ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 5, No.11 , September 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Security and Privacy Flaws in a Recent Authentication Protocol for EPC C1 G2 RFID Tags

Seyed Mohammad Alavi[1], Karim Baghery[2] and Behzad Abdolmaleki[3]

[1] Imam Hossein Comprehensive University
Tehran, Iran
malavi@ihu.ac.ir

[2] Information Systems and Security Lab (ISSL), Sharif University of Technology
Tehran, Iran
k.baghery.1988@ieee.org

[3] Information Systems and Security Lab (ISSL), Sharif University of Technology
Tehran, Iran
b.abdolmaleki.ir@ieee.org

Abstract

Recently, due to widespread use of Radio Frequency IDentification (RFID) systems in personal applications, security and privacy of these systems have got more attention. In order to provide security and privacy of RFID users, different authentication protocols have been proposed. In 2014, *Mohammadi et al.* proposed an improved authentication protocol for RFID systems. They claimed that their protocol is secure against various attacks. In this study, we investigate security and privacy of their protocol. It is shown that their protocol is not safe against several attacks including secret parameters reveal, tag impersonation, data integrity, desynchronization and also it cannot provide user privacy. Then, in order to omit aforementioned weaknesses, we apply some changes on *Mohammadi et al.*'s protocol and we propose an improved protocol. In addition, the security and privacy of the proposed protocol are analyzed against various attacks.

Keywords: *RFID Authentication Protocol, EPC C1 G2 Standard, Security and Privacy, Attack.*

1. Introduction

Radio Frequency Identification (RFID) systems allow us to identify subjects or objects without physical contact. Recently this technology have been utilized in almost all identification and authentication applications [1]- [2]. Generally, a RFID system consists of three main parts that are including tag, reader and back-end server. A tag is a small electronic chip that uses a microstrip antenna to make wireless connection with a reader. According to the power and memory of tags, they classify to the different classes. Based on supply power, the tags divided to the three categories. Some of the tags have a buttery that use it for internal processing and wireless communications. These type of tags called active tags. The next class of tags is passive tags that do not have their own battery and use reader's electrical field to supply their needed power. Communication distance of these tags is relatively short, i.e., 80-100 cm in the best case [3]. The last class is semi-passive tags and their capabilities are between active and passive tags. This kind of tags have a buttery but they use this battery just for internal processing and for wireless communications act like a passive tag and generate required power using reader's electrical field [4]. Beside mentioned applications, RFID tags and readers will play prominent role in the Internet of Things (IoT) and Internet of Device (IoD) systems that are the next generation of internet [5]. In IoT and IoD systems, all existing objects in our environment will connect to each other and will share information with other objects or subjects [5]. These connections can be made by RFID tags, GPS or any sensing device.

A system model of a RFID system is shown in Fig. 1 [6]. It can be seen that each reader located between the tags and the back-end server and can exchange data between them. In some applications there are several tags (e.g., physical access control in a company) in deployed system model. But in some RFID systems there are lots of tags (e.g., books in library or shopping centers) that can have a big influence on the authentication performances. The third and the main part of each RFID system model is database. The database contains all secret information about tags and it uses them on tags authentication and identification processes.

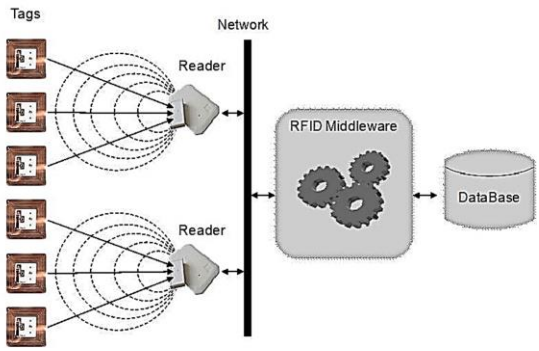

Fig. 1. A System model of RFID systems [6].

Due to nature of wireless communication, each wireless communication in insecure channel can be eavesdropped by an illegal person. In each RFID system there are two communication channels between the tag, the reader and the database. The communication channel between the tag and the reader is insecure and can be eavesdropped by an adversary. But in some cases communication channel between the reader and the database is secure.

In the recent years, due to widespread use of RFID systems in different applications, the security and the privacy of end-users have become very important. In order to protect security and privacy of RFID users, different authentication protocols have been proposed [7] - [13]. Although, all the designed protocols have been proposed to provide secure communications for RFID systems and keep safe their privacy, it is showed that most of the proposed protocols are vulnerable against various attacks and need more challenging to optimize their security [7], [14]- [15].

In the last few years, EPC Class 1 Generation 2 (EPC C1 G2) is one of the most challenging RFID standards that proposed by EPCGlobal [16]. Some protocols that are based on EPC C1 G2 standards and proposed recently are reported in [7], [14] - [15], [17] - [18].

In 2010, *Yeh et al.* proposed a RFID mutual authentication protocol for RFID systems that is accordance to the EPC C1 G2 standard [19]. They claimed that their protocol can provide security and privacy of RFID users. In 2011, *Habibi et al.* [8] showed that still *Yeh et al.*'s protocol is vulnerable against some security and privacy attacks and cannot provide secure communication. Then, they applied some changes on *Yeh et al.'s* protocol and proposed an improved version. In 2014, *Mohammadi et al.* [13] analyzed the security and the privacy of *Habibi et al.*'s protocol and showed that their protocol has some security problems and suffers from secret parameters reveal, tag impersonation attack, data desynchronization attack and traceability attack. Then, *Mohammadi et al.* revised *Habibi et al.*'s protocol and proposed an improved lightweight mutual authentication protocol (ILMAP) for RFID systems. They analyzed the security and the privacy of the ILMAP protocol and claimed that with new changes all weaknesses of *Habibi et al.*'s protocol are omitted and the improved protocol is resistant against different threats.

In this study, we investigate the security and the privacy of the ILMAP protocol. It is shown that ILMAP protocol is vulnerable against some attacks and it cannot provide secure communication for RFID users. More precisely, it is shown that ILMAP protocol suffers from secret parameters reveal, data integrity, reader forward compromise, traceability attack, backward traceability attack and forward traceability attack. Then, in order to increase the security and the privacy of ILMAP protocol, we change some processes of ILMAP protocol and proposed a strengthened version of it. Then, we investigate resistance of the improved protocol against different attacks. Security analysis show that the improved protocol removes all existing weaknesses of ILMAP protocol and also it is secure against different attacks.

The structure of paper is organized as follows: the ILMAP protocol is introduced in section 2. In section 3, we investigate vulnerabilities of the ILMAP protocol. In section 4, an improved version of the ILMAP protocol presented. The security and privacy of the proposed protocol are analyzed in section 5, also in this section analysis of the proposed protocol are compared with some similar protocols that are in the accordance with EPC C1 G2 standard and proposed recently. Finally, we conclude this paper in section 6.

2. The ILMAP Protocol

The ILMAP protocol is a RFID mutual authentication protocol conforming to EPC C1 G2 standard that proposed by *Mohamadi et al.* in [13]. The structure of protocol and authentication procedure are shown in Fig. 2. As it mentioned above, this protocol is based on EPC C1 G2 standard and uses $PRNG(.)$ and EPC_i to protect exchanged messages. Table 1 shows the notations that are used in the ILMAP protocol. In the ILMAP protocol, all communication channels between the tag, the reader and the back-end server are insecure and can be eavesdropped by an adversary.

Table 1. The Notations of ILMAP protocol

Not.	Description
$\mathbf{M}_{req}$	Request message
$\mathbf{EPC}_i$	Electronic Product Code (EPC) of the i*th* tag
$\mathbf{D}_i$	Product information of the i*th* tag
$\mathbf{K}_i$	The authentication key shared by back-end server and tag
$\mathbf{N}_i$	The communications key shared by back-end server and tag
$\mathbf{PID}_i$	The pseudonym identification code of the i*th* tag
$\mathbf{RID}_j$	The pseudonym identification code of *j*th reader

$\mathbf{r_i}$	A random number
$\mathbf{H}(.)$	Hash function
$\boldsymbol{PRNG}(.)$	Pseudo random number generator
$(.)'$	For second run of protocol
$\|$	Concatenation operation
$\mathbf{A} \oplus \mathbf{B}$	Message A is XORed with message B
$\mathbf{A} \stackrel{?}{=} \mathbf{B}$	Compare whether A is equal to B or not

3.1 Security Analysis

In this subsection, the security of ILMAP protocol is analyzed. It is shown that it has some security problems that make it vulnerable against secret parameter reveal, DATA integrity and reader forward secrecy compromise. Security analysis are given in the rest of subsection with more details.

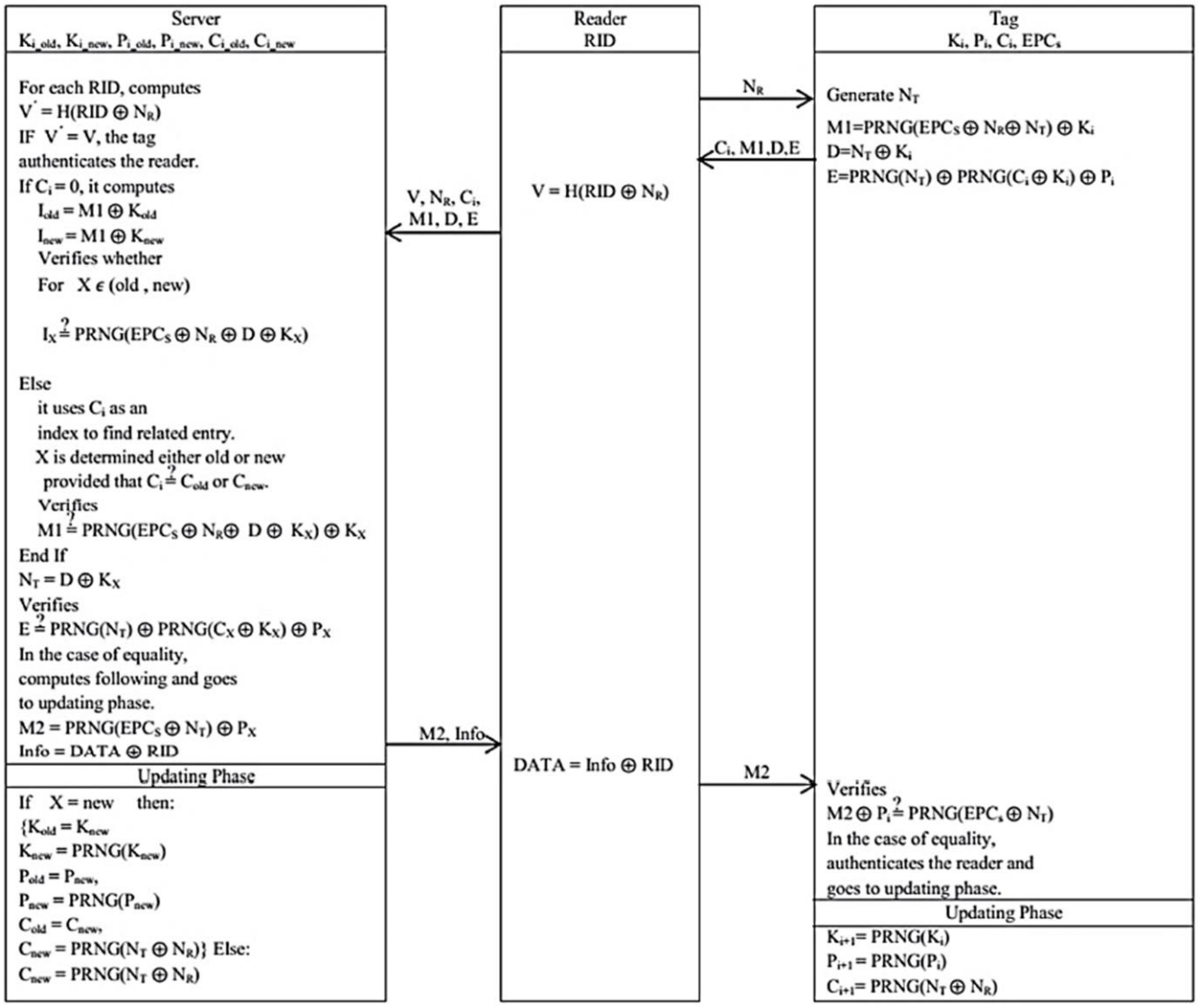

Fig. 2. The ILMAP protocol.

3. Vulnerabilities of ILMAP Protocol

This section aims to analyze the security and the privacy of ILMAP protocol. It is shown that the security and the privacy of ILMAP have some problems that makes it vulnerable against some security attacks also it cannot provide user privacy. For privacy analysis, we use a formal privacy model that proposed by *Ouafi* and *Phan* in [4].

3.1.1 Secret parameter reveal

In the designing of the RFID authentication protocols, it is very important that the secret parameters be safe in communications and an attacker could not obtain them. Here we present a practical attack on ILMAP protocol which shows that an attacker is able to reveal all secret

parameters (EPC_s, K_i, P_i). This attack consists of two phases as follows,

Learning phase: First, the attacker acts as an eavesdropper. After one successful run, he/she saves the exchanged data between the target tag and the reader including N_R , $M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$, $D = N_T \oplus K_i$, $E = PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$, $M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$.

Attack phase: In the next session, when the target tag responds to the reader, the attacker eavesdrops C_{i+1} and aborts the rest of protocol. Then, the attacker uses C_{i+1} and eavesdropped messages and performs following steps,

a) Since $\boldsymbol{N_T}$ is a 16-bit string, thus $\boldsymbol{N_T \in U}$ where $\boldsymbol{U = \{U_1, U_2, \dots, U_{2^{16}}\}}$. Now, using the obtained $\boldsymbol{N_R}$ in the learning phase,

$For\ 1 \le j \le 2^{16}$
$\quad Choose\ u_j \in U$
$\quad if\ \ C_{i+1} = PRNG(u_j \oplus N_R)\ \ then$
$\quad return\ u_j\ as\ N_T$
End

Now, using the obtained $\boldsymbol{N_T}$ and eavesdropped $\boldsymbol{D}$ in learning phase, the value of $\boldsymbol{K_i}$ can be calculated as follows,

$$K_i = N_T \oplus D$$

b) Since the length of $\boldsymbol{EPC_s}$ is 16-bit, thus $\boldsymbol{EPC_s \in V}$ where $\boldsymbol{V = \{V_1, V_2, \dots, V_{2^{16}}\}}$. Now using $\boldsymbol{K_i}$ and $\boldsymbol{N_T}$ that are obtained in the first step and messages $\boldsymbol{M_1}$ and $\boldsymbol{N_R}$ that eavesdropped in the learning phase, the attacker can perform following operations,

$For\ 1 \le j \le 2^{16}$
$Choose\ v_j \in V$
$if\ \ M_1 = PRNG(v_j \oplus N_R \oplus N_T) \oplus K_i\ \ then$
$\quad return\ v_j\ as\ EPC_s$
End

c) Now via $\boldsymbol{EPC_s}$ and $\boldsymbol{N_T}$, the secret value of $\boldsymbol{P_X}$ can be computed as follows,

$$\mathrm{P_X} = M_2 \oplus PRNG(EPC_s \oplus N_T)$$

It can be seen that in this attack the attacker needs one session eavesdropping and 2×2^{16} *PRNG* computations. It is worth to mention that after performing this attack and obtaining all secret values of the tag, the attacker can perform lots of attacks including traceability attack, tag impersonation attack, reader impersonation attack, and desynchronization attack with the success probability of "1". Furthermore, the ILMAP protocol has some another weaknesses that in the rest of paper some of the possible attacks are given.

3.1.2 DATA integrity problem

In the ILMAP protocol RID is used to protect the transmission of $DATA$ between the back-end server and the reader. Due to structure of $info = DATA \oplus RID$, *Mohammadi et al.* claimed that an attacker cannot forge the transmission $DATA$ between the back-end server and the reader. However, it is shown that ILMAP protocol cannot protect the integrity of DATA. This attack can be expressed as follows,

a) When the back-end server sends $\boldsymbol{M_2}$ and $\boldsymbol{info}$ to the reader, the attacker intercepts them.

b) The attacker calculates a forged value $\boldsymbol{info_{att} = info \oplus \delta}$, where $\boldsymbol{\delta}$ is a random value that generated by the attacker, and then forwards $\boldsymbol{M_2}$ and $\boldsymbol{info_{att}}$ to the reader.

c) Upon receiving $\boldsymbol{M_2}$ and $\boldsymbol{info_{att}}$, the reader retrieves $\boldsymbol{RID}$ and in order to obtain $\boldsymbol{DATA \oplus \delta}$, the reader XORs calculated $\boldsymbol{RID}$ with the received $\boldsymbol{info_{att}}$ and forwards $\boldsymbol{M_2}$ to the tag.

As it can be seen the XORed result $DATA \oplus \delta$ is not equal to the original value of $DATA$ which generated in the back-end server. As a result, the stored $DATA$ in the reader is not correct but the reader believes that is original $DATA$.

Note that, since the attacker did not change M_2, the tag did not recognize this forgery attack. Therefore, the ILMAP protocol has DATA integrity problem.

3.1.3 Reader Forward Secrecy Compromise

In forward secrecy, if a secret value of the reader will be compromised by an attacker, the attacker should not be able to perform traceability attacks and trace the location of victim reader in the different rounds. Here now, it is shown that ILMAP protocol cannot preserve reader forward secrecy. To this aim, the attacker obtains N_R by eavesdropping exchanged messages in one session of protocol. After that, the attacker obtains RID by compromising the victim reader and verifies $H(RID \oplus N_R) \stackrel{?}{=} V$ to trace the victim reader. As a result, ILMAP protocol is not secure against reader forward secrecy attack.

3.2 Privacy Analysis

Beside mentioned weaknesses, the ILMAP protocol cannot provide user privacy and it is vulnerable against backward traceability, traceability and forward traceability attacks. In the recent years, in order to study and analyze the privacy of RFID authentication privacy different formal methods as a formal privacy model have been proposed [4], [20], [21], [22]. In [4], *Ouafi* and *Phan* presented a privacy model to evaluate RFID protocols. In *Ouafi* and *Phan* privacy model, the attacker's abilities are classified in four different categories including $Execute\ Query$, $Crrupt\ Query$, $Sent\ Query$ and $Test\ Query$. In each

query, the attacker has different abilities that are reported in [4] with more details. In this section, we analyze the privacy of ILMAP protocol and present our privacy attacks based on *Ouafi* and *Phan* privacy model.

3.2.1 Traceability Attack

Privacy concern is one of the most important issues in designing of the RFID authentication protocols. In the rest of this subsection we show that ILMAP protocol is not safe against traceability attack and an attacker can trace the location of a specific tag. To this aim, the attacker acts as following,

Learning phase: In ith round, the attacker $\mathcal{A}$ sends an $Execute\ query(R, T_0, i)$ by sending N_R and obtains $C_i^{T_0}$.

Challenge phase: The attacker $\mathcal{A}$ choses two fresh tags T_0 and T_1 for test, and sends a $Test\ query(T_0, T_1, i+1)$. According to the bit $b \in \{0,1\}$ that chosen randomly, the attacker is given a tag $T_b \in \{T_0, T_1\}$. Next, the attacker $\mathcal{A}$ sends an $Execute\ query(R, T_b, i+1)$ by sending N_R, and it obtains $C_{i+1}^{T_b}$.

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

$$b' = \begin{cases} 0 & if\ C_{i+1}^{T_b} = C_i^{T_0} \\ 1 & otherwise \end{cases} \quad (1)$$

As a result, it can be written:

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

Proof: According to the ILMAP protocol in Fig. 2, it can be seen that since the tag T_0 does not update its secret value and uses the same C_i in the both *Learning* and *Challenge phases*, the attacker can perform traceability attacks and track the target tag.

3.2.2 Forward Traceability Attack

This subsection aims to show that ILMAP protocol suffers from forward traceability attack. In the ILMAP protocol the EPC_s is fixed in all rounds and it does not change in the next run. It can be shown that an attacker can use this fact and perform forward traceability attack as follows.

Learning phase: In the ith round, the attacker $\mathcal{A}$ sends a $Corrupt\ query(T_0, K')$ and obtains $(K_i^{T_0}, C_i^{T_0}, EPC_{s,i}^{T_0})$ from tag T_0. It also sends an $Execute\ query(R, T_0, i)$ and obtains $N_{R,i}$. Now the attacker can compute K_{i+j} at the session $i+j$ by j times repeating $PRNG$ of K_i for $j \geq 1$. Therefore, if we have D_{i+j}, $N_{T,i+j}$ can be obtained by XORing K_{i+j} and D_{i+j} as $N_{T,i+j} = K_{i+j} \oplus D_{i+j}$.

Challenge phase: The attacker $\mathcal{A}$ choses two new tags T_0 and T_1 for the test, and sends a $Test\ query(T_0, T_1, i)$. According to the bit $b \in \{0,1\}$ that chosen randomly, the attacker is given a tag $T_b \in \{T_0, T_1\}$. After that, in round $(i+2)$th, the attacker sends an $Execute\ query(R, T_b, i+2)$ by sending $N_{R,i}$ (i.e., the same value of session i) and obtains $(M_{1,i+2}^{T_b}, D_{i+2}^{T_b})$.

Guess phase: The attacker $\mathcal{A}$ stops the game G, and outputs a bit $b' \in \{0,1\}$ as a guess of bit b. In order to guess b', firstly the attacker computes $\alpha = PRNG\left(PRNG\left(K_i^{T_0}\right)\right)$, $\beta = D_{i+2}^{T_b} \oplus \alpha$ and $\gamma = PRNG\left(EPC_{s,i}^{T_0} \oplus N_{R,i} \oplus \beta\right)$, where γ is a 16-bit string. Then, outputs a bit $b' \in \{0,1\}$ as a guess of bit b using the following rule,

$$b' = \begin{cases} 0 & if\ M_{1,i+2}^{T_b} = \gamma \oplus \alpha \\ 1 & otherwise \end{cases} \quad (2)$$

As a result, it can be written that,

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

Proof: Since the value of EPC_s is fixed in all rounds, thus $EPC_{s,i}^{T_0} = EPC_{s,i+2}^{T_0}$. Using this fact, the following equations can be written.

(1) $If\ T_b = T_0$

$$=> K_{i+2}^{T_b} = PRNG\left(PRNG\left(K_i^{T_b}\right)\right)$$
$$= PRNG\left(PRNG\left(K_i^{T_0}\right)\right)$$
$$= K_{i+2}^{T_0} = \alpha$$

(2) $If\ T_b = T_0$

$$=> N_{T,i+2}^{T_b} = D_{i+2}^{T_b} \oplus K_{i+2}^{T_b}$$
$$= D_{i+2}^{T_b} \oplus \alpha = \beta$$

(1), (2) =>

$$M_{1,i+2}^{T_b} = K_{i+2}^{T_b} \oplus PRNG\left(EPC_{s,i+2}^{T_b} \oplus N_{R,i+2}^{T_b} \oplus N_{T,i+2}^{T_b}\right)$$
$$= \alpha \oplus PRNG\left(EPC_{s,i}^{T_0} \oplus N_{R,i} \oplus \beta\right)$$
$$= \alpha \oplus \gamma \quad (3)$$

3.2.3 Backward Traceability Attack

Beside mentioned traceability concerns, it can be shown that ILMAP protocol does not assure the backward untraceability attack. In updating of ILMAP protocol, it can be seen that K_i is $PRNG$ of K_{i-1}. In the rest of subsection, we showe that an attacker can use this issue and obtain K_{i-1} with 2^{16} computations.

Learning phase: In the ith round, the attacker $\mathcal{A}$ sends a $Corrupt\ query(T_0, K')$ and obtains $K_i^{T_0}$ and $EPC_{s,i}^{T_0}$ from tag T_0.Now, since K_i is a 16-bit string, thus $K_i \epsilon U$ where $U = \{U_1, U_2, \dots, U_{2^{16}}\}$. Now,

$$For\ 1 \le j \le 2^{16}$$
$$Choose\ u_j \in U$$
$$if\ \ K_i^{T_0} = PRNG(u_j)\ \ then$$
$$return\ u_j\ as\ K_{i-1}^{T_0}$$
$$End$$

It can be seen that the value of $K_{i-1}^{T_0}$ can be obtained after maximum 2^{16} computations.

Challenge phase: The attacker $\mathcal{A}$ selects two fresh tags T_0 and T_1 for test, and sends a $Test\ query(T_0, T_1, i)$. According to the randomly chosen bit $b \epsilon \{0,1\}$, the attacker is given a tag $T_b \epsilon \{T_0, T_1\}$. After that, in round $(i-1)$th, the attacker sends an $Execute\ query(R, T_b, i-1)$, and obtains $C_{i-1}^{T_b}$, $D_{i-1}^{T_b}$, $E_{i-1}^{T_b}$ and $M_{2,i-1}^{T_b}$. Then, the attacker computes $\alpha = K_{i-1}^{T_0} \oplus D_{i-1}^{T_b}$ and $\beta = PRNG\big(EPC_{S,i}^{T_0} \oplus \alpha\big) \oplus PRNG(\alpha) \oplus PRNG\big(K_{i-1}^{T_0} \oplus C_{i-1}^{T_b}\big)$.

Guess phase: The attacker $\mathcal{A}$ stops the game G, and outputs a bit $b' \epsilon \{0,1\}$ as a guess of bit b. In order to determine $b' \epsilon \{0,1\}$, the attacker uses the following rule,

$$b' = \begin{cases} 0 & if\ \ M_{2,i-1}^{T_b} \oplus E_{i-1}^{T_b} = \beta \\ 1 & otherwise \end{cases} \quad (4)$$

As a result, it can be written:

$$Adv_A^{upriv}(K) = |pr(b' = b) - pr(random\ coin\ flip)|$$
$$= \left|pr(b' = b) - \tfrac{1}{2}\right| = \left|1 - \tfrac{1}{2^{16}}\right|$$
$$= \left|\left(1 - \tfrac{1}{2^{16}}\right) - \tfrac{1}{2}\right| = \tfrac{1}{2} - 2^{-16} \gg \varepsilon$$

Proof: In the updating procedure of ILMAP protocol we see that $K_i^{T_0} \leftarrow PRNG\big(K_{i-1}^{T_0}\big)$. With assuming this fact following equations can be written,

$If\ \ T_b = T_0$

$$\beta = PRNG\big(EPC_{S.i}^{T_0} \oplus \alpha\big) \oplus PRNG(\alpha) \oplus PRNG\big(K_{i-1}^{T_0} \oplus C_{i-1}^{T_b}\big)$$
$$= PRNG\big(EPC_{S,i}^{T_0} \oplus K_{i-1}^{T_0} \oplus D_{i-1}^{T_b}\big) \oplus PRNG\big(K_{i-1}^{T_0} \oplus D_{i-1}^{T_b}\big) \oplus PRNG\big(K_{i-1}^{T_0} \oplus C_{i-1}^{T_b}\big)$$
$$= PRNG\big(EPC_{S,i}^{T_0} \oplus N_{T,i-1}^{T_b}\big) \oplus PRNG\big(N_{T,i-1}^{T_b}\big) \oplus PRNG\big(K_{i-1}^{T_0} \oplus C_{i-1}^{T_b}\big)$$
$$= PRNG\big(EPC_{S,i-1}^{T_0} \oplus N_{T,i-1}^{T_b}\big) \oplus PRNG\big(N_{T,i-1}^{T_b}\big) \oplus PRNG\big(K_{i-1}^{T_b} \oplus C_{i-1}^{T_b}\big)$$
$$= M_{2,i-1}^{T_b} \oplus E_{i-1}^{T_b} \quad (5)$$

It is worth to mention that $EPC_S^{T_0}$ is fixed in all rounds, so $EPC_{S,i}^{T_0} = EPC_{S,i-1}^{T_0}$.

4. Improved Version of ILMAP Protocol

In section 3, it is shown that ILMAP protocol has some weaknesses that due to these weaknesses this protocol suffers from secret parameters reveal, data integrity attack and reader forward secrecy compromise, also it is not safe against privacy threats. In this section, we aim to propose a strengthened version of the ILMAP protocol that removes all existing weaknesses. In the proposed protocol we apply some changes on updating, authentication and responses messages that increase the security and privacy of the proposed protocol and make it secure against different attacks. The new changes can be expressed as follows,

- In the ILMAP protocol the value of E is equal to $E = PRNG(N_T) \oplus PRNG(C_i \oplus K_i) \oplus P_i$ that in the proposed protocol we change it to the $E = N_T \oplus PRNG(C_i \oplus K_i) \oplus PRNG(P_i)$.
- In the ILMAP protocol, in each run, the tag sends C_i directly to the reader. In the proposed protocol, we changed this message and the tag does not send C_i directly to the reader. Instead it sends $C_i = C_i \oplus N_3$ to the reader, where N_3 is a random number that generate by the tag in each run of protocol.
- In the new protocol, also we change reader to the back-end server response. In the ILMAP protocol, the reader responses to the back-end server with $V = H(RID \oplus N_R)$ that in the proposed protocol we change it to the $V = H(RID \oplus N_R \oplus E)$.
- The next change is in the back-end server responses. In ILMAP protocol, the back-end server responses to the reader with $info$ and M_2. In the proposed protocol, we define a new message $MAC = H(DATA \oplus N_R)$ that the back-end server sends it to the reader together with $info$ and M_2.
- Moreover, we modify updating of ILMAP as follows,

$$K_{i+1} \leftarrow PRNG(K_i \oplus N_3)$$
$$P_{i+1} \leftarrow PRNG(P_i)$$
$$C_{i+1} \leftarrow PRNG(N_T \oplus N_R \oplus P_i).$$

The structure of the proposed protocol is shown in Fig. 3 that all mentioned changes are reported with more details.

In the next section, the security and the privacy of proposed protocol is analyzed and it is shown that how the

new changes remove all mentioned weaknesses on the ILMAP protocol.

5. Analysis of Proposed Protocol

In this section, in order to evaluate the security and the privacy of proposed protocol, some analysis are provided. Indeed, we investigate the proposed protocol against different attacks.

5.3 Impersonation Attack

In the proposed protocol, in order to perform impersonation attacks, the attacker needs EPC_s, N_T and K_i to calculate exchanged messages between the tag and the reader including M_1 , D , C_i and E , where $E = N_T \oplus PRNG(C_i \oplus K_i) \oplus PRNG(P_i)$ and $C_i = C_i \oplus N_3$. In other side, since all mentioned secret parameters are protected, thus the attacker cannot impersonate the tag or the reader. As a result the proposed protocol is secure against impersonation attacks.

Database $(K_{old}, C_{old}, P_{old}, K_{new}, C_{new}, P_{new}, RID, EPC, DATA)$	**Reader** (RID)		**Tag** (K_i, C_i, P_i, EPC_s)
For each RID in DB $Verify\ H(RID \oplus N_R \oplus E) \stackrel{?}{=} V$ *If* $I_{new} = M_1 \oplus K_{new}$ $I_{new} \stackrel{?}{=} PRNG(EPC_s \oplus N_R \oplus D \oplus K_{new})$ $X = new$ Else: $I_{old} = M_1 \oplus K_{old}$ $I_{old} \stackrel{?}{=} PRNG(EPC_s \oplus N_R \oplus D \oplus K_{old})$ $X = old$ End $Verify\ \ PRNG(C_i \oplus K_X) \oplus D \oplus K_X \oplus PRNG(P_X) \stackrel{?}{=} E$ Then computes values below: $N_T = D \oplus K_X$ $M_2 = PRNG(EPC_s \oplus N_T) \oplus P_X$ $Info = DATA \oplus RID$ $MAC = H(DATA \oplus N_R)$ $N_3 = C_i \oplus C_X$		$N_R \rightarrow$	Generates random numbers N_T and N_3 $M_1 = PRNG(EPC_s \oplus N_R \oplus N_T) \oplus K_i$ $D = N_T \oplus K_i$ $C_i = C_i \oplus N_3$ $E = N_T \oplus PRNG(C_i \oplus K_i) \oplus PRNG(P_i)$
		$\leftarrow (M_1, D, C_i, E)$	
	$V = H(RID \oplus N_R \oplus E)$		
	$\leftarrow (M_1, D, C_i, E, N_R, V)$		
	$(M_2, Info, MAC) \rightarrow$		
	$DATA = Info \oplus RID$ $Verify\ H(DATA \oplus N_R) \stackrel{?}{=} MAC$		
If $X = new$ $K_{old} \leftarrow K_{new} \leftarrow PRNG(K_{new} \oplus N_3)$ $P_{old} \leftarrow P_{new} \leftarrow PRNG(P_{new})$ $C_{old} \leftarrow C_{new} \leftarrow PRNG(N_T \oplus N_R \oplus P_X)$ *Else* $C_{new} \leftarrow PRNG(N_T \oplus N_R \oplus P_X)$ *End* If		$M_2 \rightarrow$	$Verify\ M_2 \oplus P_i \stackrel{?}{=} PRNG(EPC_s \oplus N_T)$ $K_{i+1} \leftarrow PRNG(K_i \oplus N_3)$ $P_{i+1} \leftarrow PRNG(P_i)$ $C_{i+1} \leftarrow PRNG(N_T \oplus N_R \oplus P_i)$

Fig. 3. Improved version of ILMAP protocol.

5.1 Secret Parameters Reveal

In section 3.1.1, we observed that how an attacker can use C_i to obtain N_T, and consequently how he/she can uses the obtained N_T to calculate K_i using $D = N_T \oplus K_i$. But in the proposed protocol this weaknesses omitted by changing $C_i = PRNG(N_T \oplus N_R)$ to $C_i = PRNG(N_T \oplus N_R \oplus P_i)$. It can be seen that with new C_i the attacker can not obtain N_T and K_i. As a result, the proposed protocol is safe against secret parameters reveal attack.

5.2 Replay Attack

In the proposed protocol, due to applied some changes in the exchanged data between the tag and the reader including E and C_i, and also due to generate two new numbers (N_3 and N_T) in each session of the protocol, the attacker cannot perform replay attack.

5.4 Reader forward secrecy

In the proposed protocol, in order to remove this weakness we changed $V = H(RID \oplus N_R)$ to $V_{new} = H(RID \oplus N_R \oplus E)$ where $E = N_T \oplus PRNG(C_i \oplus K_i) \oplus PRNG(P_i)$. It can be seen that since the value of E varies in each run of protocol, even if the reader be compromised by the attacker, he/she will not be able to track previous communications. As a result, the proposed protocol is safe against reader forward secrecy compromise.

5.5 Privacy

In section 3.2, it is showed that the privacy of ILMAP protocol has some problems that makes it vulnerable against all traceability attacks. In the proposed protocol, in order to enhance the privacy and remove all mentioned privacy attacks, we apply two changes in the updating

procedures. First, we change updating of $C_i = PRNG(N_T \oplus N_R)$ to $C_i = PRNG(N_T \oplus N_R \oplus P_i)$ that makes it resistance against traceability attack. In addition, in order to prevent backward and forward traceability attacks, we exchange updating procedure of $K_i = PRNG(K_i)$ with $K_i = PRNG(K_i \oplus N_3)$, where N_3 is a new random number that generated by the tag. It can be seen that with these changes, the attacker cannot threat the privacy of end-users. Therefore, the proposed protocol can provide user privacy and it is safe against different traceability attacks.

Table 2 shows a comparison of the security and privacy analysis for proposed protocol and some similar protocols that are under EPC C1 G2 standard and have been proposed recently. As it can be seen, the security and the privacy of the proposed protocol are complete and it can provide secure communications for RFID and IoT users.

Table 2. Comparison of security analysis

Protocols / Attack	Yeh *et al* [19]	Habibi *et al* [8]	ILMAP [23]	Improved ILMAP
Secret Values Reveal	×	×	×	✓
Replay	✓	✓	✓	✓
Impersonation	×	×	✓	✓
Reader Forward Secrecy	✓	✓	×	✓
Data Integrity	×	✓	×	✓
Backward Traceability	×	✓	×	✓
Traceability	×	×	×	✓
Forward Traceability	✓	✓	×	✓

✓: Secure ×: Insecure

6. Conclusions

In this study, we cryptanalyzed a mutual authentication protocol for RFID systems that proposed by *Mohammadi et al.* in 2014. They were claimed that their protocol is secure against various attacks. However we showed that their protocol has some weaknesses that makes it vulnerable against secret parameters reveal, tag impersonation, data desynchronization attacks and also it cannot provide user privacy. All privacy analysis presented based on a formal RFID privacy model that proposed by *Ouafi* and *Phan*. Moreover, we proposed an improved version of *Mohammadi et al.*'s protocol that eliminates all existing weaknesses. Security analysis illustrated that the proposed protocol is secure against different attacks and it can provide secure and confidential communication for RFID users.

References

[1] E.-C. Australia, "Access control, sensor control, and trans-ponders," Available on: http://www.rfid.com.au/rfid uhf.htm, 2008.

[2] "Transport for London, Oyster," Available on: http://www.tfl.gov.uk/tickets/27298.aspx. [Accessed 01 02 2014].

[3] G. Avoine, "Cryptography in Radio Frequency Identification and Fair Exchange Protocols", PHD thesis, Swiss Federal Institute of Technology, Switzerland, 2005.

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

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

[6] G. D. Vecchia and M. Esposito, "A Knowledge-Based Approach for Detecting Misuses in RFID Systems, Designing and Deploying RFID Applications, Available on: http://www.intechopen.com/books/designing-and-deploying-rfid-applications/a-knowledge-based-approach-for-detecting-misuses-in-rfid-systems.

[7] 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.

[8] 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.

[9] B. Song and C. J. Mitchell, "Scalable RFID security protocols supporting tag ownership transfer," *Computer Communications*, vol. 34, pp. 556-566, 2011.

[10] M. Asadpour, and M. T. Dashti, "A privacy-friendly RFID protocol using reusable anonymous tickets," in *10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha , 2011.

[11] M. H. Dehkordi, and Y. Farzaneh, "Improvement of the hash-based RFID mutual authentication protocol," *Wireless Personal Communications*, vol. 75, no. 1, pp. 219-232, 2014.

[12] Z. Sohrabi-Bonab, M. Alagheband, and M. R. Aref, "Traceability analysis of quadratic residue-based RFID authentication protocols," in *11th Annual International Conference on Privacy, Security and Trust (PST)*, Tarragona, 2013.

[13] M. Mohammadi, M. Hosseinzadeh and M. Esmaeildoust, "Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard," *Advances in Computer Science: an International Journal (ACSIJ)* , vol. 3, no. 2, pp. 10-16, 2014.

[14] M. H. Habibi and M. Gardeshi, "Cryptanalysis and improvement on a new RFID mutual authentication protocol compatible with EPC standard," in *8th International ISC Conference on Information Security and Cryptology (ISCISC)*, pp. 49-54, 2011.

[15] 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.

[16] "EPCglobal Inc.," Available: http://www.epcglobalinc.org. [Accessed 02 01 2014].

[17] J. Zhang, W. Wang, J. Ma, and X. Li, "A novel authentication protocol suitable to EPC Class 1 Generation 2 RFID system," *Journal of Convergence Information Technology(JCIT)*, vol. 7, no. 3, pp. 259-266, 2012.

[18] N. Bagheri, M. Safkhani and M. Naderi, "Cryptanalysis of a new EPC class-1 generation-2 standard compliant RFID protocol," *Neural Computing and Applications*, vol. 24, no. 3-4, pp. 799-805, 2014.

[19] 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.

[20] A. Juels, and S. Weis, "Defining strong privacy for RFID," in *5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, 2007.

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

[22] 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.

[23] 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.