COLLUDING TAGS ATTACK ON THE ECC-BASED GROUPING PROOFS FOR RFIDS

Mohammad Reza Sohizadeh Abyaneh*

Abstract. Recently, a new privacy-preserving elliptic curve based grouping proof protocol with *colluding tag prevention*(CTP) has been proposed. The CTP protocol is claimed to be resistant against colluding tags attacks in which the involved tags can exchange some messages via another reader before the protocol starts without revealing their private keys.

In this paper, we show that the CTP protocol is vulnerable to some colluding tag attacking scenario. In addition, we propose a new elliptic curve based grouping protocol which can fix the problem. Our proposal is based on a formally proved privacy preserving authentication protocol and has the advantage of being resistant against colluding tags attacks with the same amount of computation.

Keywords: RFID, Grouping Proofs, Elliptic Curve, Privacy.

1 Introduction

In 2004, Juels [1] proposed a new security notion called *Yoking Proofs*. The proposed scheme enables the generation of a proof which shows that a pair of RFID tags are scanned simultaneously by a reader. Yoking proofs were later generalized to *grouping proofs* which indicates that multiple tags participate in the generation of a proof [2, 8].

*Department of Informatics, University of Bergen

By adopting grouping proofs, the manufacturer can prove to its customers that the referred products are sold at the same time. For example in a pharmacy store, some drugs must be sold according to the recipe. For inpatients, the medical staffs can guarantee the authentication and integrity of a group of medical items like inpatient bracelets and the containers of drugs [6]. For car industry, a grouping proof ensures that all components of a car are assembled in the same factory [1, 9].

Recently, Batina *et al* have proposed a new privacy-preserving elliptic curve based grouping-proof protocol with *colluding tag prevention* (denoted by CTP protocol)[13]. The protocol is claimed to be resistant against all active attacks applied on the previous grouping proof protocols and also fulfil the privacy against a narrow-strong adversary. The notion of the CTP protocol is mainly derived from the latest version of their elliptic curve based authentication protocols called EC-RAC III [20].

Remark1. With elliptic curve cryptography emerging as a serious alternative, the desired level of security can be attained with significantly smaller key sizes. This makes ECC very attractive for devices with limited computational capabilities. On the feasibility of implementing ECC on RFID tags, one may argue that it is too heavy to be deployed on low-cost tags such as EPCglobal Class-1 Generation-2 standard tags. Nevertheless, there have been many proposals so far such as [13–17].

Our Contribution. In this paper, we present a colluding attack against the CTP protocol. We show that two colluding tags are able to complete a run of the CTP protocol successfully and generate a valid grouping proof with the presence of only one of the tags. Then, we propose a new grouping proof protocol based on elliptic curves which fixes the problem.

Outline. The remainder of this paper is organized as follows. In Section 2, we describe the CTP protocol and its security claims, then Section 3 presents a colluding attack scenario against the CTP protocol. In order to fix the problem, a new grouping protocol is proposed in Section 4 with its security analysis. In Section 5, we compare our proposal with the CTP protocol from security and computation perspectives and finally Section 6 concludes the paper.

2 THE CTP PROTOCOL

In this section, we describe the CTP protocol. But first we explain the notations and assumptions used hereafter.

- P: Elliptic curve base point.
- T_A, T_B: Tag A and tag B respectively.
- R: Reader.
- V: Verifier.
- $y, Y = yP$: Verifier's private and public keys respectively.
- s_a, s_b: Tag A and tag B's private keys respectively.
- $x(T)$: x-coordinate of point T on the elliptic curve.
- P_{AB} : grouping proof of tag A and tag B.

2.1 Assumptions

It should be noted that the CTP protocol is executed under following assumptions:

- There are three entities involved in the protocol: some *tags*, a *reader* and a *verifier*.
- The task of the reader is to coordinate the execution of the protocol, collect the grouping proof and forward it to the verifier. The reader is not necessarily trusted by the tags or the verifier.
- The verifier is trusted and the public-key Y of the verifier is a publicly known system parameter. Only the verifier knows the corresponding private-key y.
- Knowledge of y is a necessary requirement to check the correctness of a grouping proof. The result of a verification claim is failure, or it reveals the identities of the involved tags.
- It is hard to solve the Discrete Logarithm (DL) problem, i.e. given P and aP in Elliptic Curve with a randomly chosen in $\mathbb{Z}_q = [0, q-1]$, it is hard to compute a.
- It is hard to solve the Decisional Diffie-Hellman (DDH) problem, i.e. given P, aP, bP with a and b randomly chosen in $\mathbb{Z}_q$ and given $cP = abP$ with probability $\frac{1}{2}$ and $cP = dP$ with probability $\frac{1}{2}$ with d randomly chosen in $\mathbb{Z}_q$, it is hard to decide whether abP equals cP .

2.2 Description

Without loss of generality, we explain the two-party version of the CTP protocol. This protocol can be easily extended to more than two tags as described in [13].

The two-party version of the CTP protocol is shown in Fig.1. The reader initiates the interrogation by sending the messages "start left" to one of the tags (T_A). Then, T_A generates a random number r_a and computes its corresponding Elliptic curve point ($T_{a,1} = r_a P$) and sends it back to the reader. The reader then initiates a simultaneous interrogation with another tag (T_B) by transmitting the "start right" message following by a random challenge generated by the reader r_s and $T_{a,1}$ received from T_A. T_B computes $T_{b,1} = r_b P$ and $T_{b,2} = (r_b + x(r_s T_{a,1}) s_b)Y$. Then, both of the generated messages are transmitted to the reader. The reader passes $T_{b,2}$ to T_A and the protocol concludes by transmission of $T_{a,2} = (r_a + x(T_{b,2}) s_a)Y$ from T_A to the reader.

The grouping proof, collected by the reader, consists of the tuple in (1).

$$P_{AB} = \{T_{a,1}, T_{a,2}, r_s, T_{b,1}, T_{b,2}\} \qquad (1)$$

This tuple is sent to the verifier to verify the grouping proof constructed by T_A and T_B. The verifier checks whether the following equations hold.

$$\begin{aligned} S_a = s_a P &= (y^{-1} T_{a,2} - T_{a,1}) x(T_{b,2})^{-1} \qquad (2) \\ S_b = s_b P &= (y^{-1} T_{b,2} - T_{b,1}) x(r_s T_{a,1})^{-1} \qquad (3) \end{aligned}$$

where S_a and S_b are the public keys of T_A and T_B respectively and are registered in the database of the verifier. If so, the grouping proof is accepted.

2.3 Security Claims

Due to its construction, the CTP grouping-proof protocol is claimed to inherit the security properties of the EC-RAC III authentication protocol [20]. The EC-RAC III latter is designed to provide secure entity authentication against an active adversary, and was informally shown to be equivalent to the Schnorr protocol [18].

The security claims on the CTP protocol can be divided into to two different security issues, *Privacy* and *Forgery prevention* of the grouping proof.

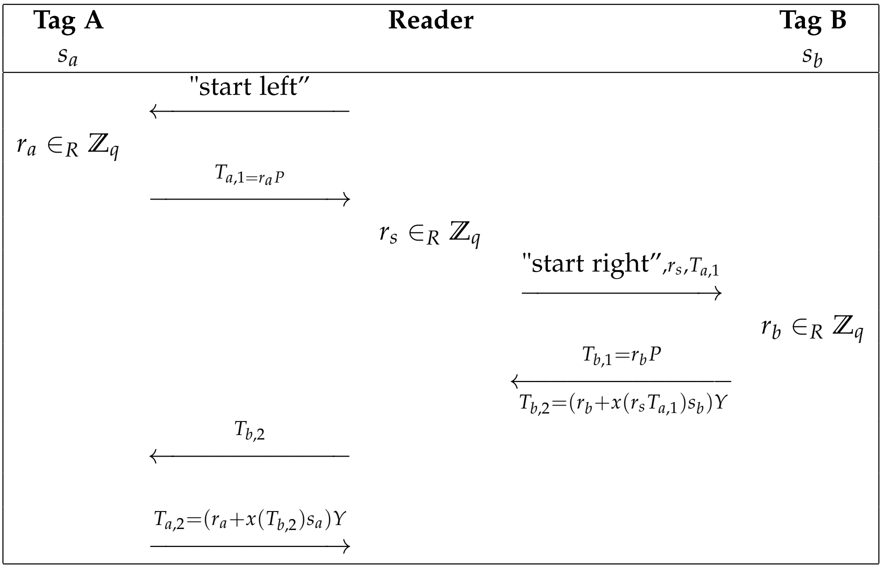

Fig. 1: *Two-party version of the CTP protocol*

2.3.1 Privacy

In [22], Vaudenay has presented a classification of privacy in RFID systems. Vaudenay's model defines eight classes of adversarial capabilities. These capabilities are in two orthogonal parts:

1. Four different types of tag corruptions: *strong, forward, destructive* and *weak*.
2. Two modes of observations: *wide* and *narrow*.

Referring to this classification, the CTP protocol is claimed to be *narrow-strong* private, although no formal proof for this is given in the original paper. This claim has been recently invalidated [23]. However, verification of this claim has not been addressed in this paper.

2.3.2 Forgery Prevention

Being a grouping proof protocol, the CTP must prevent the generation of a valid grouping proof without the involved tags actually participating in the protocol. This implies that the protocol must resist against the following potential attack scenarios:

- *Compromised tag:* One tag is compromised, the reader is non-compromised.
- *Man-in-the-middle attack*: The reader is compromised (the tags are honest).
- *Colluding reader and tag:* The reader and one of the tags are compromised.
- *Colluding tags:* The reader is non-compromised, both tags are compromised. The tags can exchange some messages in advance (e.g., via another reader), but do not know each other's private key.
- *Replay attack performed by an outsider:* An eavesdropper scans two non-compromised tags simultaneously and replays the copied message-flow to impersonate the two tags.

The CTP protocol is claimed to be resistant against the impersonation of a tag in all of the above attack scenarios. Namely,an adversary needs to either know the private-key of that particular tag or be able to solve the Decisional Diffie-Hellman (DDH) problem to impersonate it in this protocol. This claim has been addressed through this paper and an attack, which negates this claim, will be described in the next section.

3 Our colluding tags attack

In this section, we elaborate an attacking scenario against the CTP protocol. In our attack, we take the colluding tags scenario which implies that the reader is trusted, but both tags are compromised, and tags can exchange some messages in advance (e.g. via another reader), but they do not know each other's private key.

Our attacking scenario is divided into two phases: *conspiracy* phase and *deceit* phase. In the conspiracy phase, the two tags secretly negotiate via a rogue reader (Reader*). In this negotiation, as Figure 2 shows, one of the tags (e.g. tag B) sends $H = s_b Y$ to tag A. H is the point multiplication operation of tag B's private key (s_b) and verifier's public key (Y) on the Elliptic Curve group. It should be mentioned that message H does not reveal any information on s_b due to discrete logarithm (DL) problem.

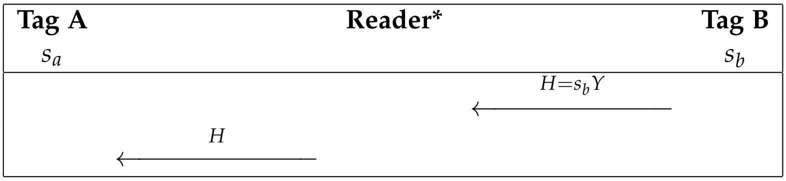

Fig. 2: *Phase I: Conspiracy Phase*

Having H known, tag A is able to impersonate tag B in the CTP protocol.

Figure 3 shows the detail of a successful completion of the CTP protocol run with inclusion of only one of the tags. The only message of the CTP protocol, which includes tag B's private key, is $T_{b,2}$ which can be easily forged by (5) if a tag accesses H.

$$T_{b,2} = (r_b + x(r_s T_{a,1})s_b)Y \tag{4}$$

$$T_{b,2} = (r_bY + x(r_s T_{a,1})s_bY) = (r_bY + x(r_s T_{a,1})H) \tag{5}$$

As it can be seen, knowing $H = s_bY$ is adequate to impersonate tag B in the CTP protocol without revealing any information about its private key s_b.

4 Proposed Protocol

In Section 3, we showed that the CTP protocol is vulnerable to some colluding tags attacks. In this section, we propose a new scheme based on elliptic curve notion with the same security level from privacy perspective but resistant against colluding attacks from forgery prevention perspective.

4.1 Description

Our proposal is based on an authentication protocol proposed by Bringer *et al.* called "Randomized Schnorr"(Figure 4 [19]. This protocol has been formally proved to be narrow-strong private.

The two-party version of our proposed protocol is shown in Figure 5. The reader initiates the interrogation by sending the messages "start left" to one of the tags (T_A). Then, T_A generates two random numbers α_a and β_a and computes their point multiplication on P and Y Elliptic curve

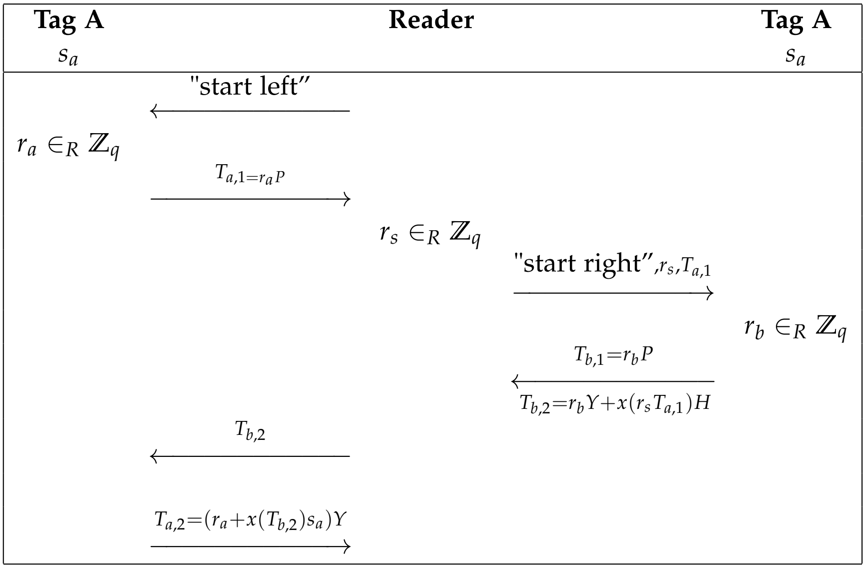

Fig. 3: *Phase II: Deceit Phase*

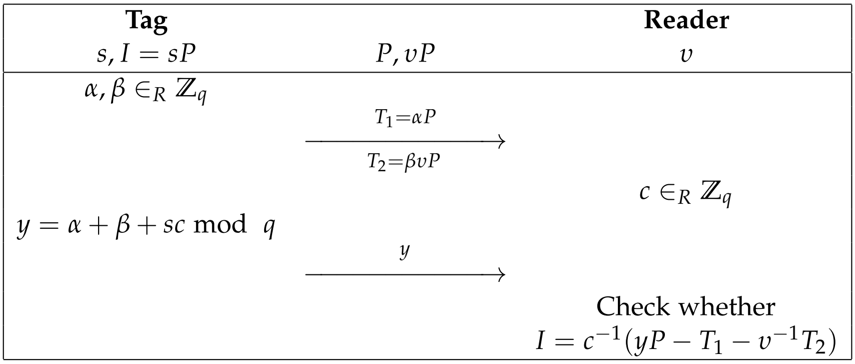
Tag
Reader
$s, I = sP$
P, vP
v
$\alpha, \beta \in_R \mathbb{Z}_q$
$T_1=\alpha P$
$T_2=\beta v P$
$c \in_R \mathbb{Z}_q$
$y = \alpha + \beta + sc \bmod q$
y
Check whether
$I = c^{-1}(yP - T_1 - v^{-1}T_2)$

Fig. 4: *Randomized Schnorr protocol*

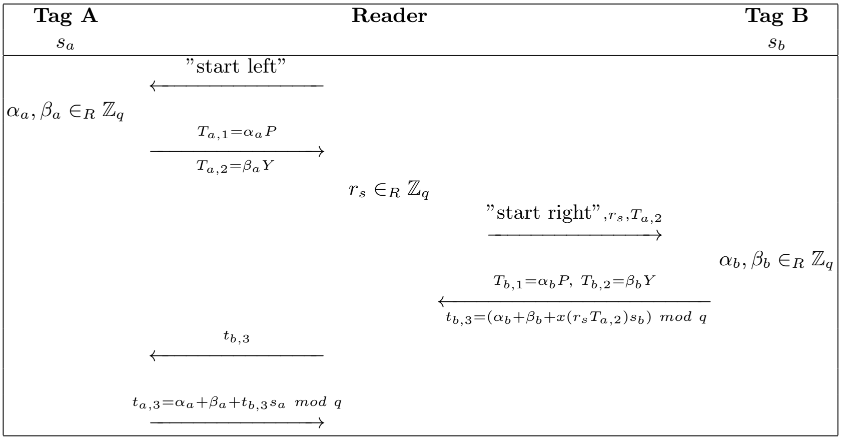
Tag A
s_a
Reader
Tag B
s_b
"start left"
$\alpha_a, \beta_a \in_R \mathbb{Z}_q$
$T_{a,1}=\alpha_a P$
$T_{a,2}=\beta_a Y$
$r_s \in_R \mathbb{Z}_q$
"start right", r_s, $T_{a,2}$
$\alpha_b, \beta_b \in_R \mathbb{Z}_q$
$T_{b,1}=\alpha_b P,\ T_{b,2}=\beta_b Y$
$t_{b,3}=(\alpha_b+\beta_b+x(r_s T_{a,2})s_b)\ mod\ q$
$t_{b,3}$
$t_{a,3}=\alpha_a+\beta_a+t_{b,3}s_a\ mod\ q$

Fig. 5: *Proposed grouping protocol*

points respectively ($T_{a,1} = \alpha_a P$, $T_{a,2} = \beta_a Y$) and sends it to the reader in return. The reader then initiates a simultaneous interrogation with another tag (T_B) by transmitting the "start right" message following by a random challenge generated by the reader r_s and $T_{a,2}$ received from T_A. T_B computes $T_{b,1} = \alpha_b P$ and $T_{b,2}\beta_b Y$, the same as T_A did. In addition, it also generates a scalar number $t_{b,3} = (\alpha_b + \beta_b + x(r_s T_{a,2})s_b)$ mod q. Then, all of the three generated messages are transmitted to the reader. The reader passes $t_{b,3}$ to T_A and the protocol concludes by transmission of scalar $t_{a,3} = \alpha_a + \beta_a + t_{b,3}s_a$ from T_A to the reader. The grouping proof, collected by the reader, consists of the tuple (6).

$$P_{AB} = \{T_{a,1}, T_{a,2}, T_{a,3}, r_s, T_{b,1}, T_{b,2}, T_{b,3}\} \tag{6}$$

To verify the grouping proof constructed by T_A and T_B, the verifier checks whether the Equations (7) and (8) hold.

$$S_a = s_a P \;=\; x^{-1}(T_{b,3})(t_{a,3}P - T_{a,1} - y^{-1}T_{a,2}) \tag{7}$$

$$S_b = s_b P \;=\; x^{-1}(r_s T_{a,2})(t_{b,3}P - T_{b,1} - y^{-1}T_{b,2}) \tag{8}$$

4.2 Security Analysis

In this section, we analyze the security of our protocol in the same security framework used for the CTP protocol.

4.2.1 Privacy

Theorem 1. *Assume the hardness of the DDH problem, then Randomized Schnorr is narrow-strong private.*

Proof: [19]

Theorem 2. *Assume that the Randomized Schnorr is narrow-strong private, our proposed protocol is privacy-preserving against narrow-strong adversary.*

Proof: As explained, to prove the privacy, it is necessary to prove that we can simulate the tags outputs. In the following, we construct a simulation and we show that an adversary who is able to distinguish between this simulation and the outputs of genuine tags in the proposed protocol will be able to do the same for the Randomized Schnorr protocol.

The outputs of the tags in the proposed are as following:

T_A: $T_{a,1} = \alpha_a P, T_{a,2} = \beta_a Y, t_{a,3} = \alpha_a + \beta_a + t_{b,3} s_a$

T_B: $T_{b,1} = \alpha_b P,\ T_{b,2} = \beta_b Y, t_{b,3} = (\alpha_b + \beta_b + x(r_s T_{a,2}) s_b)$

The outputs of each tag is easily mapped on the outputs of a generic tag in the Randomized Schnorr protocol, namely $T_1 = \alpha P, T_2 = \beta v P, y = \alpha + \beta + sc$. In other words, the proposed protocol is simply two runs of the Randomized Schnorr protocol regarding the tags outputs. This simply proves the privacy attribute inheritance of the proposed protocol from the Randomized Schnorr protocol.

4.2.2 Forgery Prevention

Theorem 3. *Assume the Schnorr scheme is secure against active impersonation attacks, then Randomized Schnorr is secure against active impersonation attacks.*

Proof: [19]

Theorem 4. *Assume the randomized Schnorr scheme is secure against active impersonation attacks, then our proposed protocol is secure against active impersonation attacks.*

Proof: It is obvious that interrogation of T_A in the proposed protocol is a complete run of the Randomized Schnorr protocol and inherits the security attribute of the Randomized Schnorr protocol stated in

Theorem 3. The interrogation of T_B, however, is slightly different from a normal run of the Randomized Schnorr protocol. So, in our proof we focus on the right part of the protocol runs between the reader and T_B.

In order to proof the theorem, we devise a *proof by contradiction* approach. Assume there exists an active adversary $\mathcal{A}$ against the proposed protocol. Given a system of tags $\mathcal{T}$ and a reader executing the Randomized Schnorr protocol, we transform the tags' normal outputs to simulate tags' outputs in the proposed protocol. So doing, we convert $\mathcal{A}$ into an adversary against the Randomized Schnorr protocol.

First, when $\mathcal{A}$ interrogates T_B, she sends r_s and $T_{a,2}$ to the tag. We intercept this message. Then, tag outputs $T_1 = T_{b,1}$ and $T_2 = T_{a,2}$. We intercept these two messages and send back $c = x(r_s T_{a,2})$ to the tag. The tag responses $y = (\alpha_b + \beta_b + c s_b)$. We forward this message to the adversary as $t_{b,3} = y$. Clearly, from $\mathcal{A}$'s point of view, T_A is using the proposed protocol.

Now, $\mathcal{A}$ tries to impersonate T_B by interacting with the reader. First, we pick a random number r'_s and one random Elliptic curve point $T'_{a,2}$ and send them to $\mathcal{A}$. As $\mathcal{A}$ is able to impersonate T_B against the proposed protocol then she is able to compute a couple tuple $T'_{b,1} = \alpha'_b P, T'_{b,2} = \beta'_b Y$ and $t'_{b,3} = (\alpha'_b + \beta'_b + x(r'_s T'_{a,2}) s'_b)$ on receiving the challenges such that there exists an S_b verifying $S'_b = s'_b P = x^{-1}(r_s T_{a,2})(t_{b,3} P - T_{b,1} - y^{-1} T_{b,2})$.

For this reason, we are able to uniquely compute T_1 and T_2, to receive a challenge c and to compute y such that there exists an I with $I = c^{-1}(yP - T_1 - v^{-1} T_2)$. In this way, we showed that by using $\mathcal{A}$, we are able to impersonate T_B against the Randomized Schnorr protocol which negates our assumption.

One can demonstrate that to impersonate a tag in either of the attack scenarios stated in Section 2.3, the adversary needs to know the private-key of that particular tag (or be able to solve the DDH problem).

5 Comparison

Table 2 summarizes the comparison between the CTP and our proposed protocol in terms of security and computation.

Security wise, our proposed protocol has accomplished to yield the same but formally proved privacy level and higher security from forgery prevention perspective, due to formally proved resistance against the colluding tags attack.

	Security		Computation	
	Privacy	**Forgery Prevention**	**# of EC point multiplications for the verifier**	**# of EC point multiplications for each tag**
CTP	narrow-strong (Not formally proved)	Not Secure	4	2
Proposed Protocol	narrow-strong (Formally proved)	Secure	6	2

Table 1. Comparison of the CTP protocol and the proposed protocol

From computational perspective, the forth column of the table compares the number of EC point multiplications(ECPM) required for the verifier to verify the grouping proofs. This number is four for the CTP protocol as it can be seen in (2) and (3). On the other hand, (7) and (8) show that this number is six in our protocol. This implies that our proposed protocol imposes more computational overhead to the verifier than the CTP protocol. But this is trivial due to higher computational capabilities of the verifier in comparison to the tags. On the tag side, the fifth column shows the number of ECPM needed for a tag during one run of the protocol. This number is the same for both protocols as they both impose two EC point multiplications on each tag, e.g. tag A needs to do two EC point multiplications for both protocols to calculate $T_{a,1}$ and $T_{a,2}$.

6 CONCLUSIONS

In this paper, we have presented a successful colluding tag attack on the CTP grouping proof protocol. This implies that the CTP protocol is not able to prevent colluding tags attacks as claimed. The main weakness in the protocol that we have exploited is that the necessary information required to impersonate a tag in the protocol is not structurally restricted to be its private key. It was shown that the point multiplication of a tag's private key and the verifier's public key, which does not reveal any information about the tag's private key, can be exploited by colluding tags to generate a grouping proof with presence of only one of the tags. In order to fix this problem, we proposed a new grouping protocol based on elliptic curves which prevents the colluding attacks and proved its security properties. In summary, compared to the CTP protocol, our proposal has the following properties:

- Formally provable narrow-strong privacy.
- Formally provable prevention against forged proof generation.
- The same amount of computational overhead on tag sides.

REFERENCES

[1] Ari Juels, Yoking-Proofs for RFID Tags, In the Proceedings of First International Workshop on Pervasive Computing and Communication Security, IEEE Press, pp.138–143, (2004).

[2] Junichiro Saitoh and Kouichi Sakurai, Grouping Proofs for RFID Tags, In the Proceedings of AINA International Conference, IEEE Computer Society, pp. 621–624, (2005).

[3] Selwyn Piramuthu, On Existence Proofs for Multiple RFID Tags, In the Proceedings of ACS/IEEE International Conference on Pervasive Services, IEEE Computer Society, pp. 317–320, (2006).

[4] Chih-Chung Lin, Yuan-Cheng Lai, J. D. Tygar, Chuan-Kai Yang and Chi-Lung Chiang, Coexistence Proof using Chain of Timestamps for Multiple RFID Tags, In the Proceedings of APWeb/WAIM International Workshop, Springer-Verlag LNCS 5189, pp. 634–643, (2007).

[5] Mike Burmester, Breno de Medeiros, and Rossana Motta, Provably Secure Grouping-Proofs for RFID Tags, In the Proceedings of CARDIS International Conference, Springer-Verlag LNCS 5189, pp. 176–190, (2008).

[6] C.-Y. K. Hsieh-Hong Huang, A RFID Grouping Proof Protocol for Medication Safety of Inpatient, Journal of Medical Systems, (2008).

[7] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags, in Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SECPerU (2007).

[8] L. Bolotnyy and G. Robins, Generalized Yoking-Proofs for a Group of RFID Tags, in Proc. International Conference on Mobile and Ubiquitous Systems (Mobiquitous), (2006).

[9] Hung-Min Sun, Wei-Chih Ting, Shih-Ying Chang, Offlined Simultaneous Grouping Proof for RFID Tags,The Second International

Workshop on Multimedia, Information Privacy and Intelligent Computing Systems(MPIS),(2009).

[10] Y. Lien, X. Leng, K. Mayes, and J. Chiu, Reading Order Independent Grouping Proof for RFID Tags, IEEE International Conference on Intelligence and Security Informatics,ISI 2008. , (2008).

[11] Hung-Yu Chien, Tree-Based RFID Yoking Proof, International Conference on Networks Security, Wireless Communications and Trusted Computing, (2009).

[12] Dang Nguyen Duc, Jangseong Kim, Kwangjo Kim, Scalable Grouping-proof Protocol for RFID Tags, SCIS 2010 The Symposium on Cryptography and Information Security, (2010).

[13] Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelee, Ingrid Verbauwhede, *Short Paper: Privacy-preserving ECC-based grouping proofs for RFID*, In Information Security - 13th International Conference, ISC 2010 , Boca Raton, Florida, Oct. 25–28,(2010).

[14] Sandeep S. Kumar, Christof Paar. *Are standards compliant Elliptic Curve Cryptosystems feasible on RFID?*.Workshop on RFID Security , Graz, Austria, July (2006).

[15] Franz Furbass, Johannes Wolkerstorfer. *ECC Processor with Low Die Size for RFID Applications*, IEEE International Symposium on Circuits and Systems (ISCAS), (2007).

[16] Yong Ki Lee Sakiyama, K. Batina, L. Verbauwhede. *Elliptic-Curve-Based Security Processor for RFID*, IEEE Transactions on Computers, 1514 –1527 ,(2008).

[17] Daniel Hein, Johannes Wolkerstorfer, Norbert Felber,*ECC Is Ready for RFID - A Proof in Silicon*, SAC 2008, LNCS , pp. 401–413, (2008).

[18] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In G. Brassard, editor, Advances in Cryptology (CRYPTO ’89), Lecture Notes in Computer Science, LNCS 435, pages 239–252. Springer-Verlag, (1989).

[19] Julien Bringer, Herv´e Chabanne, and Thomas Icart. *Cryptanalysis of EC-RAC, a RFID identification protocol.* In CANS, volume 5339 of Lecture Notes in Computer Science, (2008).

[20] Yong Ki Lee, Lejla Batina, Dave Singelee, and Ingrid Verbauwhede. *Low-Cost Untraceable Authentication Protocols for RFID*. In Proceed-

ings of the 3rd ACM conference on Wireless network security (WiSec 2010),(2010).

[21] Fan, J., Hermans, J., Vercauteren, F.: *On the claimed privacy of EC-RAC III*. Cryptology ePrint Archive, Report 2010/132,, http://eprint.iacr.org, (2010).

[22] Serge Vaudenay. *On privacy models for RFID*. In ASIACRYPT, (2007).

[23] C. Lv and H. Li and J. Ma and B. Niu and H. Jiang. *Security Analysis of a Privacy-preserving ECC-based Grouping-proof Protocol*. Journal of Convergence Information Technology,(2011).