Amirkabir University of Technology
(Tehran Polytechnic)
Vol. 46, No. 1, Spring 2014, pp. 27- 36

Amirkabir International Journal of Science& Research
(Electrical & Electronics Engineering)
(AIJ-EEE)

Game-Based Cryptanalysis of a Lightweight CRC-Based Authentication Protocol for EPC Tags

K. Baghery[1], B. Abdolmaleki[1] and M. J. Emadi[2*]

1-MSc Student, Department of Electrical Engineering, Shahed University, Tehran, Iran
2- Assistant Professor, Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran

ABSTRACT

The term "Internet of Things (IoT)" expresses a huge network of smart and connected objects which can interact with other devices without our interposition. Radio frequency identification (RFID) is a great technology and an interesting candidate to provide communications for IoT networks, but numerous security and privacy issues need to be considered. In this paper, we analyze the security and the privacy of a new RFID authentication protocol proposed by *Shi et al.* in 2014. We prove that although *Shi et al.* have tried to present a secure and untraceable authentication protocol, their protocol still suffers from several security and privacy weaknesses which make it vulnerable to various security and privacy attacks. We present our privacy analysis based on a well-known formal privacy model which is presented by *Ouafi* and *Phan* in 2008. Moreover, to stop such attacks on the protocol and increase the performance of *Shi et al.*'s scheme, we present some modifications and propound an improved version of the protocol. Finally, the security and the privacy of the proposed protocol were analyzed against various attacks.

KEYWORDS

Internet of Things, RFID authentication protocols, Security and Privacy, Ouafi-Phan Privacy Model, EPC C1 G2 Standard.

* Corresponding Author, Email : mj.emadi@aut.ac.ir

1- INTRODUCTION

RFID is a user friendly technology which is useful in various applications in which identification, tracking or authentication are necessary [1]. An RFID system could be the best choice for asset management, tracking and positioning with precision, supply chain management, healthcare control, automobile ignition keys, production control and pass control [2]-[6]. Besides, RFID systems are interesting and popular candidates to be implemented in the Internet of Things world which is introduced as a next generation of internet [7]. In the IoT paradigm, we will face a huge global network which makes connections between large number of smart and IP-based devices in our environments Anytime, Anyplace, with Anything and Anyone [8]. Communications between IoT elements may be set up via various sensing devices like Global

Positioning System (GPS), intelligent sensors, RFID systems or any other smart device that can exchange data between two objects [9]. Mainly, an RFID system has three main parts including *back-end server*, *readers* and large number of *tags*. The architecture of an RFID system is illustrated in Fig. 1. The tags are transponders equipped with a microstrip antenna and communicate with the readers using radio waves. Due to the nature of *wireless* communications, communication channels between the tags and the readers are not secure and can be accessed by an outsider agent. Based on the power supply, available memory, operational frequency, processing power and range of work, the tags are classified to various categories which are employed in the desired applications. The second parts of each RFID system are the readers which act as interrogators and exchange messages between the tag and back-end server. This fact is graphically shown in Fig. 1. According to the desired applications, a reader can operate as a fixed or mobile reader. In the case that the reader is mobile, wireless communication channels between the readers and the back-end server might be insecure. The third and the essential part of each RFID system is the back-end server which acts as a core of an RFID system and performs various processing such as identification and authentication of the tags and in some cases the readers. The back-end server has all secret information about the tags and utilizes them in authentication procedures [10]. Usually, the back-end server is a central computer which has a powerful Central Processor Unit (CPU) and is connected to readers over a wireless or wired channel.

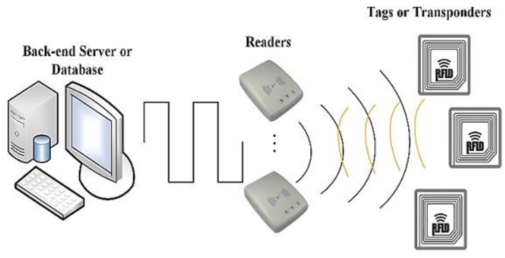

Fig. 1. An RFID system architecture

In the IoT paradigm, RFID tags can be attached to different objects and make a wireless connection with the RFID readers which act as an IoT gateway. A simple communication scenario of an RFID system in the IoT world is shown in Fig. 2. According to the figure, it can be seen that RFID readers can play the role of IoT gateway. In [8], *Gross et al.* proposed a prototype for the IoT paradigm based on the RFID passive tags in which the tags are conforming to the Electronic Product Code Class 1 Generation 2 (EPC C1 G2) standard. The IoT presents new services in which some of them bring security and privacy concerns for end-users. Thus, implementing a secure and confidential authentication protocol between the elements of the IoT significantly decreases these concerns.

The EPC C1 G2 standard is the most famous and popular standard which has been proposed for RFID passive tags by EPC global organization [11]. In the EPC C1 G2 standard, the tags are passive which supply their required powers using electromagnetic fields of readers. The tags, which are conforming to the EPC C1 G2 standard, have some processing limitations and are not allowed to use heavy-duty encryptions as well as hash functions [12]. This type of tag uses Pseudo Random Number Generator (PRNG), Cyclic Redundancy Code (CRC) and bitwise operators to protect the stored information and transmitted data.

In recent years, due to the widespread usage of EPC C1 G2 tags in a variety of modern applications, the security and the privacy of consumers have found great importance [13]-[14]. In this context, various lightweight RFID authentication protocols have been proposed which are under EPC C1 G2 standard and have tried to ensure the security and privacy of RFID end-users [15]-[18]. An EPC-based lightweight RFID authentication protocol is a particular security scheme that is designed to provide secure and confidential authentication between the back-end server and the tags which are conforming to the EPC C1 G2 standard. Although all the mentioned protocols are designed to protect RFID users, in the literature, several drawbacks of some EPC-based RFID authentication protocols are pointed out [12], [15], [19] and [20].

Recently, *Shi et al.* [21] have proposed a novel CRC-based lightweight RFID authentication protocol for EPC compliant tags. In the proposed protocol, they have used CRC and PRNG functions to protect and update the exchanged messages. In their protocol, communication channel between the tag and the reader is insecure and can be eavesdropped by an adversary. On the other hand, the reader and the back-end server communicate over a secure channel. They have analyzed the security and the privacy of their protocol against lots of existing threats including eavesdropping, traceability attacks, Denial of Service (DoS) attack, replay attack and spoofing attacks. They have claimed that the protocol can protect RFID users against various security and privacy concerns [21]. However, in this paper, we cryptanalyze *Shi et al.*'s protocol and we prove that due to some flaws in the structure of the exchanged messages and updating

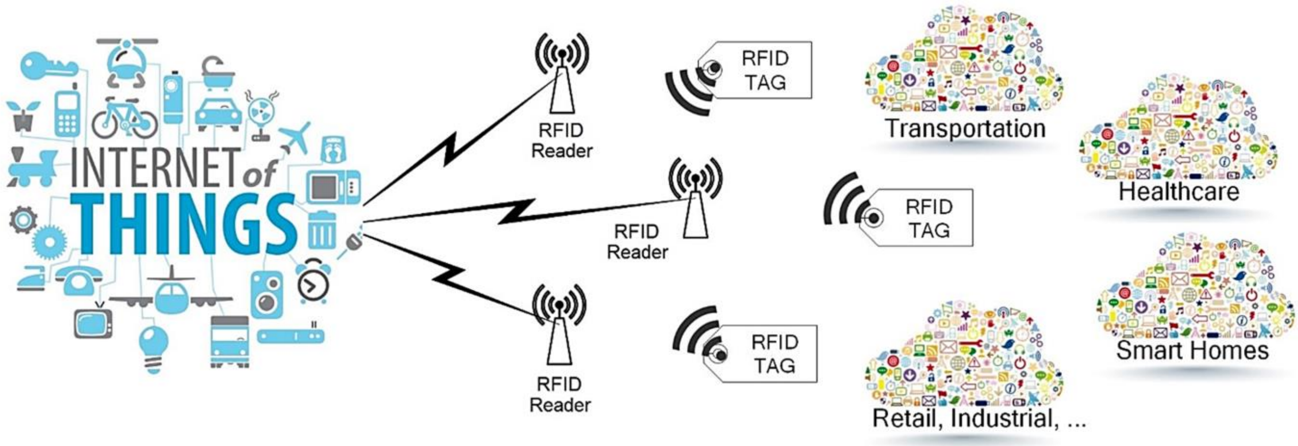

Fig. 2. A communication scenario of RFID tags and readers in the IoT world.

procedures, their protocol is unable to provide secure and untraceable authentication for RFID end-users and it suffers from several security and privacy attacks. More precisely, we show that *Shi et al.*'s protocol is vulnerable to *secret parameters reveal*, *tag impersonation attack* and also their protocol does not provide *users privacy*. Then, in order to prevent all the mentioned attacks and increase the performance of the *Shi et al.*'s protocol, we apply some modifications in the structure of the protocol and propose an *improved* version of it. Our security and privacy analysis show that new modifications overcome all the existing weaknesses in *Shi et al.*'s protocol.

The privacy of RFID authentication protocols can be studied by two different approaches: *ad-hoc* [22] and *formal* [23]-[24]. In the ad-hoc approach, the adversary defines some notation and performs an attack based on the defined notations. On the other hand, in the formal approaches, the abilities of the adversary are classified into different categories which can be used in different privacy analysis. In the different studies, several RFID formal privacy models are proposed [25]-[31]. In this paper, we use a formal RFID privacy model which proposed by *Ouafi* and *Phan* (referred as Ouafi-Phan) [28] in our privacy analysis. In *Ouafi-Phan* privacy model, the adversary's abilities are classified into four categories including $Execute\ Query$, $Corrupt\ Query$, $Sent\ Query$ and $Test\ Query$ which are discussed with more details in the following section.

The rest of this paper is organized as follows. In section 2, *Ouafi-Phan* formal privacy model is described. We review *Shi et al.*'s protocol in section 3. Security and privacy weaknesses of *Shi et al.*'s protocol are investigated in section 4. In section 5, an improved and robust version of *Shi et al.*'s protocol is proposed. In this section, the security and the privacy of the proposed protocol are also analyzed and compared with some similar protocols. The paper is concluded in Section 6.

2-OUAFI AND PHAN PRIVACY MODEL

In 2008, *Ouafi* and *Phan* [28] presented a privacy model to evaluate RFID authentication protocols. In this paper, we use this model for our privacy analysis. So, in this section, we summarize *Ouafi-Phan* privacy model which will be used in the rest of paper.

In this model, the adversary $\mathcal{A}$ can eavesdrop all channels between tags and readers and also it can attack them actively or passively. Similarly, the adversary $\mathcal{A}$ has been allowed to run the following queries:

- ***Execute query*** $(\boldsymbol{R}, \boldsymbol{T}, \boldsymbol{i})$***:*** Passive attacks take place in this query. In other words, the adversary can eavesdrop all transmitted messages between the tag T and the reader R in ith session. As a result, the adversary obtains all exchanged data between the tag T and the reader R.
- ***Send query*** $(\boldsymbol{U}, \boldsymbol{V}, \boldsymbol{m}, \boldsymbol{i})$***:*** This query models the active attacks in RFID systems. In this query, the adversary $\mathcal{A}$ has permission to impersonate a reader U in the ith session, and forwards a message m to a tag V. In addition, the adversary $\mathcal{A}$ has permission to alert or block the exchanged message m between the tag and the reader. Note that U and V are the members of readers and tags sets, respectively.
- ***Corrupt query*** $(\boldsymbol{T}, \boldsymbol{K'})$***:*** In this query, the adversary $\mathcal{A}$ has permission to access secret keys of the tag. In fact, the adversary $\mathcal{A}$ has physical access to the tag's database. In addition, the adversary $\mathcal{A}$ can set secret key to K'.
- ***Test query*** $(\boldsymbol{T_0}, \boldsymbol{T_1}, \boldsymbol{i})$***:*** When this query is executed in the particular session i**,** after completing ith session**,** a random number bit $b \in \{0,1\}$ is generated by challenger and delivered $T_b \in \{T_0, T_1\}$ to the adversary. Now, the adversary succeeds if he/she can guess the bit b correctly.

Untraceability privacy (UPriv): Untraceability privacy could be defined by the game *G* that is played between an adversary $\mathcal{A}$ and a set of the tag and the reader instances. In other words, an adversary $\mathcal{A}$ plays game G using collected instances of the reader and the tag. The game *G* can be played using mentioned queries as follows.

- ***Learning phase:*** The adversary $\mathcal{A}$ has permission to send each one of the queries such as *Execute*, *Send* and *Corrupt*, and interact with the reader R and T_0, T_1 that are chosen randomly.

- ***Challenge phase:*** The adversary $\mathcal{A}$ selects two tags T_0, T_1 and forwards a $Test\ query(T_0, T_1, i)$ to the challenger. After that, the challenger selects $b \epsilon \{0,1\}$ randomly and the adversary $\mathcal{A}$ determines a tag $\mathrm{T}_b \in \{\mathrm{T}_0, \mathrm{T}_1\}$ using *Execute* and *Send* queries.
- ***Guess phase:*** Eventually, the adversary $\mathcal{A}$ finishes the game G and outputs a bit $b' \epsilon \{0,1\}$ as guess of b. The success of adversary $\mathcal{A}$ in game G and consequently breaking the notion of *UPriv* is quantified via $\mathcal{A}$'s advantage in recognizing whether adversary $\mathcal{A}$ received T_0 or T_1, and denoted by $\mathrm{Adv}_{\mathcal{A}}^{UPriv}(k)$ where k is the security parameter.

$$\mathrm{Adv}_{\mathcal{A}}^{UPriv}(k) = |\mathrm{pr}(b' = b) - \mathrm{pr}(\text{random coin flip})|$$
$$= \left|\mathrm{pr}(b' = b) - \tfrac{1}{2}\right|.$$

Where $0 \leq \mathrm{Adv}_{\mathcal{A}}^{UPriv}(k) \leq \frac{1}{2}$. Note that, if $\mathrm{Adv}_{\mathcal{A}}^{UPriv}(k) \ll \varepsilon(k)$, the protocol is traceable with a negligible probability.

3-SHI ET AL.'S PROTOCOL

Recently, in [21], *Shi et al.* presented a five-step CRC-based authentication protocol for RFID systems. The notations used in the paper are presented in Table 1.

TABLE 1. THE NOTATIONS.

Notations	Description
ID	the unique identifier of a specific tag
Meta- ID	the pseudonym of the tag
K	the 32-bit secret key shared by readers and tags
$\boldsymbol{CRC}(.)$	the CRC function
$\boldsymbol{R_r}$	the pseudorandom number generated by a reader
$\boldsymbol{R_t}$	the pseudorandom number generated by a tag
$\boldsymbol{funh(x)}$	the function to get the left half-part of x
$\boldsymbol{funl(x)}$	the function to get the right half-part of x
$\boldsymbol{PRNG}(.)$	Pseudo random number generator
‖	Concatenation operation
$\mathbf{A \oplus B}$	Message A is XORed with message B
$\mathbf{A \stackrel{?}{=} B}$	Compare whether A is equal to B or not

The authentication procedure of Shi et al. protocol is summarized in Fig. 3 and discussed in details in a 5-step round in the following.

Step 1. [Reader → Tag]: The reader generates R_r as a random number and computes message $M_1 = funh(k) \oplus R_r$. It then sends a Query and message M_1 to the tag.

Step 2. [Tag → Reader]: After receiving the reader's response, the tag calculates $R_r = M_1 \oplus funh(k)$, then it generates a random number R_t and computes the following messages and sends them to the reader.

$$M_2 = CRC(funl(Meta\_ID) \oplus R_t) \parallel CRC(funh(Meta\_ID) \oplus R_r),$$

$$M_3 = CRC(funl(ID) \oplus R_t \oplus R_r),$$

$$M_4 = funl(k) \oplus R_t \oplus R_r.$$

Step 3. [Reader → Back-end server]: By using the message M_4, the reader abstracts the random number R_t, and then it forwards messages (M_2, M_3, R_r, R_t) to the back-end server.

Step 4. [Back-end server → Reader]: Upon receiving the sent messages from the reader, the back-end server performs the following operations.

a) Using new_ID and new_Meta_ID or old_ID and old_Meta_ID , It generates $\mathrm{M}_2' = \mathrm{CRC}(\mathrm{funl}(\mathrm{X\_Meta\_ID}) \oplus \mathrm{R_t}) \parallel \mathrm{CRC}(\mathrm{funh}(\mathrm{X\_Meta\_ID}) \oplus \mathrm{R_r})$ and $\mathrm{M}_3' = \mathrm{CRC}(\mathrm{funl}(\mathrm{X\_ID}) \oplus \mathrm{R_t} \oplus \mathrm{R_r})$ for $\mathrm{X} = \text{old and new}$. Afterwards, it verifies $\mathrm{M}_2' \stackrel{?}{=} \mathrm{M}_2$ and $\mathrm{M}_3' \stackrel{?}{=} \mathrm{M}_3$ and determines that $\mathrm{X} = \text{old or new}$. If $M_2' = M_2$ and $M_3' \stackrel{?}{=} M_3$ for $X = old$ or new, it authenticates the tag and responds to the reader through the following messages,

$$M_5 = CRC(funh(\mathrm{Meta\_ID}) \oplus \mathrm{funl(ID)} \oplus R_t),$$
$$M_6 = CRC(\mathrm{funl(Meta\_ID)} \oplus \mathrm{funh(ID)} \oplus R_r).$$

Otherwise, the back-end server quit the protocol.

b) Finally, the back-end server updates its secret values as follows;

If $X = new$

$$old\_ID \leftarrow new\_ID \leftarrow PRNG(funl(new\_ID) \oplus R_t) \parallel PRNG(funh(new\_ID) \oplus R_r)$$

$$old\_Meta\_ID \leftarrow new\_Meta\_ID \leftarrow PRNG(funl(new\_Meta\_ID) \oplus R_t) \parallel PRNG(funh(new\_Meta\_ID) \oplus R_r)$$

Else

do nothing

End

Step 5. [Reader → Tag]: The reader sends message M_5 and M_6 to the tag. Upon receiving messages from the reader, the tag calculates message M_5' and M_6', then in order to authenticate the back-end server, the tag verifies $M_5' \stackrel{?}{=} M_5$ and $M_6' \stackrel{?}{=} M_6$. Finally it updates its secret values as

$$new\_ID \leftarrow PRNG(funl(ID) \oplus R_t) \parallel PRNG(funh(ID) \oplus R_r)$$

$$new\_Meta\_ID \leftarrow PRNG(funl(Meta\_ID) \oplus R_t) \parallel PRNG(funh(Meta\_ID) \oplus R_r),$$

Otherwise, the tag aborts the protocol. Fig. 3 shows the detailed steps of *Shi et al.*'s protocol.

Database $(old\_ID, new\_ID, old\_Meta\_ID, new\_Meta\_ID,)$	**Reader** (K)		**Tag** $(K, Meta\_ID_i, ID_i)$
$For\ each\ Meta\_ID_X\ and\ ID_X$ in DB generates M_2' and M_3' to verifying the tag and determines X=old or new for $Meta\_ID$ and ID. If X=new the server acts as follows, $M_5 = CRC(funh(\text{Meta\_ID}) \oplus \text{funl(ID)} \oplus R_t)$ $M_6 = CRC(\text{funl(Meta\_ID)} \oplus \text{funh(ID)} \oplus R_r)$	$R_r = PRNG(.)$ $M_1 = funh(k) \oplus R_r$	$M_1 \parallel Query \rightarrow$ $\leftarrow (M_2, M_3, M_4)$	Generates random numbers N_T and N_3 $M_2 = CRC(funl(Meta_{ID}) \oplus R_t)$ $\parallel CRC(funh(Meta\_ID) \oplus R_r)$ $M_3 = CRC(funl(ID) \oplus R_t \oplus R_r)$ $M_4 = funl(k) \oplus R_t \oplus R_r$
Finally, the back-end server updates its secret values as follows; $If\ \ X = new$ $old\_ID \leftarrow new\_ID \leftarrow PRNG(funl(new\_ID) \oplus R_t)$ $\parallel PRNG(funh(new\_ID) \oplus R_r)$ $old\_Meta\_ID \leftarrow new\_Meta\_ID$ $\leftarrow PRNG(funl(new\_Meta\_ID)$ $\oplus R_t) \parallel PRNG(funh(new\_Meta\_ID) \oplus R_r)$ $Else$ Do nothing End	$R_t = M_4 \oplus funl(k) \oplus R_r$ $\leftarrow (M_2, M_3, R_r, R_t)$ $(M_5, M_6) \rightarrow$	$(M_5, M_6) \rightarrow$	Using its ID and $Meta_{ID}$ to calculates M_5' and M_6', comparing them with M_5 and M_6. If the tag verifies the server secessesfully , it updates as follows, $ID_{i+1} \leftarrow PRNG(funl(ID_i) \oplus R_t) \parallel PRNG(funh(ID_i) \oplus R_r)$. $Meta_{ID_{i+1}} \leftarrow PRNG(funl(Meta_{ID_i}) \oplus R_t) \parallel PRNG(funh(Meta\_ID_i) \oplus R_r)$

Fig. 3. Shi et al.'s protocol [21].

4-CRYPTANALYSIS OF SHI ET AL.'S PROTOCOL

In [21], *Shi et al.* analyzed their protocol and claimed that their protocol is secure against various security and privacy attacks. We show that *Shi et al.*'s protocol not only cannot protect the secret keys properly, but also it is vulnerable to tag impersonation and traceability attacks. In the rest of section, we first introduce a linear property of CRC operator that is used in our presented attacks and then present several practical attacks against *Shi et al.*'s protocol.

Linear Property: This property of CRC operator indicates that $CRC(A \oplus B) = CRC(A) \oplus CRC(A)$, where A and B represent the arbitrary values.

4-1- TAG IMPERSONATION ATTACK

In this subsection, it is shown that an adversary is able to impersonate the legitimate tag. This attack consists of two phases; learning phase and attach phase.

Learning phase: In the round i, the adversary acts as an eavesdropper. After one successful run, the adversary saves the exchanged data between the target tag and the reader including $M_{1,i} = funh(k) \oplus R_{r,i}$, $M_{2,i} = CRC(funl(Meta\_ID_i) \oplus R_{t,i}) \parallel CRC(funh(Meta\_ID_i) \oplus R_{r,i})$, $M_{3,i} = CRC(funl(ID_i) \oplus R_{t,i} \oplus R_{r,i})$, $M_{4,i} = funl(k) \oplus R_{t,i} \oplus R_{r,i}$. After that, using message $M_{2,i}$ the adversary defines $\rho = CRC(funl(Meta\_ID_i) \oplus R_{t,i})$ and $\varphi = CRC(funh(Meta\_ID_i) \oplus R_{r,i})$.

Attack phase: In this phase, the adversary acts as a legitimate tag and when the reader sends a $Query$ and message $M_{1,i+1} = funh(k) \oplus R_{r,i+1}$ to the target tag. The adversary obtains message $M_{1,i+1}$. Then, by using obtained messages in the *learning phase*, the following messages are computed and sent to the reader.

$$M_{2,att} = \rho \parallel \left(\varphi \oplus CRC\left(M_{1,i}\right) \oplus CRC\left(M_{1,i+1}\right)\right)$$

$$M_{3,att} = M_{3,i} \oplus CRC(M_{1,i}) \oplus CRC(M_{1,i+1})$$

$$M_{4,att} = M_{4,i} \oplus M_{1,i} \oplus M_{i+1}.$$

Based on the receiving messages from the adversary, the reader first calculates $R_{t,i}$ as $R_{t,i} = M_{4,att} \oplus \text{funl(k)} \oplus R_{r,i+1}$. Then, the reader sends messages $M_{2,att}$, $M_{3,att}$, $R_{t,i}$ and $R_{r,i+1}$ to the back-end server. To verify the adversary as a legitimate tag, by using old_ID and $\_Meta\_ID$, the back-end server performs two phases as follows;

phase1: First the adversary calculates message M_2' as $M_2' = CRC(funl(old\_Meta\_ID) \oplus R_{t,i}) \parallel CRC(funh(old\_Meta\_ID) \oplus R_{r,i+1})$ and verifies $M_2' \overset{?}{=} M_{2,att}$ as follows,

$$M_{2,att} = \rho \parallel \left(\varphi \oplus CRC\left(M_{1,i}\right) \oplus CRC\left(M_{1,i+1}\right)\right)$$
$$= \rho \parallel \left(\varphi \oplus CRC\left(funh(k) \oplus R_{r,i}\right) \oplus CRC\left(funh(k) \oplus R_{r,i+1}\right)\right).$$

By using the linear property, we have

$$M_{2,att} = \rho \parallel \left(\varphi \oplus CRC(funh(k)) \oplus CRC\left(R_{r,i}\right) \oplus CRC(funh(k)) \oplus CRC\left(R_{r,i+1}\right)\right)$$
$$= \rho \parallel \left(\varphi \oplus CRC\left(R_{r,i}\right) \oplus CRC\left(R_{r,i+1}\right)\right). \quad (1)$$

Then, by substituting $\varphi = CRC(funh(Meta\_ID_i) \oplus R_{r,i})$ in equation (1), we have

$$M_{2,att} = \rho \parallel \left(CRC(\text{funh}(\text{Meta\_ID}_i) \oplus R_{r,i}) \oplus CRC\left(R_{r,i}\right) \oplus CRC\left(R_{r,i+1}\right)\right). \quad (2)$$

Again, by considering the linear property, M_{2t} is rewritten as

$$= \rho \parallel \Big(CRC(\text{funh}(\text{Meta\_ID}_i)) \oplus CRC(R_{r,i}) \oplus CRC(R_{r,i}) \oplus CRC(R_{r,i+1})\Big)$$

$$= \rho \parallel \Big(CRC(funh(Meta\_ID_i)) \oplus CRC(R_{r,i+1})\Big)$$

$$= \rho \parallel \Big(CRC\big(funh(Meta_{ID_i}) \oplus R_{r,i+1}\big)\Big). \quad (3)$$

Finally, by substituting $\rho = CRC(funl(Meta\_ID_i) \oplus R_{t,i})$ in equation (3), we can write

$$= CRC(funl(Meta\_ID_i) \oplus R_{t,i}) \parallel \Big(CRC\big(funh(Meta\_ID_i) \oplus R_{r,i+1}\big)\Big)$$

$$= CRC\big(funl(old_{Meta_{ID}}) \oplus R_{t,i}\big) \parallel \Big(CRC\big(funh(old\_Meta\_ID) \oplus R_{r,i+1}\big)\Big)$$

$$= M_2' \quad (4)$$

Phase 2: The back-end sever computes message M_3' as $M_3' = CRC(funl(ID_i) \oplus R_{t,i} \oplus R_{r,i+1})$. Then, in order to authenticate the adversary as a legitimate tag, back-end sever verifies $M_3' \stackrel{?}{=} M_{3,att}$ as follows:

$$M_{3,att} = M_{3,i} \oplus CRC(M_{1,i}) \oplus CRC(M_{1,i+1}).$$

Substituting $M_{3,i} = CRC(funl(ID_i) \oplus R_t \oplus R_r)$, $M_{1,i} = funh(k) \oplus R_{r,i}$ and $M_{1,i+1} = funh(k) \oplus R_{r,i+1}$, equation (4) can be rewritten as follows,

$$M_{3,att} = CRC\big(\text{funl}(\text{ID}_i) \oplus R_{t,i} \oplus R_{r,i}\big) \oplus CRC\big(funh(k) \oplus R_{r,i}\big) \oplus CRC\big(funh(k) \oplus R_{r,i+1}\big). \quad (5)$$

By using the linear property of *CRC* operation, we have

$$= CRC\big(funl(ID_i) \oplus R_{t,i}\big) \oplus CRC\big(R_{r,i}\big) \oplus CRC\big(funh(k)\big) \oplus CRC(R_{r,i}) \oplus CRC(funh(k)) \oplus CRC(R_{r,i+1})$$

$$= CRC(funl(ID_i) \oplus R_t) \oplus CRC(R_{r,i+1})$$

$$= CRC(funl(ID_i) \oplus R_t \oplus R_{r,i+1})$$

$$= CRC(funl(old\_ID) \oplus R_t \oplus R_{r,i+1})$$

$$= M_3'. \quad (6)$$

Therefore, the back-end server authenticates the adversary as a legitimate tag.

4-2- SECRET PARAMETER REVEAL ATTACK

In this subsection, we present a practical secret parameter reveal attack against *Shi et al.*'s protocol. It is shown that an adversary is able to reveal secret parameter $Meta\_ID$ and ID. This attack is performed in two phases as follows.

Learning phase: In this phase, the adversary acts as an eavesdropper. After two successful runs of the protocol, the adversary saves the exchanged data between the target tag and the reader including $M_{2,i} = CRC(funl(Meta\_ID_i) \oplus R_{t,i}) \parallel CRC(funh(Meta\_ID_i) \oplus R_{r,i})$, $M_{2,i+1} = CRC(funl(Meta\_ID_{i+1}) \oplus R_{t,i+1}) \parallel CRC(funh(Meta\_ID_{i+1}) \oplus R_{r,i+1})$, $M_{5,i+1} = CRC(funh(Meta\_ID_{i+1}) \oplus funl(ID_{i+1}) \oplus R_{t,i+1})$ and $M_{6,i+1} = CRC(funl(Meta\_ID_{i+1}) \oplus funh(ID_{i+1}) \oplus R_{r,i+1})$.

Attack phase: The adversary defines two new parameters ρ and φ as $\rho = CRC(funl(Meta\_ID_i) \oplus R_{t,i})$, $\varphi = CRC(funh(Meta\_ID_i) \oplus R_{r,i})$ which are the first and the second parts of message $M_{2,\text{i}}$. Then adversary performs the following steps;

a) Since $(funl(Meta\_ID_i) \oplus R_{t,i})$ is a 16-bit string, thus $(funl(Meta\_ID_i) \oplus R_{t,i}) \epsilon\, U$ where $U = \{u_1, u_2, \dots, u_{2^{16}}\}$. Now, using the new parameter ρ,

For $1 \le j \le 2^{16}$
  Choose $u_j \in U$
   if $\rho = CRC(u_j)$ then
    return u_j as $(funl(Meta\_ID_i) \oplus R_{t,i})$
 End

b) Now, like step (a), since $(funh(Meta\_ID_i) \oplus R_{r,i})$ is a 16-bit string, thus $(funh(Meta\_ID_i) \oplus R_{r,i}) \epsilon\, V$ where $V = \{v_1, v_2, \dots, v_{2^{16}}\}$. Now, using the new parameter φ,

For $1 \le j \le 2^{16}$
  Choose $u_j \in U$
   if $\varphi = CRC(v_j)$ then
   return v_j as $(funh(Meta\_ID_i) \oplus R_{r,i})$
 End.

Now, by using $(funl(Meta\_ID_i) \oplus R_{t,i})$ and $funh(Meta\_ID_i) \oplus R_{r,i}$ in the steps (a) and (b), the adversary calculates the secret value $Meta\_ID_{i+1}$ as $Meta\_ID_{i+1} = PRGN(funl(Meta\_ID_i) \oplus R_{t,i}) \parallel PRNG(funh(Meta\_ID_i) \oplus R_{r,i})$, that will be used in the round $(i+1)$,

c) In order to compute the secret value K, the adversary uses the eavesdropped messages $M_{2,i+1}$, $M_{1,i+1}$ and $M_{4,i+1}$ in the learning phase and the linear property of CRC operator, adversary calculates $R_{t,i+1}$ and $R_{r,i+1}$ as follows.

- First, in order to calculate $R_{t,i+1}$, adversary uses the *first* part of the message $M_{2,i+1}$ and calculates the secret value $Meta\_ID_{i+1}$ in steps (a) and (b), so

$$R_{t,i+1} = CRC(funl(Meta\_ID_{i+1}) \oplus R_{t,i+1}) \oplus CRC(funl(Meta\_ID_{i+1})).$$

Using the linear property, $R_{t,i+1}$ is rewritten as

$$= CRC\Big(\text{funl}\big(\text{Meta}_{\text{ID}_{i+1}}\big)\Big) \oplus$$

$$CRC(R_{t,i+1}) \oplus CRC(\mathrm{funl}(\mathrm{Meta\_ID}_{i+1})).$$

- Now , in order to calculate $R_{r,i+1}$, adversary uses the *second* part of the message $M_{2,i+1}$ and evaluates secret value $Meta\_ID_{i+1}$ in steps (a) and (b), and performs the following process

$$R_{r,i+1} = CRC\big(funh\big(Meta_{ID}{}_{i+1}\big) \oplus R_{r,i+1}\big) \oplus CRC\left(funh\big(Meta_{ID}{}_{i+1}\big)\right).$$

By considering the linear property, we have

$$= CRC\left(funh\big(Meta_{ID}{}_{i+1}\big)\right) \oplus CRC(R_{r,i+1}) \oplus CRC(funh(Meta\_ID_{i+1})).$$

- Then, adversary computes $funl(K)$ as

$$funl(K) = M_{4,i+1} \oplus R_{t,i+1} \oplus R_{r,i+1}.$$

Substituting $M_{4,i+1} = funl(K) \oplus R_{t,i+1} \oplus R_{r,i+1})$ and using the linear property, we have

$$funl(K) = funl(K) \oplus R_{t,i+1} \oplus R_{r,i+1} \oplus R_{t,i+1} \oplus R_{r,i+1}.$$

- After that, the adversary computes $funh(K)$ as

$$funh(K) = M_{1,i+1} \oplus R_{r,i+1}$$

By substituting $M_{1,i+1} = \mathrm{funh}(K) \oplus R_{r,i+1})$ and using the linear property we have,

$$funh(K) = funh(K) \oplus R_{r,i+1} \oplus R_{r,i+1}.$$

Finally, adversary concatenates calculated $funh(K)$ and $funl(K)$ and computes the secret value K as $K = funh(K) \parallel funl(K)$.

4-3- TRACEABILITY ATTACK

The other important weakness of *Shi et al.*'s protocol is the privacy of this protocol. We show that the adversary can trace the location of a specific tag. To do so, we have the following procedures.

Learning phase: In round (i), the adversary $\mathcal{A}$ sends an $Execute\ query(R, T_0, i)$ and obtains $(M_{2,i}^{T_0}, M_{3,i}^{T_0})$. Then, the adversary sends a $Send\ query(R, T_0, i)$ and blocks the protocols. As results, the tag does not update the secret values. After that, by using the first and the second parts of the message $M_{2,i}^{T_0}$, the adversary defines new parameters $\rho^{T_0} = CRC(funl(Meta\_ID_i^{T_0}) \oplus R_{t,i}^{T_0})$ and $\varphi^{T_0} = CRC(funh(Meta\_ID_i^{T_0}) \oplus R_{r,i})$ and computes ζ as $\zeta = \rho^{T_0} \oplus \varphi^{T_0} \oplus M_{3,i}^{T_0} = CRC(funl(Meta\_ID_i^{T_0})) \oplus CRC(funh(Meta\_ID_i^{T_0})) \oplus CRC(funl(ID_i^{T_0})$.

Challenge phase: In round $(i+1)$, the adversary $\mathcal{A}$ selects two fresh tags T_0 and T_1 for test, and sends a $Test\ query(T_0, T_1, i+1)$. According to the randomly chosen bit $b \in \{0,1\}$, the adversary is given a tag $T_b \in \{T_0, T_1\}$. After that, the adversary $\mathcal{A}$ sends an $Execute\ query(R, T_b, i+1)$, and obtains $(M_{2,i+1}^{T_b}, M_{3,i+1}^{T_b})$. Then, by using the first and the second parts of message $M_{2,i+1}^{T_b}$ the adversary defines new parameters $\rho^{T_b} = CRC(funl(Meta\_ID_{i+1}^{T_b}) \oplus R_{t,i+1}^{T_b})$ and $\varphi^{T_b} = CRC(funh(Meta\_ID_{i+1}^{T_b}) \oplus R_{r,i+1})$.

Guess phase: The adversary $\mathcal{A}$ stops the game G, and outputs a bit $b' \in \{0,1\}$ as a guess of bit b. That is

$$b' = \begin{cases} 0 & if\ \zeta = \rho^{T_b} \oplus \varphi^{T_b} \oplus M_{3,i+1}^{T_b} \\ 1 & otherwise \end{cases}$$

As a result, the advantage function is given by

$$Adv_A^{upriv}(K) = |pr(b' = b) - pr(random\ coin\ flip)| = \left|pr(b' = b) - \tfrac{1}{2}\right| = \left|1 - \tfrac{1}{2}\right| = \tfrac{1}{2} \gg \varepsilon.$$

Proof: According to *Shi et al.*'s protocol, the following equations are given

If $T_b = T_0$

$$\rho^{T_b} \oplus \varphi^{T_b} \oplus M_{3,i+1}^{T_b} = CRC(funl(Meta_{ID}{}_{i+1}^{T_b}) \oplus R_{t,i+1}^{T_b}) \oplus CRC(funh(Meta_{ID}{}_{i+1}^{T_b}) \oplus R_{r,i+1}) \oplus CRC(funl(ID_{i+1}^{T_b}) \oplus R_{t,i+1}^{T_b} \oplus R_{r,i+1}).$$

Using the linear property, we have

$$= CRC\left(funl\big(Meta_{ID}{}_{i+1}^{T_b}\big)\right) \oplus CRC\big(R_{t,i+1}^{T_b}\big) \oplus CRC(funh(Meta_{ID}{}_{i+1}^{T_b})) \oplus CRC\big(R_{r,i+1}\big) \oplus CRC(funl(ID_{i+1}^{T_b}) \oplus CRC(R_{t,i+1}^{T_b}) \oplus CRC(R_{r,i+1}),$$

$$= CRC(funl(Meta_{ID}{}_{i+1}^{T_b})) \oplus CRC(funh(Meta_{ID}{}_{i+1}^{T_b})) \oplus CRC(funl\big(ID_{i+1}^{T_b}\big).$$

Using this fact that $T_b = T_0$, we have

$$= CRC(funl(Meta_{ID}{}_{i+1}^{T_0})) \oplus CRC(funh(Meta_{ID}{}_{i+1}^{T_0})) \oplus CRC(funl\big(ID_{i+1}^{T_0}\big).$$

In the learning phase, since the tag T_0 did not update its secret values, so $Meta\_ID_{i+1}^{T_0} = Meta\_ID_i^{T_0}$ and $ID_{i+1}^{T_0} = ID_i^{T_0}$, as a result $= CRC(funl(Meta\_ID_i^{T_0})) \oplus CRC(funh(Meta\_ID_i^{T_0})) \oplus CRC(funl(ID_i^{T_0})$
$= \zeta.$ ■

In summary, we proved that an adversary can trace the location of a specific tag in a specific session.

5- IMPROVED VERSION OF SHI ET AL.'S PROTOCOL

In this section, we propose some modifications in the structure of *Shi et al.*'s protocol to overcome all the reported weaknesses in Section 4. It is shown that due to some flaws in the tag responses and updating procedure of the *Shi et al.*'s protocol, their protocol cannot protect RFID users against secret parameter reveal, impersonation and traceability attack. Thus, in the improved version, we propose some changes in the exchanges messages between the tag and the reader, and modify the updating procedure of the tag and the back-end server. The changes and modifications are discussed in details in the following.

- In *Shi et al.*'s protocol, the values of M_2 and M_3 are given by $M_2 = CRC(funl(Meta\_ID) \oplus R_t) \parallel CRC(funh(Meta\_ID) \oplus R_r)$ and $M_3 = CRC(funl(ID) \oplus R_t \oplus R_r)$. We change their values to $M_2 = PRNG(funl(Meta\_ID) \oplus R_t) \parallel PRNG(funh(Meta\_ID) \oplus R_r)$ and $M_3 = PRNG(funl(ID) \oplus R_t \oplus R_r)$.
- The next change is in updating the tag and the back-end server as follows:

$$old_{ID} \leftarrow new_{ID} \leftarrow CRC(funl(new_{ID}) \oplus R_r) \parallel CRC(funh(new_{ID}) \oplus R_t).$$

$$old_{Meta_{ID}} \leftarrow new_{Meta_{ID}} \leftarrow CRC\big(funl\big(new_{Meta_{ID}}\big) \oplus R_r\big) \parallel CRC\big(funh\big(new_{Meta_{ID}}\big) \oplus R_t\big).$$

All authentication steps of the improved protocol are the same as *Shi et al.*'s protocol, except the proposed modifications in the updating procedure and the tag responses. Final structure of the improved protocol is shown on Fig. 4 wherein the authentication steps are provided with more details.

In the rest of this section, it is shown that how these changes prevent all the presented attacks and make the protocol more efficient and robust than before.

5-1- SECRET PARAMETER REVEAL

As it is shown in subsection 4-1, due to the dependency between the updating of secret keys and the structure of the tag response M_2, *Shi et al.*'s protocol cannot protect secret keys and an adversary can obtain the secret parameters with maximum 2^{16} computations. In the improved protocol, this problem is eliminated with our new changes in the updating procedure of $Meta\_ID$ and M_2 structure.

5-2- IMPERSONATION AND REPLAY ATTACK

In the proposed improved version of *Shi et al.*'s protocol, due to some changes applied in messages $M_2 = PRNG(funl(Meta\_ID) \oplus R_t) \parallel PRNG(funh(Meta\_ID) \oplus R_r)$ and $M_3 = PRNG(funl(ID) \oplus R_t \oplus R_r)$, which are exchanged between the tag and the reader, by using PRNG operator instead of CRC operator, the weaknesses that are reported in section 4 are omitted. Therefore, the adversary cannot use the eavesdropped messages and perform impersonation and replay attack.

5-3- PRIVACY

Providing confidential and untraceable communications for the end-users is one of the main goals of each RFID authentication protocol. In subsection 4-3, we showed that the privacy of *Shi et al.*'s protocol has some drawbacks and makes it unable to provide untraceable communication. In the modified protocol, we solve this problem by changing the message M_3 as $M_3 = PRNG(funl(ID) \oplus R_t \oplus R_r)$ and updating of $Meta\_ID$ as $Meta\_ID \leftarrow CRC(funl(Meta\_ID) \oplus R_r) \parallel CRC(funh(Meta\_ID) \oplus R_t)$. With these modifications,

Database $(old\_ID, new\_ID, old\_Meta\_ID, new\_Meta\_ID,)$	**Reader** (K)		**Tag** $(K, Meta\_ID_i, ID_i)$
For each $Meta\_ID_X$ *and* ID_X in DB generates M_2' and M_3' to verifying the tag and determines X=old or new for $Meta\_ID$ and ID. If X=new the server acts as follows, $M_5 = CRC(funh(\mathrm{Meta\_ID}) \oplus \mathrm{funl(ID)} \oplus R_t)$ $M_6 = CRC(\mathrm{funl(Meta\_ID)} \oplus \mathrm{funh(ID)} \oplus R_r)$	$R_r = PRNG(.)$ $M_1 = funh(k) \oplus R_r$	$M_1 \parallel Query \rightarrow$ $\leftarrow (M_2, M_3, M_4)$	Generates random numbers N_T and N_3 $\underline{M_2 = PRNG(funl(Meta\_ID) \oplus R_t)}$ $\underline{\parallel PRNG(funh(Meta\_ID) \oplus R_r)}$ $\underline{M_3 = PRNG(funl(ID) \oplus R_t \oplus R_r)}$ $M_4 = funl(k) \oplus R_t \oplus R_r$
Finally, the back-end server updates its secret values as follows; $If\ \ X = new$ $\underline{old\_ID \leftarrow new\_ID \leftarrow CRC(funl(new\_ID) \oplus R_r) \parallel CRC(funh(new\_ID) \oplus R_t)}$ $\underline{old\_Meta\_ID \leftarrow new\_Meta\_ID \leftarrow CRC(funl(new\_Meta\_ID) \oplus R_r) \parallel CRC(funh(new\_Meta\_ID) \oplus R_t)}$ $Else$ Do nothing End	$R_t = M_4 \oplus funl(k) \oplus R_r$ $\leftarrow (M_2, M_3, R_r, R_t)$ $(M_5, M_6) \rightarrow$		
		$(M_5, M_6) \rightarrow$	Using its ID and $\mathrm{Meta_{ID}}$ to calculates $\mathrm{M_5'}$ and $\mathrm{M_6'}$, comparing them with $\mathrm{M_5}$ and $\mathrm{M_6}$. If the tag verify the server secessesfully , it updates its secret values as follows, $\underline{\mathrm{ID_{i+1} \leftarrow CRC(funl(ID_i) \oplus R_r) \parallel CRC(funh(ID_i) \oplus R_t)}}$ $\underline{\mathrm{Meta_{ID_{i+1}} \leftarrow CRC\big(funl\big(Meta_{ID_i}\big) \oplus R_r\big) \parallel CRC(funh(MMeta\_ID_i) \oplus R_t}}$

Fig. 4. Improved version of Shi et al.'s protocol. The Dashed boxes show the modifications.

an adversary cannot remove the effect of random numbers R_t and R_r and traces the location of a specific tag.

Finally, we compare the security and the privacy of the improved protocol with some similar new-found RFID authentication protocols in Table 2. According to the last column, it can be seen that all the discovered drawbacks are eliminated in the improved version.

TABLE 2. A COMPARISON OF SECURITY ANALYSIS.

Protocols / Attacks	A [32]	B [33]	C [34]	D [35]	E [36]	F [21]	G
Secret Values Reveal	✓	✓	✓	×	×	×	✓
Replay	×	✓	✓	✓	✓	✓	✓
Impersonation	×	✓	×	×	×	×	✓
DoS	×	×	×	✓	✓	✓	✓
Traceability	×	×	×	×	×	×	✓

✓: Secure ×: Insecure

A. Chien et al. **B.** Pang et al. **C.** Safkhani et al. **D.** Yeh et al. **E.** Wang et al. **F.** Shi et al. **G.** Proposed protocol

5- CONCLUSION

We cryptanalyzed a CRC-based lightweight mutual authentication protocol which has been proposed recently for RFID systems by Shi et al. [21]. Shi et al. claimed that their protocol is safe against different security and privacy attacks. However, we showed that their protocol has some drawbacks which make it vulnerable to secret parameter reveal, tag impersonation and traceability attacks. We presented our traceability attack based on a well-known RFID formal privacy model proposed by *Ouafi* and *Phan*. Moreover, in order to increase the performance of Shi et al.'s protocol and prevent the presented attacks, we proposed some modifications in the structure of the original protocol and presented an improved protocol which removes all the existing weaknesses. The analysis illustrated that the improved protocol can provide secure and untraceable communication for RFID end-users. Finally, a comparison of security analysis for the improved protocol and some similar RFID authentication protocols was presented.

REFERENCE

[1] J. Banks, M. Pachano. L. Thompson, and D. Hanny, RFID applied, John Wiley & Sons, Inc., 2007.

[2] D. He, and Sh. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72 - 83 , 2015.

[3] M.H. Ok, and G. Uiwang, "A location tracking by RFID to assist the transportation vulnerable in subway stations," in 11th WSEAS International Conference on Mathematical methods and computational techniques in electrical engineering, 2009.

[4] L. Ruiz-Garcia, and L. Lunadei, "The role of RFID in agriculture: Applications, limitations and challenges," Computers and Electronics in Agriculture, vol. 79, no. 1, pp. 42-50, 2011.

[5] M. L. Ng, K. S. Leong, D. M. Hall, and P. H. Cole, "A small passive UHF RFID tag for livestock identification," in IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2005.

[6] P. Picazo-Sanchez, N. Bagheri, P. Peris-Lopez, and J. E. Tapiador, "Two RFID Standard-based Security protocols for healthcare environments," Journal of Medical Systems, vol. 37, no. 5, pp. 1-12, 2013.

[7] S. Maharjan, "RFID and IOT: An overview," Simula Research Laboratory University of Oslo, 2010.

[8] H. Gross, E. Wenger, H. Martín, and M. Hutter, "PIONEER: a Prototype for the Internet of Things Based on an Extendable EPC Gen2 RFID Tag," in Radio Frequency Identification: Security and Privacy Issues, pp. 54-73, 2014.

[9] L. Yang, P. Yu, W. Bailing, Q. Yun, B. Xuefeng, and Y. Xinling, "Hash-based RFID mutual authentication protocol," International Journal of Security & Its Applications, vol. 7, no. 3, 2013.

[10] D. Henrici, "RFID Security and privacy: concepts, protocols and architectures," Lecture Notes Electrical Engineering, Springer-Verlag Berlin Heidelberg, vol. 17, 2008.

[11] EPCglobal Inc., Available: http://www.epcglobalinc.org.

[12] H. Gross, E. Wenger, H. Martín, and M. Hutter, "PIONEER: a Prototype for the Internet of Things Based on an Extendable EPC Gen2 RFID Tag," in Radio Frequency Identification: Security and Privacy Issues, pp. 54-73, 2014.

[13] H. Hada, and J. Mitsugi, "EPC based internet of things architecture," in IEEE International Conference on RFID-Technologies and Applications (RFID-TA), 2011.

[14] B. Hameed, I. Khan, F. Durr, and K. Rothermel, "An RFID based consistency management framework for production monitoring in a smart real-time factory," in 2rd International Conference on the Internet of Things (IOT), Tokyo, 2010.

[15] T. C. Yeh, Y. J. Wanga, T. Ch. Kuo, and S. S. Wanga, "Securing RFID systems conforming to

EPC Class 1 Generation 2 standard," Expert Systems with Applications, vol. 37, p. 7678–7683, 2010.

[16] M.H. Habibi, M. R. Alaghband, and M. R. Aref, "Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard," in Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, Springer, 2011, pp. 254-263.

[17] E.-J. Yoon, "Improvement of the securing rfid systems conforming to EPC Class 1 Generation 2 standard," Expert Syst. Appl., vol. 39, no. 11, p. 1589–1594, 2012.

[18] S. M. Alavi, K. Baghery, B. Abdolmaleki, and M. R. Aref, "Traceability analysis of recent RFID authentication protocols," Wireless Personal Communications Journal, DOI 10.1007/s11277-015-2469-0, March 2015.

[19] A. Mohammadali, Z. Ahmadian, and M. R. Aref, "Analysis and Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard," IACR Cryptology ePrint Archive, vol. 66, pp. 1-9, 2013.

[20] F. Xiao, Y. Zhou, J. Zhou, H. Zhu, and X. Niu, "Security protocol for RFID system conforming to EPC-C1G2 standard," Journal of Computers, vol. 8, no. 3, pp. 605-612, 2013.

[21] Z. Shi, Y. Xia, Y. Zhang, Y. Wang, and J. Dai, "A CRC-based lightweight authentication protocol for EPCglobal Class-1 Gen-2 tags," in 14th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), 2014.

[22] I. Coisel, and T. Martin , "Untangling RFID privacy models," Journal of Computer Networks and Communications, pp. 1-26, 2013, DOI:10.1155/2013/710275.

[23] S. M. Alavi, B. Abdolmaleki, and K. Baghery, "Vulnerabilities and improvements on HRAP+, a hash-based RFID authentication protocol," Advances in Computer Science: an International Journal, vol. 3, no. 6, pp. 51-56, 2014.

[24] Z. Sohrabi-Bonab, M. R. Alagheband, and M. R. Aref, "Formal cryptanalysis of a CRC-based RFID authentication protocol," in The 22nd Iranian Conference on Electrical Engineering (ICEE 2014), Tehran, 2014.

[25] G. Avoine, "Adversarial model for radio frequency identification," Cryptology ePrint Archive, report 2005/049. http://eprint.iacr.org/2005/049, 2005.

[26] C. H. Lim, and T. Kwon, "Strong and robust RFID authentication enabling perfect ownership transfer," In Proceedings of ICICS '06, LNCS 4307 , pp. 1-20, 2006.

[27] A. Juels, and S.A Weis, "Defining strong privacy for RFID," in Proceedings of PerCom ′07, pp. 342–347. , 2006.

[28] K. Ouafi and R. C.-W. Phan, "Privacy of recent RFID authentication protocols," in 4th International Conference on Information Security Practice and Experience, Springer, 2008.

[29] R. H. Deng, Y. Li, M. Yung, and Y. Zhao, "A new framework work for RFID privacy," in 15th European Symposium on Research in Computer Security (ESORICS), Athens, 2010.

[30] D. Moriyama, S. Matsuo, and M. Ohkubo, "Relation among the security models for RFID authentication," in In 17th European symposium on research in computer security, pp. 661–678, 2012.

[31] S. Vaudenay, "On privacy models for RFID," in ASIACRYPT 2007, LNCS 4833, pp. 68–87., 2007.

[32] H. Y. Chien, and C. H. Chen, "Mutual authentication protocol for RFID confirming to EPC Class 1 Generation 2 standards," Computer Standards & Interfaces, vol. 29, no. 2, pp.254-259, 2007.

[33] L. Pang, H. Li, L. He, A. Alramadhan, and Y. Wang, "Secure and efficient lightweight RFID authentication protocol based on fast tag indexing," International Journal of Communication Systems, vol. 27, no. 11, pp. 3244-3254, 2014.

[34] M. Safkhani and N. Bagheri, "For an EPC-C1G2 RFID compliant Protocol, CRC with Concatenation: No; PRNG with Concatenation: Yes," Cryptology ePrint Archive, Report 2013/490, 2013

[35] Yeh T C, Wanga Y J, Kuo T C, Wanga S S, "Securing RFID systems conforming to EPC Class 1 Generation 2 standard," Expert Systems with Applications, 37 :7678–7683, 2010.

[36] Wang S, Liu S, Chen D, "Security analysis and improvement on two RFID authentication protocols," Wireless Personal Communications DOI 10.1007/s11277-014-2189-x, 2014.