous round (see [9, Remark 3.3]).

Let $m \geq 1$, and let $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ be a vectorial Boolean function. We denote by $\hat{f}_u(x) = f(x+u) + f(x)$ the derivative of f in the direction of $u \in (\mathbb{F}_2)^m$.

Definition 2.3. Let f be a vectorial Boolean function, for any $a, b \in (\mathbb{F}_2)^m$ we define
$$\delta_f(a,b) = |\{x \in (\mathbb{F}_2)^m \mid \hat{f}_a(x) = b\}|.$$
Then, f is said differentially δ-uniform if
$$\delta = \max_{\substack{a,b \in (\mathbb{F}_2)^m, \\ a \neq 0}} \delta_f(a,b).$$

Vectorial Boolean functions used as S-boxes in block ciphers must have low uniformity to prevent differential cryptanalysis (see [7]). By [9, Fact 3], a vectorial Boolean function differentially δ-uniform satisfies
$$|\mathrm{Im}(\hat{f}_u)| \geq \frac{2^m}{\delta}.$$

Definition 2.4. Let $1 \leq r < m$ and $f(0) = 0$, we say that f is *strongly r-anti-invariant* if, for any two subspaces U and W of $(\mathbb{F}_2)^m$ such that $f(U) = W$, then either $\dim(U) = \dim(W) < m - r$ or $U = W = (\mathbb{F}_2)^m$.

2.2. **Partition-based trapdoors.** We recall that a permutation group G acting on V is called primitive if it has no nontrivial G-invariant partition of V. That is, there no exists a partition $\mathcal{A}$ of V different from the trivial partitions $\{\{v\} \mid v \in V\}$, $\{V\}$, such that $Ag \in \mathcal{A}$ for all $A \in \mathcal{A}$ and $g \in G$. On the other hand, if a nontrivial G-invariant partition exists, the group is called imprimitive.

As said before a property of Γ_∞ considered undesirable is the imprimitivity. Paterson [17] showed that if this group is imprimitive, then it is possible to embed a trapdoor in the cipher.

Another trapdoor, based on the idea of the imprimitive action, is the Partition-based trapdoor, introduced in a recent work [5]. In this work the authors give some conditions to construct a translation-based cipher which associates a partition of the plaintext space to another partition of the ciphertext space.

We report some of the definitions and results presented in [5].

Definition 2.5. Let ρ be a permutation of V and $\mathcal{A}, \mathcal{B}$ be two partitions of V. Let $\mathcal{A}\rho$ denote the set $\{A\rho \mid A \in \mathcal{A}\}$. We say that ρ maps $\mathcal{A}$ to $\mathcal{B}$ if $\mathcal{A}\rho = \mathcal{B}$. Moreover, let G be a permutation group we say that G maps $\mathcal{A}$ to $\mathcal{B}$ if for all $\rho \in G$, ρ maps $\mathcal{A}$ to $\mathcal{B}$.

Remark 1. Note that a permutation group G is imprimitive if there exists a non-trivial partition $\mathcal{A}$ such that for all $\rho \in G$ $\mathcal{A}\rho = \mathcal{A}$.

Definition 2.6. A partition $\mathcal{A}$ of V is said linear if there exists U a subspace of V such that
$$\mathcal{A} = \{U + v \mid v \in V\}.$$
We denote with $\mathcal{L}(U)$ such a partition.

The following result, introduced by Harpes in [14], characterizes the possible partitions $\mathcal{A}$ and $\mathcal{B}$ such that $T(V)$ maps $\mathcal{A}$ to $\mathcal{B}$.

Proposition 1. *Let $\mathcal{A}$ and $\mathcal{B}$ be two partitions of $V = (\mathbb{F}_2)^d$. Then the permutation group $T(V)$ maps $\mathcal{A}$ to $\mathcal{B}$ if and only if $\mathcal{A} = \mathcal{B}$ and $\mathcal{A}$ is a linear partition.*

Focusing on the mixing-layer we have.

Proposition 2 ([5])**.** *Let λ be a linear permutation of V, i.e. $\lambda \in \mathrm{GL}(V)$, and let U be a subspace of V. Then $\mathcal{L}(U)\lambda = \mathcal{L}(U\lambda)$.*

We report now the main theorem of [5]. In [5] the following result is reported for a SPN cipher with the same S-box and mixing-layer for each round, but can be extended to any translation based cipher with independent round keys.

Theorem 2.7. *Let $\mathcal{C}$ be a translation based cipher on V. Suppose that there exist $\mathcal{A}$ and $\mathcal{B}$ non-trivial partitions such that for all ℓ-tuples of round-keys $k = (k_1, ..., k_\ell)$ the encryption function τ_k maps $\mathcal{A}$ to $\mathcal{B}$. Define $\mathcal{A}_1 = \mathcal{A}$ and for $1 \leq i \leq \ell$ $\mathcal{A}_{i+1} = \mathcal{A}_i\tau_i$, where $\tau_i = \gamma_i\lambda_i$ is the i-th round function without the round key translation. Then*

- *$\mathcal{A}_{\ell+1} = \mathcal{B}$*
- *for any $1 \leq i \leq \ell + 1$ $\mathcal{A}_i$ is a linear partition.*

3. **Avoiding the partition-based trapdoor.** In this section we will give sufficient conditions on the components of a tb cipher to guarantee that such a trapdoor cannot be implemented.

Lemma 3.1. *Let γ be a permutation on V such that $0\gamma = 0$ and suppose that γ maps $\mathcal{L}(U)$ to $\mathcal{L}(W)$ then for all $u \in U$*
$$\mathrm{Im}(\hat{\gamma}_u) \subseteq W.$$

Proof. The fact that γ maps $\mathcal{L}(U)$ to $\mathcal{L}(W)$ and $0\gamma = 0$ imply that $U\gamma = W$. Moreover for all $v \in V$ we have that $v\gamma \in (U + v)\gamma$. Then $(U + v)\gamma = W + v\gamma$. This implies that
$$(u + v)\gamma + v\gamma \in W$$
for all $v \in V$ and $u \in U$. $\square$

¿From Lemma 3.1 we have the following.

Proposition 3. *Let γ be a brick-layer transformation, i.e. $\gamma = (\gamma_1, ..., \gamma_b)$ with $\gamma_i \in \mathrm{Sym}(V_i)$ for all i. Suppose that for all i γ_i is*

1. *differentially 2^r-uniform, with $r < m$,*
2. *strongly $(r - 1)$-anti-invariant*

Let $\mathcal{L}(U)$ and $\mathcal{L}(W)$ be non-trivial linear partitions of V, then γ maps $\mathcal{L}(U)$ to $\mathcal{L}(W)$ if and only if U and W are walls, in particular $U = W$.

Proof. Suppose that γ maps $\mathcal{L}(U)$ to $\mathcal{L}(W)$ and that U is not a wall. Then let $I = \{i \mid \pi_i(U) \neq 0\}$. There exists $i \in I$ such that $U \cap V_i \neq V_i$ because U is not a wall. Moreover $U \cap V_i \neq \{0\}$. Indeed, let $u \in U$, with $u_i \neq 0$. For all $v \in V$ such that $v_j = 0$ for all $j \neq i$ we have that

$$(u + v_i)\gamma + v_i\gamma \in W$$

from Lemma 3.1. Moreover $u\gamma \in W$. It follows that $u\gamma + (u + v_i)\gamma + v_i\gamma \in W$. The vector $u\gamma + (u + v_i)\gamma + v_i\gamma$ has all nonzero components but for the one in V_i, which is $u_i\gamma_i + (u_i + v_i)\gamma_i + v_i\gamma_i \in W \cap V_i$. As γ is a brick layer transformation, if $U \cap V_i = \{0\}$, then $W \cap V_i = \{0\}$. So, if the vector $u_i\gamma_i + (u_i + v_i)\gamma_i + v_i\gamma_i$ is zero for all $v_i \in V_i$, then $\mathrm{Im}(\hat{\gamma}_i) = \{u_i\gamma_i\}$, of size 1. This contradicts the first condition on the γ_i's.

Thus $U \cap V_i$ is a proper subspace of V_i and $(U \cap V_i)\gamma = W \cap V_i$ is also a proper subspace of V_i. Since $\mathrm{Im}(\hat{\gamma}_u) \subseteq W$ for all $u \in U$, we have $\mathrm{Im}(\hat{\gamma}_{i_u}) \subseteq W \cap V_i$ for all $u \in U \cap V_i$. Thus, $|\mathrm{Im}(\hat{\gamma}_{i_u})|$ for any non-zero u is greater or equal to 2^{m-r} and, being γ_i a permutation, the set $\mathrm{Im}(\hat{\gamma}_{i_u})$ does not contain the zero vector, which implies $\dim(W \cap V_i) \geq m - r + 1$. This contradicts the second condition on the γ_i's. Then, U is a wall and, since γ is a parallel map, we have $U = W$.

Vice versa, consider any wall U, as γ is a parallel map, it is easy to check that γ maps $\{U + v \mid v \in V\}$ in itself. $\qquad\square$

The following definition was introduced in [2].

Definition 3.2. Let $\lambda \in \mathrm{GL}(V)$. λ is said to be a strongly proper mixing-layer if it does not map a proper wall in an other wall.

We define a strongly-proper round of a tb cipher as a proper round, where the mixing-layer is also strongly proper.

Theorem 3.3. *Let a round $h < \ell$ be a strongly proper round and suppose that the brick-layer transformations of round h and round $h + 1$, γ_h and γ_{h+1}, satisfy Condition 1) and 2) of Proposition 3. Then, there do not exist $\mathcal{A}$ and $\mathcal{B}$ non-trivial partitions such that for all ℓ-tuples of round keys the encryption functions map $\mathcal{A}$ to $\mathcal{B}$.*
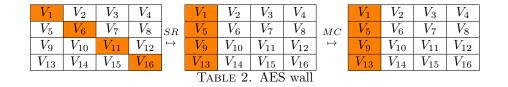
Proof. Suppose that the partition-based trapdoor is applicable for all ℓ-tuples of round keys. From Theorem 2.7 we have that there exist two linear partitions $\mathcal{L}(U)$ and $\mathcal{L}(W)$ such that $\gamma_h\lambda_h$ maps $\mathcal{L}(U)$ to $\mathcal{L}(W)$. Thus γ_h maps $\mathcal{L}(U)$ to $\mathcal{L}(W(\lambda_h)^{-1})$. From Proposition 3 we have that U is a wall and the same for $W(\lambda_h)^{-1}$. Now being λ_h strongly-proper we have that W is not a wall. Then from Theorem 2.7 we have that γ_{h+1} maps $\mathcal{L}(W)$ to another linear partition, but it is not possible since W is not a wall and this contradicts Proposition 3. $\qquad\square$

The result of Theorem 3.3 can be generalized, using a weaker condition on the mixing-layers composing the round functions. Consider, for example, the mixing-layer of AES. This is not strongly-proper, as there exists a wall which is sent in another wall. Indeed, the state of AES can be represented as a 4×4 matrix of bytes (Table 1). That is, $V = V_1 \oplus ... \oplus V_{16}$, where V_i is isomorphic to $(\mathbb{F}_2)^8$.

The mixing-layer of AES is composed by two linear functions ShiftRow (SR) and MixColumn (MC). The ShiftRows transformation acts in a way such that a wall is sent in an other wall, and in particular $V_1 \oplus V_6 \oplus V_{11} \oplus V_{16}$ is sent in $V_1 \oplus V_5 \oplus V_9 \oplus V_{13}$. Now, as MixColumn combines the blocks of a same column of the state, we have that $V_1 \oplus V_5 \oplus V_9 \oplus V_{13}$ (which is the first column of the state) is sent in itself

V_1	V_2	V_3	V_4
V_5	V_6	V_7	V_8
V_9	V_{10}	V_{11}	V_{12}
V_{13}	V_{14}	V_{15}	V_{16}

TABLE 1. AES state

V_1	V_2	V_3	V_4		V_1	V_2	V_3	V_4		V_1	V_2	V_3	V_4
V_5	V_6	V_7	V_8	SR	V_5	V_6	V_7	V_8	MC	V_5	V_6	V_7	V_8
V_9	V_{10}	V_{11}	V_{12}	$\mapsto$	V_9	V_{10}	V_{11}	V_{12}	$\mapsto$	V_9	V_{10}	V_{11}	V_{12}
V_{13}	V_{14}	V_{15}	V_{16}		V_{13}	V_{14}	V_{15}	V_{16}		V_{13}	V_{14}	V_{15}	V_{16}

TABLE 2. AES wall

(Table 2). However, the previous attack cannot be applied to AES as the mixing layer satisfies the following property.

Definition 3.4. Let $\lambda_1, ..., \lambda_\ell$ be the mixing-layers used in a tb cipher with ℓ rounds. We say that the ordered family $\Lambda = (\lambda_1, ..., \lambda_\ell)$ is strongly proper if for all possible non-trivial wall W there exists $j < \ell$ such that $W\lambda_1 \cdot ... \cdot \lambda_j$ is not a wall.

Corollary 1. *Let $\mathcal{C}$ be a tb cipher with $\Lambda = (\lambda_1, ..., \lambda_\ell)$ strongly proper and for each round h the parallel map γ_h satisfies the conditions of Proposition 3. Then the partition-based trapdoor is not applicable.*

Proof. Suppose that the partition-based trapdoor is applicable. From Theorem 2.7 we have that each round functions (without the translation with respect to the round key) $\tau_h = \gamma_h \lambda_h$ maps a linear partition $\mathcal{L}(U_h)$ into $\mathcal{L}(U_{h+1})$. From Lemma 3.1 the space U_h is a wall for all $1 \le h \le \ell$. Then, being γ_h a parallel map and $0\gamma_h = 0$ we have

$$U_{h+1} = U_h\lambda_h = U_1\lambda_1 \cdot ... \cdot \lambda_h$$

for all h.

Since Λ is strongly proper, there exists $j < \ell$ such that $U_1\lambda_1 \cdot ... \cdot \lambda_j$ is not a wall, which contradicts the fact that U_h is a wall for all $1 \le h \le \ell$.   □

It may seem that the previous corollary requires strong conditions on the mixing layers and on the S-boxes. We show that the requirement on the mixing layers is necessary.

Proposition 4. *Let $\mathcal{C}$ be a tb cipher, with $\Lambda = (\lambda_1, ..., \lambda_\ell)$ not strongly proper. Then the partition trapdoor is applicable.*

Proof. Because $\Lambda = (\lambda_1, ..., \lambda_\ell)$ is not strongly propers, then there exists W a proper wall such that $W\lambda_1 \cdot ... \cdot \lambda_j$ is a wall for all $1 \le j \le \ell$. Now being the γ_h a parallel map we have that for all wall W' and $v \in V$

$$(W' + v)\gamma_h = W' + v\gamma_h,$$

which concludes the proof.   □

4. **Security proof for a cipher with independent round-keys.** In this section we will discuss the fact that studying the group Γ_∞ to understand the security of a block cipher $\mathcal{C}$ could not be enough.

We report an example of block cipher $\mathcal{C}$ whose components satisfy the cryptographic properties given in [2] sufficient to thwart the trapdoor introduced by Paterson [17], but that is weak with respect to the partition-based trapdoor.

Let $V = (\mathbb{F}_2)^{mb}$, $V_i = (\mathbb{F}_2)^m$, with $m, b \geq 1$ and $\gamma_i \in \mathrm{Sym}(V_i)$ be the inverse permutation for all $0 \leq i \leq b - 1$, i,e. $\gamma_i : x \mapsto x^{2^m - 2}$ (using the representation as univariate polynomial). Consider the following mixing-layer

$$
\lambda = \begin{bmatrix}
0 & I_{m \times m} & 0 & ... & 0 \\
0 & 0 & I_{m \times m} & ... & 0 \\
\vdots & & & & \vdots \\
0 & & ... & & I_{m \times m} \\
I_{m \times m} & & ... & & 0
\end{bmatrix}
$$

where $I_{m \times m}$ is the identity matrix of size $m \times m$. It is easy to check that λ is a proper mixing-layer but not strongly proper.

Consider now the linear partitions $\mathcal{L}(V_1), ..., \mathcal{L}(V_b)$, and suppose to have ℓ rounds where we use λ and γ in each one. From [2, Theorem 3.1] $\Gamma_\infty(\mathcal{C})$ is primitive, but each encryption function maps $\mathcal{L}(V_i)$ to $\mathcal{L}(V_{\sigma^\ell(i)})$, where σ is the permutation of $\{1, ..., b\}$ such that $\sigma : i \mapsto i + 1$ for all $i < b$ and $\sigma : b \mapsto 1$.

Obviously, the mixing-layer λ is not interesting from a cryptographic point of view. We use this only as an example to show that if $\Gamma_\infty(\mathcal{C})$ is primitive this does not guarantee security on $\mathcal{C}$. Moreover, if we use a number ℓ of rounds such that $\mathcal{L}(V_i) = \mathcal{L}(V_{\sigma^\ell(i)})$ for some i, then $\Gamma_\infty(\mathcal{C})$ is primitive and the group $\Gamma(\mathcal{C})$ is imprimitive.

As we pointed out in Section 2, it would be interesting to study the group $\Gamma(\mathcal{C})$. However, this group depends, strongly, on the key-schedule used to create the round-keys. For this reason, usually, we study the properties of the group $\Gamma_\infty(\mathcal{C})$ (see for instance [4, 13, 19, 20, 21]). But, as we showed above, we could have that even if the group $\Gamma_\infty(\mathcal{C})$ is considered secure, the group $\Gamma(\mathcal{C})$ may be not secure with respect to the trapdoors considered here. Then, we think that it is better to consider, and study, the group of a cipher $\mathcal{C}$ obtained using independent round-keys, that is,

$$
\Gamma_{ind}(\mathcal{C}) = \langle \tau_K \mid K \in V^\ell \rangle,
$$

where, letting $K = (k_1, \ldots, k_\ell)$, τ_K is the encryption function obtained using $k_h \in V$ as round-key at round h. Clearly, $\Gamma_{ind}(\mathcal{C})$ is such that

$$
\Gamma(\mathcal{C}) \subseteq \Gamma_{ind}(\mathcal{C}) \subseteq \Gamma_\infty(\mathcal{C}).
$$

We can summarize the results obtained in this work for $\Gamma_{ind}(\mathcal{C})$ in the following:

Theorem 4.1. *Let $\mathcal{C}$ be a tb cipher. Suppose that one of the following properties is satisfied:*

1. *there exists a round h which is a strongly proper round and the brick-layer transformations γ_h, γ_{h+1} satisfy Condition 1) and 2) of Proposition 3,*

or

2. *the family $\Lambda = (\lambda_1, ..., \lambda_\ell)$ is strongly proper and for each round h the parallel map γ_h satisfies Condition 1) and 2) of Proposition 3.*

Then the partition-based trapdoor is not applicable. Moreover, $\Gamma_{ind}(\mathcal{C})$ is primitive.

Proof. ¿From Theorem 3.3 (or Corollary 1) we have that there do not exist two partitions $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{A}\tau_k = \mathcal{B}$ for all $\tau_k \in \Gamma_{ind}(\mathcal{C})$. Moreover, the group $\Gamma_{ind}(\mathcal{C})$ is imprimitive if and only if there exists a partition such that $\mathcal{A}\tau_k = \mathcal{A}$ for

all $\tau_k \in \Gamma_{ind}(\mathcal{C})$ (see Remark 1), which is a particular case where the partition-based trapdoor is applicable.   □

5. **Conclusions and final remarks.** An interesting open problem proposed by Paterson [17] was to investigate if it is possible to construct a block cipher such that the group Γ_∞ is primitive, but the resulting cipher is weak with respect to the imprimitive trapdoor. As we pointed out in Section 4, it may happen that the cipher is vulnerable even if the group generated by the round functions results to be primitive. For this reason, here, we studied the group Γ_{ind} generated by the cipher with independent round keys. We think that studying algebraic properties for this group could be more appropriate to investigate security properties of a cipher. In particular, we gave sufficient conditions on the components of a cipher $\mathcal{C}$, so that the partition trapdoor given in [5] cannot be applied to the encryption functions generating $\Gamma_{ind}(\mathcal{C})$. As a consequence, we obtained also the primitivity for the group $\Gamma_{ind}(\mathcal{C})$.

Note that this type of trapdoor can be easily avoided. Indeed, as noted in [2], for an invertible vectorial Boolean function to be strongly 1-anti-invariant is equivalent to have no linear components (i.e. the nonlinearity is greater than 0). Such a property is usually requested by the S-boxes of a cipher to avoid linear cryptanalysis [16]. Moreover, to achieve a good *diffusion* we need that the mixing layer satisfies the condition given in Definition 3.4. Therefore, from Theorem 4.1, sufficient conditions to thwart the partition trapdoor are:

- S-boxes with differential 4-uniformity and nonlinearity different from 0.
- strongly proper mixing layers (or that satisfy the condition in Definition 3.4).

For well-know ciphers like AES, PRESENT and SERPENT we have that these two characteristics are satisfied.

In the work [6], the authors give a method to construct the S-boxes of a block-cipher in order to let be possible the partition trapdoor (see Section 3 in [6]). Using their method they construct a cipher, with S-boxes defined over $\mathbb{F}_2^{10}$, which is weak with respect to their trapdoor. It is possible to check that such a cipher cannot be attacked using the classical linear and differential cryptanalysis. However, as the same author stated, the structure of their linear and differential tables is likely to betray the existence of a backdoor and can be used to find it. For this reason they create an other attack perturbing the S-boxes of the cipher, in order to strengthen it. These new S-boxes "behave" similarly to their secret counterparts, that means the output of a perturbed S-box is with high probability equals to the output of the corresponding non-perturbed S-box.

The mixing layer used in this block cipher is similar to the AES mixing layer, in particular we can check that the condition in Definition 3.4 is satisfied. The perturbed S-boxes are at most differentially 40-uniform (and thus 2^5-uniform). So, if we would analize if the properties of Theorem 4.1 are satisfied we need to check if it is strongly 4-anti-invariant. This computation could be possible, but quite long. So we could verify the resistance of the block cipher to the partition trapdoor in an other way.

In Theorem 4.1 we use the differential uniformity of the S-boxes to say that $\text{Im}(\hat{\gamma}_u)$ is greaten than $2^n/2^r$. So, we could generalize the first condition in Proposition 3 as follow.

(1') $\text{Im}(\hat{\gamma}_u) > 2^{n-r}$ for all nonzero $u \in \mathbb{F}_2^n$.

Note that this condition is pretty similar to the *weak differential uniformity* introduced in [10] and also studied in [3].

Using this fact, we have, for the case of the perturbed S-boxes of the cipher, that $\mathrm{Im}(\hat{\gamma}_u) > 2^6$. So, we can check if the the S-boxes are strongly 3-anti-invariant. This check is much easier, indeed we need to check if vector subspaces of dimension at least 7 are mapped onto an other vector subspace. Using the software MAGMA it is possible, now, to check that all the S-boxes of the cipher are strongly 3-anti-invariant. Which implies that the cipher is secure with respect to the trapdoor. Then, using only the analysis reported in this work, we cannot detect the backdoor introduced in [6]. However the high differential uniformity of the S-boxes could lead to some suspect, suggesting the existence of a backdoor.

So it is a very interesting open problem to understand which cryptographic properties can be useful to avoid also the attack with perturbed S-boxes.

Another requested property for a cipher is that the group generated by the encryption functions is not "small" (see for instance [15]). Usually, this property is investigated for the group of the round functions ([4, 13, 19]). With an ad hoc proof, in [21] and [20] Wernsdorf proved respectively that $\Gamma_\infty(AES) = \mathrm{Alt}(V)$ and $\Gamma_\infty(SERPENT) = \mathrm{Alt}(V)$, where $\mathrm{Alt}(V)$ is the alternating group. In [2, 10] are given conditions for tb ciphers so that $\Gamma_\infty(\mathcal{C})$ is the symmetric (alternating) group.

In the case of ciphers like AES and PRESENT, where the same S-box and mixing layer are used in each round, we have that $\Gamma_{ind}(\mathcal{C})$ is normal in $\Gamma_\infty(\mathcal{C})$ (see for instance [4, Lemma 3.4]), so if $\Gamma_\infty(\mathcal{C})$ is the symmetric (alternating) group we have $\Gamma_{ind}(\mathcal{C}) = \Gamma_\infty(\mathcal{C})$. However, this is no more the case of ciphers like, e.g., SERPENT, where the used S-box depends on the round. Then, it may happen that the group of the round functions generates the symmetric (alternating) group, while the group generated by the encryption functions is not.

Moreover, the only condition that $\Gamma_\infty(\mathcal{C})$ is the symmetric (alternating) group does not guarantee that the cipher is secure with respect the trapdoor studied in this work. Indeed, if we consider the example of the cipher given in Section 4, adding at the last round a strongly-proper mixing layer we will obtain that $\Gamma_\infty(\mathcal{C})$ is the alternating group. This is implied by Theorem 4.7 in [2]. However, as in Section 4, such a cipher can be broken using the partition based trapdoor. Another example of a weak cipher having $\Gamma_\infty(\mathcal{C}) = \mathrm{Sym}(V)$ is given in [18].

Another interesting future research could be investigating assumptions on the components of a cipher $\mathcal{C}$ which can guarantee that the group $\Gamma_{ind}(\mathcal{C})$ is the symmetric (alternating) group.

References

[1] R. Anderson, E. Biham and L. Knudsen, SERPENT: A new block cipher proposal, *in: Fast Software Encryption, LNCS, Springer, Berlin*, **1372** (1998), 222–238.

[2] R. Aragona, M. Calderini, A. Tortora and M. Tota, Primitivity of PRESENT and other lightweight ciphers, *Journal of Algebra and Its Applications*, **17** (2018), 1850115, 16pp.

[3] R. Aragona, M. Calderini, D. Maccauro and M. Sala, On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion, *Appl. Algebra Engrg. Comm. Comput.*, **27** (2016), 359–372.

[4] R. Aragona, A. Caranti and M. Sala, The group generated by the round functions of a GOST-like cipher, *Ann. Mat. Pura Appl.*, **196** (2016), 1–17.

[5] A. Bannier, N. Bodin and E. Filiol, Partition-Based Trapdoor Ciphers, preprint, https://eprint.iacr.org/2016/493.pdf.

[6] A. Bannier and E. Filiol, *Partition-based Trapdoor Ciphers*, Partition-Based Trapdoor Ciphers. InTech, 2017.

[7] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, **4** (1991), 3–72.

[8] A. Andrey Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, in: *Proc. of CHES 2007, LNCS, Springer*, **4727** (2007), 450–466.

[9] A. Caranti, F. Dalla Volta and M. Sala, On some block ciphers and imprimitive groups, *Appl. Algebra Engrg. Comm. Comput.*, **20** (2009), 229–350.

[10] A. Caranti, F. Dalla Volta and M. Sala, An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher, *Designs, Codes and Cryptography*, **52** (2009), 293–301.

[11] D. Coppersmith and E. Grossman, Generators for certain alternating groups with applications to cryptography, *SIAM Journal on Applied Mathematics*, **29** (1975), 624–627.

[12] J. Daemen and V. Rijmen, *The Design of Rijndael: AES-the Advanced Encryption Standard*, Springer Science & Business Media, 2002.

[13] S. Even and O. Goldreich, DES-Like functions can generate the alternating group, *IEEE Trans. Inform. Theory*, **29** (1983), 863–865.

[14] C. Harpes and J. L. Massey, Partitioning cryptanalysis, in: *Fast Software Encryption, LNCS, Springer, Berlin*, **1267** (1997), 13–27.

[15] B. S. Kaliski, R. L. Rivest and A. T. Sherman, Is the Data Encryption Standard a group? (Results of cycling experiments on DES), *Journal of Cryptology*, **1** (1988), 3–36.

[16] M. Matsui, Linear Cryptanalysis Method for DES Cipher, *Advances in Cryptology – EUROCRYPT '93, LNCS, Springer, Berlin*, **765** (1994), 386–397.

[17] K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in: *Fast Software Encryption, LNCS, Springer, Berlin*, **1636** (1999), 201–214.

[18] M. Sean, K. Paterson and P. Wild. A weak cipher that generates the symmetric group, *Journal of Cryptology*, **7** (1994), 61–65.

[19] R. Sparr and R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, *Discrete Appl. Math*, **156** (2008), 3139–3149.

[20] R. Wernsdorf, *The round functions of SERPENT generate the alternating group*, 2000; available at http://csrc.nist.gov/archive/aes/round2/comments/20000512-rwernsdorf.pdf.

[21] R. Wernsdorf, The round functions of RIJNDAEL generate the alternating group, *Fast Software Encryption, LNCS, Springer, Berlin*, **2365** (2002), 143–148.

E-mail address: marco.calderini@uib.no

E-mail address: marco.calderini@uib.no