**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.
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 Magnetic fields of readers.

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.

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 EPCglobal 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 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...

![Fig. 1. An RFID system architecture.](image-url)
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 \((R, T, i)\)**: 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 \( i \)th session. As a result, the adversary obtains all exchanged data between the tag \( T \) and the reader \( R \).
- **Send query \((U, V, m, i)\)**: 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 \( i \)th 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 \((T, K')\)**: 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 \((T_0, T_1, i)\)**: When this query is executed in the particular session \( i \), after completing \( i \)th 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 \( b \in \{0,1\} \) randomly and the adversary \( \mathcal{A} \) determines a tag \( T_b \in \{T_0,T_1\} \) using Execute and Send queries.

- **Guess phase**: Eventually, the adversary \( \mathcal{A} \) finishes the game \( G \) and outputs a bit \( b' \in \{0,1\} \) as guess of \( b \).
The success of adversary $\mathcal{A}$ in game $G$ and consequently breaking the notion of $U_{Priv}$ is quantified via $\mathcal{A}$ ’s advantage in recognizing whether adversary $\mathcal{A}$ received $T_0$ or $T_1$, and denoted by $Adv_{\mathcal{A}}^{U_{Priv}}(k)$ where $k$ is the security parameter.

$$Adv_{\mathcal{A}}^{U_{Priv}}(k) = |pr(b' = b) - pr(\text{random coin flip})| = \left| pr(b' = b) - \frac{1}{2} \right|.$$  

Where $0 \leq Adv_{\mathcal{A}}^{U_{Priv}}(k) \leq \frac{1}{2}$. Note that, if $Adv_{\mathcal{A}}^{U_{Priv}}(k) \ll \epsilon(k)$, 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 I.

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>the unique identifier of a specific tag</td>
</tr>
<tr>
<td>Meta-ID</td>
<td>the pseudonym of the tag</td>
</tr>
<tr>
<td>K</td>
<td>the 32-bit secret key shared by readers and</td>
</tr>
<tr>
<td>CRC( )</td>
<td>the CRC function</td>
</tr>
<tr>
<td>$R_r$</td>
<td>the pseudorandom number generated by a</td>
</tr>
<tr>
<td>$R_t$</td>
<td>the pseudorandom number generated by a</td>
</tr>
<tr>
<td>$funh(x)$</td>
<td>the function to get the left half-part of x</td>
</tr>
<tr>
<td>$funl(x)$</td>
<td>the function to get the right half-part of x</td>
</tr>
<tr>
<td>PRNG( )</td>
<td>Pseudo random number generator</td>
</tr>
<tr>
<td>$A \oplus B$</td>
<td>Concatenation operation</td>
</tr>
<tr>
<td>$A \not\oplus B$</td>
<td>Message A is XORed with message B</td>
</tr>
<tr>
<td>$A \not\oplus B$</td>
<td>Compare whether A is equal to B or not</td>
</tr>
</tbody>
</table>

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 $R_t = M_1 \oplus funh(k)$, then it generates a random number $R_t$ and computes the following messages and sends them to the reader.

$$M_2 = CRC(funh(Meta\_ID) \oplus R_t) \parallel CRC(funh(Meta\_ID) \oplus R_t).$$

$$M_3 = CRC(funh(ID) \oplus R_t \oplus R_r).$$

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

**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 ($M_2, M_3, R_t, R_r$) 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 $M_5 = CRC(funh(Meta\_ID) \oplus R_t) \parallel CRC(funh(Meta\_ID) \oplus R_t)$ and $M_6 = CRC(funh(ID) \oplus R_t \oplus R_r)$ for $X = old$ and new. Afterwards, it verifies $M_5 \oplus M_2 \oplus M_3$ and $M_6 \oplus M_5$ and determines that $X = old$ or new. If $M_5 \neq M_2$ and $M_6 \neq M_3$ for $X = old$ or new, it authenticates the tag and responds to the reader through the following messages.

$$M_5 = CRC(funh(Meta\_ID) \oplus funh(ID) \oplus R_t).$$

$$M_6 = CRC(funh(Meta\_ID) \oplus funh(ID) \oplus R_r).$$

Otherwise, the back-end server quizzes the protocol.

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

If $X = new$

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

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

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 $M'_5 \oplus M_5$ and $M'_6 \oplus M_6$. Finally, it updates its secret values as

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

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

otherwise, the tag aborts the protocol. Fig. 3 shows the detailed steps of Shi et al.’s protocol.

### 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 $CRC(A \oplus B) = CRC(A) \oplus CRC(B)$, 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 attack 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 $M_{1,i} = \text{funh}(k) \oplus R_{r,i}$, $M_{2,i} = \text{CRC}(\text{funl}(\text{Meta}_{ID_i}) \oplus R_{r,i}) \parallel \text{CRC}(\text{funl}(\text{Meta}_{ID_i}) \oplus R_{r,i})$, and $M_{3,i} = \text{CRC}(\text{funl}(ID_i) \oplus R_{r,i})$. After that, using message $M_{2,i}$ the adversary defines $\rho = \text{CRC}(\text{funl}(\text{Meta}_{ID_i}) \oplus R_{r,i})$ and $\varphi = \text{CRC}(\text{funl}(\text{Meta}_{ID_i}) \oplus R_{r,i})$. 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:

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

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

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

**Attack phase:** In this phase, the adversary acts as a legitimate tag and when the reader sends a Query and message $M_{1,i+1} = \text{funh}(k) \oplus R_{r,i+1}$ to the target tag. The adversary obtains message $M_{2,i+1}$. Then, by using obtained messages in the learning phase, the following messages are computed and sent to the reader.

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

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

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

Based on the receiving messages from the adversary, the reader first calculates $R_{r,i} = M_{4,\text{att}} \oplus \text{funl}(k) \oplus R_{r,i+1}$. Then, the reader sends messages $M_{2,\text{att}}, M_{3,\text{att}}, R_{r,i}$ 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 $M'_2 = \text{CRC}(\text{funl}(\text{Meta}_{ID} \oplus R_{r,i+1})$ and verifies $M'_2 \equiv M_{2,\text{att}}$ as follows,

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

$$M'_2 = \rho \parallel (\varphi \oplus \text{CRC}(M_{1,i}) \oplus \text{CRC}(M_{1,i+1}))$$

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

By using the linear property, we have

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

$$= \varphi \parallel \left(\rho \oplus \text{CRC}(R_{r,i}) \oplus \text{CRC}(R_{r,i+1})\right).$$

(1)

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

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

(2)

Again, by considering the linear property, $M_{2,\text{att}}$ is rewritten as

$$= \rho \parallel \left(\text{CRC}(\text{funh}(\text{Meta}_{ID_i}) \oplus R_{r,i}) \oplus \text{CRC}(R_{r,i}) \oplus \text{CRC}(R_{r,i+1})\right).$$

$$= \varphi \parallel \left(\rho \oplus \text{CRC}(\text{funh}(\text{Meta}_{ID_i}) \oplus R_{r,i+1})\right).$$

Finally, by substituting $\varphi = \text{CRC}(\text{funh}(\text{Meta}_{ID_i}) \oplus R_{r,i})$ in equation (3), we can write

$$= \text{CRC}(\text{funh}(\text{Meta}_{ID_i}) \oplus R_{r,i+1}) \parallel \left(\text{CRC}(\text{funh}(\text{Meta}_{ID_i}) \oplus R_{r,i+1})\right).$$

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

(4)

**Phase 2:** The back-end sever computes message $M'_2$ as

$$M'_2 = \text{CRC}(\text{funh}(\text{old}_{Meta_{ID}} \oplus R_{r,i+1})).$$

### Table: Shi et al.’s protocol [21]

<table>
<thead>
<tr>
<th>Database: $(\text{old}<em>{ID}, \text{new}</em>{ID}, \text{old}<em>{Meta</em>{ID}}, \text{new}<em>{Meta</em>{ID}})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader: $(K)$</td>
</tr>
<tr>
<td>Tag: $(K, \text{Meta}_{ID}, \text{ID})$</td>
</tr>
<tr>
<td>$R_r = \text{PRNG}(\cdot)$</td>
</tr>
<tr>
<td>$M_1 \parallel \text{Query} \rightarrow$</td>
</tr>
<tr>
<td>Generates random numbers $N_f$ and $N_g$</td>
</tr>
<tr>
<td>$M_2 = \text{CRC}(\text{funh}(\text{Meta}_{ID}) \oplus R_i)$</td>
</tr>
<tr>
<td>$\parallel \text{CRC}(\text{funh}(\text{Meta}_{ID}) \parallel R_i)$</td>
</tr>
<tr>
<td>$M_3 = \text{CRC}(\text{funh}(\text{ID}) \parallel R_i)$</td>
</tr>
<tr>
<td>$M_4 = \text{funh}(k) \parallel R_i \parallel R_r$</td>
</tr>
<tr>
<td>$R_i = M_4 \parallel \text{funh}(k) \parallel R_r$</td>
</tr>
<tr>
<td>$(M_2, M_3, M_4) \rightarrow$</td>
</tr>
<tr>
<td>$(M_2, M_3) \rightarrow$</td>
</tr>
<tr>
<td>Using its ID and Meta$<em>{ID_r}$ to calculates $M'<em>2$ and $M'</em>{2,\text{att}}$, comparing them with $M_2$ and $M_3$. If the tag verifies the server successfully, it updates as follows, $ID</em>{i+1} \leftarrow \text{PRNG}(\text{funh}(\text{ID}) \parallel R_i) \parallel \text{PRNG}(\text{funh}(\text{ID}) \parallel R_i)$. $\text{Meta}<em>{a</em>{ID_{i+1}}} \leftarrow \text{PRNG}(\text{funh}(\text{Meta}<em>{ID})) \parallel \text{PRNG}(\text{funh}(\text{Meta}</em>{ID}) \parallel R_i)$.</td>
</tr>
</tbody>
</table>

---

**Fig. 3. Shi et al.’s protocol [21].**
where $V = \{v_1, v_2, ..., v_{2^{16}}\}$. Now, using the new parameter $\varphi$.

For $1 \leq j \leq 2^{16}$

Choose $u_j \in U$

if $\varphi = \text{CRC}(u_j)$ then

return $v_j$ as $(\text{funh}(\text{Meta}_{IDI}) \oplus R_{i,j})$

End

Now, by using $(\text{funh}(\text{Meta}_{IDI}) \oplus R_{i,j})$ and $\text{funh}(\text{Meta}_{IDI}) \oplus R_{i,j}$ in the steps (a) and (b), the adversary calculates the secret value $\text{Meta}_{IDI}$ as $\text{Meta}_{IDI} = \text{PRNG}(\text{funh}(\text{Meta}_{IDI}) \oplus R_{i,j})$. Then, in order to compute the secret value $K$, the adversary uses the eavesdropped messages $M_{2,i+1}$, $M_{1,i+1}$ and $M_{6,i+1}$ 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 $\text{Meta}_{IDI}$ in steps (a) and (b), so

$$ R_{t,i+1} = \text{CRC}(\text{funh}(\text{Meta}_{IDI}) \oplus R_{i,j+1}) \oplus \text{CRC}(\text{funh}(\text{Meta}_{IDI})) $$

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

$$ = \text{CRC}(\text{funh}(\text{Meta}_{IDI})) \oplus \text{CRC}(\text{funh}(\text{Meta}_{IDI})) $$

- Then, adversary computes $\text{funh}(K)$ as

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

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

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

- After that, the adversary computes $\text{funh}(K)$ as

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

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

$$ \text{funh}(K) = \text{funh}(K) \oplus R_{r,i+1} \oplus R_{r,i+1} $$
Finally, adversary concatenates calculated $\text{funh}(K)$ and $\text{funl}(K)$ and computes the secret value $K$ as $K = \text{funh}(K) \oplus \text{funl}(K)$.

### 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 $\text{Execute query}(R, T_0, i)$ and obtains $(M_{2,i}^{T_0}, M_{3,i}^{T_0})$. Then, the adversary sends a $\text{Send query}(R, T_0, i)$ 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 $\rho_{T_0} = \text{CRC}(\text{funl}(\text{Meta}_{ID_1^{T_0}}) \oplus R_{t,i}^{T_0})$ and $\phi_{T_0} = \text{CRC}(\text{funh}(\text{Meta}_{ID_1^{T_0}}) \oplus R_{r,i}^{T_0})$ and computes $\zeta$ as $\zeta = \rho_{T_0} \oplus \phi_{T_0} \oplus M_{3,i}^{T_0} = \text{CRC}(\text{funl}(\text{Meta}_{ID_1^{T_0}})) \oplus \text{CRC}(\text{funh}(\text{Meta}_{ID_1^{T_0}})) \oplus \text{CRC}(\text{funl}(ID_{1}^{T_0})).$

#### Challenge phase:
In round $(i + 1)$, the adversary $\mathcal{A}$ selects two fresh tags $T_0$ and $T_1$ for test, and sends a $\text{Test query}(T_0, T_1, i + 1)$. 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 sends an $\text{Execute query}(R, T_b, i + 1)$, and obtains $(M_{2,t+1}^{T_b}, M_{3,t+1}^{T_b})$. Then, by using the first and the second parts of message $M_{2,t+1}^{T_b}$ the adversary defines new parameters $\rho_{T_b} = \text{CRC}(\text{funl}(\text{Meta}_{ID_1^{T_b}}) \oplus R_{t,i+1}^{T_b})$ and $\phi_{T_b} = \text{CRC}(\text{funh}(\text{Meta}_{ID_1^{T_b}}) \oplus R_{r,i+1}^{T_b})$. 

#### 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

$$b' = \begin{cases} 0 & \text{if } \zeta = \rho_{T_0} \oplus \phi_{T_0} \oplus M_{3,i+1}^{T_0} \\ 1 & \text{otherwise} \end{cases}$$

As a result, the advantage function is given by

$$Adv^\text{priv}_A(K) = |pr(b' = b) - pr(\text{random coin flip})| = |pr(b' = b) - \frac{1}{2}| = \left| 1 - \frac{1}{2} \right| = \frac{1}{2} \gg \varepsilon.$$ 

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

If $T_b = T_0$

$$\rho_{T_0} \oplus \phi_{T_0} \oplus M_{3,i+1}^{T_0} = \text{CRC}(\text{funl}(\text{Meta}_{ID_1^{T_0}}) \oplus R_{t,i+1}^{T_0}) \oplus \text{CRC}(\text{funh}(\text{Meta}_{ID_1^{T_0}}) \oplus R_{r,i+1}^{T_0}) \oplus \text{CRC}(\text{funl}(ID_{1}^{T_0}) \oplus \text{CRC}(R_{t,i+1}^{T_0}) \oplus \text{CRC}(R_{r,i+1}^{T_0})).$$

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

$$= \text{CRC}(\text{funl}(\text{Meta}_{ID_1^{T_0}})) \oplus \text{CRC}(\text{funh}(\text{Meta}_{ID_1^{T_0}})) \oplus \text{CRC}(\text{funl}(ID_{1}^{T_0})).$$

In the learning phase, since the tag $T_0$ did not update its secret values, so $\text{Meta}_{ID_1^{T_0}} = \text{Meta}_{ID_1^{T_0}}$ and $ID_{1}^{T_0} = ID_{1}^{T_0}$, as a result

$$= \text{CRC}(\text{funl}(\text{Meta}_{ID_1^{T_0}})) \oplus \text{CRC}(\text{funh}(\text{Meta}_{ID_1^{T_0}})) \oplus \text{CRC}(\text{funl}(ID_{1}^{T_0})).$$

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 $M_2 = \text{CRC}(\text{funl}(\text{Meta}_{ID}) \oplus R_r) \parallel \text{CRC}(\text{funh}(\text{Meta}_{ID}) \oplus R_r)$ and $M_3 = \text{CRC}(\text{funl}(ID) \oplus R_r \parallel \text{CRC}(\text{funh}(ID) \oplus R_r)$ for test, and sends a $\text{Message}_{query}(R, T_b, i + 1)$ to the update server.

- The next change is in updating the tag and the back-end server as follows:

$$\text{old}_{ID} \leftarrow \text{new}_{ID} \leftarrow \text{CRC}(\text{funl}(\text{new}_{ID}) \oplus R_r) \parallel \text{CRC}(\text{funh}(\text{new}_{ID}) \oplus R_r).$$

$$\text{old}_{Meta_{ID}} \leftarrow \text{new}_{Meta_{ID}} \leftarrow \text{CRC}(\text{funl}(\text{new}_{Meta_{ID}}) \oplus R_r) \parallel \text{CRC}(\text{funh}(\text{new}_{Meta_{ID}}) \oplus R_r).$$

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 $2^{36}$ 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 $M_2 = PRNG(funl(Meta_{ID}) \oplus R_t) \parallel PRNG(funl(Meta_{ID}) \oplus R_t)$ 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 $Meta_{ID} \leftarrow CRC(funl(Meta_{ID}) \oplus R_r)$. With these 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 II. According to the last column, it can be seen that all the discovered drawbacks are eliminated in the improved version.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret Values</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Reve</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Impersonation</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>DoS</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Traceability</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>


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 Ouaafi 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.

![Fig. 4. Improved version of Shi et al.’s protocol. The Dashed boxes show the modifications.](image-url)
Finally, a comparison of security analysis for the improved protocol and some similar RFID authentication protocols was presented.

6- REFERENCE


