Traceability Improvements of a New RFID Protocol Based On EPC C1 G2

Seyed Salman Sajjadi GhaemMaghami[1], Afrooz Haghbin[2], Mahtab Mimohseni[3]

[1] Department of Computer Engineering, Science and Research branch,
Islamic Azad University,
Tehran, Iran
Salman.ghaemmaghami@srbiau.ac.ir

[2] Department of Computer Engineering, Science and Research branch,
Islamic Azad University,
Tehran, Iran
haghbin@srbiau.ac.ir

[3] Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
mirmohseni@sharif.edu

Abstract

Radio Frequency Identification (RFID) applications have spread all over the world and, in order to provide their security and privacy, researchers proposed different kind of protocols. In this paper, we analyzes the privacy of a new protocol, proposed by Yu-Jehn in 2015 which is based on Electronic Product Code Class1 Generation 2 (EPC C1 G2) standard. By applying the Ouafi-Phan privacy model, we show that the Yu-Jehn protocol is vulnerable against traceability attack and forward traceability attack and it does not provide the privacy of RFID users. Then, to enhance the privacy of the analyzed protocol, an improved version of the protocol is proposed which eliminates the existing weaknesses of Yu-Jehn protocol.

Keywords: *RFID authentication protocols,* Yu-Jehn *protocol, Privacy, Traceability Attack, Forward Traceability Attack.*

1. Introduction

Radio Frequency Identification (RFID) technology is a pioneer of great change in social life which has been started in recent decades and is developing increasingly in different kinds of services all around the world [1, 2, 3]. Transportation, healthcare, medical applications, trading, human or animal identification, security services are some examples which improve their facilities by using the RFID technologies. RFID systems consist of three main parts as shown in Fig. 1: Tag, Reader and Back end server. The identification data for interaction with the Reader are stored in the Tag. The Back-end server contains a complete database of identification information of all the Tags and the Readers and the Reader is placed between the Tag and the Back-end server. Depending on the protocol of any RFID system, Readers are permitted to change or add some input to the received data from the Tag (Back-end server) and forward it to the Back-end server (Tag). The connection between the Tag and the Reader is insecure while the connection between the Reader and the Back-end server is mostly secure. However, in some applications, Reader is merged with the Back-end server and the new structure consist of two main parts, the Tag and the Back-end server.

Depending on the power of RFID tags, they are falling in one of the three categories: active, passive and semi-passive [4]. The active Tag has an inner battery which enables it to start a new conversation with the Reader or the Back-end server. On the other hand, the passive tag does not have any battery and obtains its required energy for calculations and responding by using the Reader's electrical field. The semi-passive tag has a battery, but it uses this battery just for the internal processing while for wireless communications it is like the passive Tag.

In the last few years, researchers have proposed different RFID authentication protocols to provide security and privacy requirements of RFID end-users. According to the structure of the protocols and deployed cryptographic functions in them, these protocols can be classified into four main groups [5]. The first class, called full-fledged, contains the protocols that apply ordinary cryptographic functions,

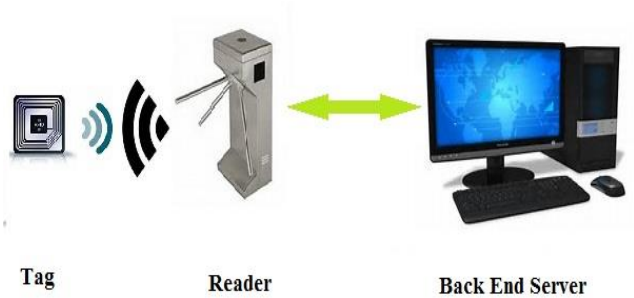

Fig. 1. A System model of RFID systems

such as one-way hash functions, public or private key cryptography systems, and so forth [6]. The second class contains the protocols that use Random Number Generators (RNG) and one-way hash functions [7]. Lightweight is the name of the third class that is relevant to those protocols which apply RNG and Cyclic Redundancy Code (CRC) checksum [8]. And the last class are the Ultra Lightweight protocols which are only allowed to use simple bitwise operators such as XOR, AND, OR and it means that they are not even permitted for using RNG in the Tag's side [1, 9].

In the last few years, due to ubiquitously deployment of RFID systems in some sensitive applications, studying the security and the privacy of RFID end-users has got more attention by researchers [2, 10-14]. Electronic Product Code Class 1 Generation 2 (EPC C1 G2) [15] is the most popular standard which has been proposed for RFID passive tags. Recently, due to popularity and implementing of RFID EPC-based tags in wide range of identification and authentication applications, designing authentication protocols under EPC C1 G2 standard has become a primary research areas for researchers in RFID protocols [16-19].

In 2007, Chien and Chen [20] proposed an improved mutual authentication protocol for RFID systems that is related to the standard of EPC C1 G2. Peris-Lopez et al. in [21] show that Chien and Chen's scheme cannot resist against the tracking, forged-server, DoS, forged-tag, and forward secrecy attacks. In 2012, Yu-Jehn [1] studied Chien and Chen's protocol and proposed a new mutual authentication protocol for EPC C1 G2 RFID tags. This protocol uses only ultra-lightweight operations, such as RNG, PRNG and XOR. In [1], the security and the privacy of the protocol are analyzed and it is claimed that the protocol is immune against existing security and privacy attacks.

In this paper, we study the privacy of Yu-Jehn protocol [1] and show that their protocol still suffers from some weaknesses and cannot provide private communication for RFID users. One of the main points in designing an RFID protocol is defining a new and randomized quantity as the secret values, which will be impossible for the attacker to guess them even by eavesdropping the protocol, moreover there must be the least likeliness between the transmitted messages and the updating procedure to prevent an adversary from understanding the next ID or secret values. But Yu-Jehn [1] miss these note in scheming of their proposed protocol, so it makes the attacker to trace the position of the Tag which is in contravention of the Privacy Performance in the protocol design. In this paper we mention to these weakness by performing two different traceability attacks and a forward traceability attack against their protocol. Moreover, in order to enhance the privacy of Yu-Jehn protocol, by paying attention to the stated notes, an improved version of their protocol is proposed.

The structure of paper is organized as follows: privacy model of Ouafi and Phan is described in section 2. Section 3 introduces the Yu-Jehn protocol. In section 4, Yu-Jehn protocol is analyzed from the privacy point of view. In section 5, we apply some changes to Yu-Jehn protocol and propose an improved version of it. Moreover, the privacy of our proposed protocol is analyzed in this section, and it is shown that the weaknesses of Yu-Jehn protocol are fixed. Finally, we conclude the paper in section 6.

2. Ouafi and Phan Privacy model

The researchers have proposed a number of privacy models to evaluate the privacy of the RFID protocols. Here, we briefly describe Ouafi and Phan privacy model [22] since we analyze the privacy of Yu-Jehn protocol using this model. In this model, the adversary $\mathcal{A}$ is able to both eavesdrop the communication channel between Tags and Readers, and change the protocol's flows actively or passively. Actually the adversary $\mathcal{A}$ can run the following queries:

■ ***Execute query (R, T, i):*** This query models passive attacks. Its output involves the messages that were exchanged between Reader *R* and Tag *T* during a truthful execution of the protocol in the session *i*.

■ ***Send query (U, V, m, i):*** In this query, an adversary $\mathcal{A}$ is able to perform an active attack. In the other words, the attacker impersonate an entity such as $U \in T$ in the ith session of the protocol by sending a message (m) to an entity $V \in R$.

■ ***Corrupt query (T, K):*** In corrupt query, the adversary $\mathcal{A}$ has physical access to the Tag *T*, so it becomes as a stronger query than send. With this query, the adversary $\mathcal{A}$ learns the stored secret K_0 of *T*, and sets it to *K*. This query is used to capture the notion of forward and backward traceability and the extent of the damage caused by compromising tag's stored secret.

■ ***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 $T_b \in \{T_0, T_1\}$ is delivered to the attacker. Adversary wins if it can truly guess the bit b.

***Untraceability (UPriv)*:** The adversary plays the game G and gathers *R* and *T* instances by implementing the mentioned queries in the following phases:

:: ***Learning phase:*** The adversary $\mathcal{A}$ can drive the Execute, Send, and Corrupt queries to any random T_0 and T_1 tags.

:: ***Challenge phase:*** The attacker $\mathcal{A}$ selects two fresh tags T_0 and 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 attacker$\mathcal{A}$ expresses a tag $T_b \in \{T_0, T_1\}$ using Execute and Send queries.

:: ***Guess phase:*** The adversary $\mathcal{A}$ terminates the game and outputs a bit b', which is its guess of the value of b.

Back-end Server 	***Reader*** 	***Tag*** 
$(N_{old}, N_{new}, K_{old}, K_{new}, PID_{old}, PID_{new}, EPC_i)$	(RID_j)	(N_i, K_i, EPC_i, PID_i)
	1.1 Generates r_1 1.2 $V_R = h(RID_j \oplus r_1)$ 1.3 $\xrightarrow{r_1}$	
		2.1 Generates r_2 Randomly 2.2 $M_1 = N_i \oplus r_2$ 2.3 $M_2 = P(EPC_i \parallel r_1 \parallel r_2 \parallel K_i)$
4.1 $V_R \stackrel{?}{=} h(RID_j \oplus r_1)$ 4.2 Search PID_i in the database to find out $(EPC_i, N_i^{old}, K_i^{old}, PID_i^{old}, N_i^{new}, K_i^{new}, PID_i^{new})$ 4.3 $r_2 = M_1 \oplus N_i^{old}$ or $r_2 = M_1 \oplus N_i^{new}$ 4.4 $M_2 \stackrel{?}{=} P(EPC_i \parallel r_1 \parallel r_2 \parallel K_i^{old}$ or $K_i^{new})$ 4.5 $x = old$ or new 4.6 $M_3 = P(EPC_i \parallel r_2 \parallel N_i^x \parallel K_i^x)$ 4.7 $\xrightarrow{M_3}$	3 $\xleftarrow{(M_1, M_2, PID_i, r_1, V_R)}$ 5 $\xrightarrow{M_3}$	2.4 $\xleftarrow{(M_1, M_2, PID_i)}$ 6.1 $M_3 \stackrel{?}{=} P(EPC_i \parallel r_2 \parallel N_i \parallel K_i)$ 6.2 $N_i = P(N_i \oplus r_2)$ 6.3 $K_i = P(K_i \oplus r_2)$ 6.4 $PID_i = P(PID_i \oplus r_2)$
4.8 If (x = new) $N_i^{old} = N_i^{new}$, $N_i^{new} = P(N_i^{new} \oplus r_2)$ $K_i^{old} = K_i^{new}$, $K_i^{new} = P(K_i^{new} \oplus r_2)$ $PID_i^{old} = PID_i^{new}$, $PID_i^{new} = P(PID_i^{new} \oplus r_2)$ END If		

The success of the attacker $\mathcal{A}$ in playing G is equal to its success of breaking untraceability notion which is equal to the probability of recognizing whether attacker $\mathcal{A}$ received T_0 or T_1. It can be denoted by $Adv_A^{UPiv}(K)$, where k is the security parameter:

$$Adv_A^{UPiv}(k) = |\text{pr}(\mathcal{A}\ wins) - \text{pr}(random\ coin\ flip)| = |\text{pr}(b' = b) - \frac{1}{2}| \quad (1)$$

where $0 \le Adv_A^{UPiv}(k) \le \frac{1}{2}$. If $Adv_A^{UPiv}(k) < \varepsilon(k)$, the protocol is traceable with negligible probability.

3. The Yu-Jehn Protocol

In [1], Yu-Jehn proposed a new mutual authentication protocol for EPC C1 G2 RFID tags. EPC is the new Electronic Product Code that replaces the older UPC (Universal Product Code) found on many item labels and is a set of numbers plus a bar code. The structure of Yu-Jehn protocol is illustrated in Fig. 2. The notation that are used in Yu-Jehn protocol are listed below:

$\boldsymbol{EPC_i}$: Electronic Product Code of the *i*th Tag
$\boldsymbol{K_i}$: Authentication key
$\boldsymbol{PID_i}$: The pseudonym identification code of the *i*th Tag
$\boldsymbol{RID_j}$: The pseudonym identification code of the *j*th Reader
$\boldsymbol{R_i}$: A random number
$\boldsymbol{h}(.)$: Hash function
$\boldsymbol{P}$: Pseudo Random Number Generator
$\parallel$: Concatenation operation
A $\oplus$ **B**: Message A is XORed with message B

4. Privacy Analyzes of Yu-Jehn Protocol

4.1 Traceability Attack

This subsection aims to show that Yu-Jehn protocol is vulnerable against two different kinds of traceability attacks where an adversary can trace a specific tag as follows,

Learning phase: In the session (i) and $(i+1)$, the adversary $\mathcal{A}$ sends an $Execute\ query\ (R, T_0, i)$ and $Execute\ query\ (R, T_0, i+1)$ and gets $M_{1,i}^{T_0} = N_i^{T_0} \oplus r_{2,i}$, $PID_{i+1}^{T_0}$, $M_{1,i+1}^{T_0}$. Then he/she calculates $\lambda = P(M_{1,i}^{T_0}) = P(N_i^{T_0} \oplus r_{2,i})$ and $\gamma = M_{1,i+1}^{T_0} \oplus \lambda$.

Challenge phase: The adversary $\mathcal{A}$ selects two fresh tags T_0 and T_1 for test, and sends a $Test\ query(T_0, T_1, i+2)$. According to the randomly chosen bit $b \in \{0, 1\}$, the adversary is given a tag $T_b \in \{T_0, T_1\}$. Afterwards, the adversary $\mathcal{A}$ sends an $Execute\ query(R, T_b, i+2)$, and obtains

$PID_{i+2}^{T_b}$.

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

$$b' = \begin{cases} 0 & if\ PID_{i+2}^{T_b} = PRNG\left(PID_{i+1}^{T_0} \oplus \gamma\right) \\ 1 & otherwise \end{cases} \quad (2)$$

As a result, we have:

$$Adv_A^{upriv}(k) = |pr(b' = b) - pr(random\ coin\ flip)|$$
$$= \left|pr(b' = b) - \frac{1}{2}\right| = \left|1 - \frac{1}{2}\right| = \frac{1}{2} \gg \varepsilon \quad (3)$$

Proof: According to the Fig. 2 we can write,

$$If\ \ T_b = T_0:$$
$$P\left(PID_{i+1}^{T_0} \oplus \gamma\right) = P\left(PID_{i+1}^{T_0} \oplus M_{1,i+1}^{T_0} \oplus \lambda\right)$$
$$= P\left(PID_{i+1}^{T_0} \oplus M_{1,i+1}^{T_0} \oplus P\left(N_i^{T_0} \oplus r_{2,i}\right)\right)$$
$$= P\left(PID_{i+1}^{T_0} \oplus M_{1,i+1}^{T_0} \oplus N_{i+1}^{T_0}\right)$$
$$= P\left(PID_{i+1}^{T_b} \oplus M_{1,i+1}^{T_b} \oplus N_{i+1}^{T_b}\right)$$
$$= P\left(PID_{i+1}^{T_b} \oplus r_{2,i+1}\right) = PID_{i+2}^{T_b} \quad (4)$$

Hence, $Adv_A^{upriv}(k) = \frac{1}{2} \gg \varepsilon$ and the Tag is traceable. Note that the notion Adv_A^{upriv} is defined in [22].

Moreover, the Yu-Jehn protocol is again vulnerable against traceability attack too. According to the structure of Yu-Jehn protocol, it can be seen that the PID_i will not be updated till session (5) of the protocol. So an adversary can perform traceability attack by preventing the PID_i update in the Tag using one time interception of protocol. This attack can be performed as follows:

Learning phase: In session (*i*), the attacker $\mathcal{A}$ sends an $Execute\ query(R, T_0, i)$ to the Tag by sending a random number, r_1', and obtains M_1', M_2', PID_i'.

Challenge phase: The attacker $\mathcal{A}$ selects two fresh tags T_0 and T_1 for the test, and sends a $Test\ query(T_0, T_1, i+1)$. 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, the attacker $\mathcal{A}$ sends an $Execute\ query(R, T_b, i+1)$ by sending r_1'', and obtains M_1'', M_2'', PID_i''.

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

$$b' = \begin{cases} 0 & if\ PID_i' = PID_i'' \\ 1 & otherwise \end{cases} \quad (5)$$

As a result, we get:

$$Adv_A^{upriv}(k) = |pr(b' = b) - pr(random\ coin\ flip)|$$
$$= \left|pr(b' = b) - \frac{1}{2}\right| = \left|1 - \frac{1}{2}\right| = \frac{1}{2} \gg \varepsilon \quad (6)$$

Proof: After an unsuccessful challenge between the attacker and the tag, the tag does not update PID_i. Hence, the tag uses the same value in the next session.

4.2 Forward traceability Attack

In addition to the mentioned privacy disquiets, it can be shown that Yu-Jehn protocol does not assure forward traceability. According to the structure of Yu-Jehn protocol, the EPC is fixed in all sessions. Because of this weakness, an adversary can track a target tag as follows:

Learning phase: In the *i*th session, the adversary $\mathcal{A}$ sends a $Corrupt\ query(T_0, K')$ and obtains $\left(K_i^{T_0}, N_i^{T_0}, EPC_i^{T_0}\right)$ from Tag T_0. It also sends an $Execute\ query(R, T_0, i)$ and obtains $\left(r_{1,i}, M_{1,i}^{T_0}\right)$. Now, simply the adversary computes $r_{2,i}$ as $r_{2,i} = M_{1,i}^{T_0} \oplus N_i^{T_0}$. Afterward using the obtained $r_{2,i}$, the adversary computes A and B as follows:

$$A = P\left(N_i^{T_0} \oplus r_{2,i}\right), B = P\left(K_i^{T_0} \oplus r_{2,i}\right) \quad (7)$$

Challenge phase: The adversary $\mathcal{A}$ selects two fresh tags T_0 and T_1 for the test, and sends a $Test\ query(T_0, T_1, i+1)$. According to the randomly chosen bit $b \epsilon \{0,1\}$, the adversary is given a tag $T_b \epsilon \{T_0, T_1\}$. Now in session $(i+1)$ th, the adversary $\mathcal{A}$ sends an $Execute\ query(R, T_b, i+1)$ by sending $r_{1,i}$ (i.e., the same value as for session i) and obtains $\left(M_{1,i+1}^{T_b}, M_{2,i+1}^{T_b}\right)$. Now the adversary computes $r_{2,i+1}$ as $r_{2,i+1} = M_{1,i+1}^{T_b} \oplus A$.

Guess phase: The adversary $\mathcal{A}$ stops the game G, and outputs a bit $b' \epsilon \{0,1\}$ as a guess of bit b using the following rule:

$$b' = \begin{cases} 0 & if\ \ M_{2,i+1}^{T_b} = P\left(EPC_i^{T_0} \parallel r_{1,i} \parallel r_{2,i+1} \parallel B\right) \\ 1 & otherwise \end{cases} \quad (8)$$

As a result, it can be written that,

$$Adv_A^{upriv}(k) = |pr(b' = b) - pr(random\ coin\ flip)|$$
$$= \left|pr(b' = b) - \frac{1}{2}\right| = \left|1 - \frac{1}{2}\right| = \frac{1}{2} \gg \varepsilon \quad (9)$$

Proof: As the value of EPC is fixed in all sessions, we have $EPC_i^{T_0} = EPC_{i+1}^{T_0}$. Using this fact, the following equations is obtained:

$$(1)\ If\ \ T_b = T_0: \quad N_{i+1}^{T_b} = P\left(N_i^{T_b} \oplus r_{2,i}\right)$$
$$= P\left(N_i^{T_0} \oplus r_{2,i}\right) = A$$
$$(2)\ If\ T_b = T_0: \quad K_{i+1}^{T_b} = P\left(K_i^{T_b} \oplus r_{2,i}\right)$$
$$= P\left(K_i^{T_0} \oplus r_{2,i}\right) = B$$
$$(1), (2) => M_{2,i+1}^{T_b} = P\left(EPC_i^{T_b} \parallel r_{1,i} \parallel r_{2,i+1} \parallel K_{i+1}^{T_b}\right)$$

Back-end Server 	***Reader*** 	***Tag*** 
$(N_{old}, N_{new}, K_{old}, K_{new}, PID_{old}, PID_{new}, EPC_i, RID)$	(RID_j)	(N_i, K_i, EPC_i, PID_i)
	1.1 Generates r_1 1.2 $V_R = h(RID_j \oplus r_1)$ 1.3 $\xrightarrow{r_1}$	
		2.1 Generates r_2 and r_3 Randomly 2.2 $M_1 = P(N_i \oplus r_3) \oplus r_2$ 2.3 $M_2 = P(EPC_i \parallel r_1 \parallel r_2 \parallel K_i)$ 2.4 $PID_{add} = PID_i \oplus r_3$ 2.5 $\xleftarrow{(M_1, M_2, PID_{add})}$
	3 $\xleftarrow{(M_1, M_2, PID_{add}, r_1, V_R)}$	
4.1 $V_R \stackrel{?}{=} h(RID_j \oplus r_1)$ 4.2 *For each tuple* (PID_{old}, PID_{new}) 4.3 $r_3^{old} = PID_{\text{add}} \oplus PID_{old}$ $r_3^{new} = PID_{\text{add}} \oplus PID_{\text{new}}$ 4.4 $r_2^{old} = r_2^{old} = M_1 \oplus P(r_3^{old} \oplus N_i^{old})$ $r_2^{new} = M_1 \oplus P(r_3^{new} \oplus N_i^{new})$ 4.5 $M_2 \stackrel{?}{=} P(EPC_i \parallel r_1 \parallel r_2^x \parallel K_i^x)$ 4.6 $x = old$ or new 4.7 $M_3 = P(EPC_i \parallel r_2 \parallel N_i^x \parallel K_i^x)$ 4.8 $\xrightarrow{M_3}$ 4.9 If (x = new) $N_i^{old} = N_i^{new}$, $N_i^{new} = P(N_i^{new} \oplus r_2 \oplus r_3)$ $K_i^{old} = K_i^{new}$, $K_i^{new} = P(K_i^{new} \oplus r_2 \oplus r_3)$ $PID_i^{old} = PID_i^{new}$, $PID_i^{new} = P(PID_i^{new} \oplus r_2)$ END If	5 $\xrightarrow{M_3}$	6.1 $M_3 \stackrel{?}{=} P(EPC_i \parallel r_2 \parallel N_i \parallel K_i)$ 6.2 $N_i = P(N_i \oplus r_2 \oplus r_3)$ 6.3 $K_i = P(K_i \oplus r_2 \oplus r_3)$ 6.4 $PID_i = P(PID_i \oplus r_2)$

$$= P\left(EPC_i^{T_0} \parallel r_{1,i} \parallel r_{2,i+1} \parallel K_{i+1}^{T_0}\right)$$

$$= P\left(EPC_i^{T_0} \parallel r_{1,i} \parallel r_{2,i+1} \parallel B\right) \quad (10)$$

5. Improved Version of Yu-Jehn Protocol

In this section, in order to eliminate the privacy weaknesses of Yu-Jehn protocol mentioned in section 4, an improved version is proposed. Analyzes illustrates that our proposed protocol is resistant against all of the mentioned traceability attacks. Yu-Jehn protocol has two main weaknesses that make it vulnerable to traceability attacks. The first one is the structure of generating $M_1 = N_i \oplus r_2$. Because, using this way of generation, if the adversary obtains N_i, upon eavesdropping M_1, he/she can calculate the random number r_2 and perform traceability and forward traceability attacks. The second one is the way PID_i is used in the updating procedure, which makes the protocol vulnerable to traceability attack.

Now, in order to prevent all mentioned weaknesses in the Yu-Jehn protocol, we apply some changes in its authentication and updating procedures. First, we change the computation of M_1 and the transmitted PID_i as follows:

$$M_1 = P(N_i \oplus r_3) \oplus r_2, PID_{add} = PID_i \oplus r_3 \quad (11)$$

where we define a new random number r_3 which is generated in the tag. Furthermore, we change updating of N_i and K_i as follows,

$$N_{i+1} = P(N_i \oplus r_2 \oplus r_3), K_{i+1} = P(K_i \oplus r_2 \oplus r_3) \quad (12)$$

The improved protocol is shown in Fig. 3 in details. In the improved protocol, to avoid traceability attack, we prevent sending PID_i explicitly and change it with PID_{add} which

Table 1. COMPARISON OF PRIVACY ANALYZES

Protocols → / Attacks ↓	Chien&Chen [20]	Yu-Jehn [1]	Improved Yu-Jehn
Forward Traceability	✓	✘	✓
Backward Traceability	✘	✘	✓
Traceability	✘	✘	✓

✓: Secure ✘: Insecure

the amount of computation in the Back-end server side, but the presence of powerful processor in Back-end server will make this issue ignorable [4-5]. In the rest of this subsection, the privacy of improved Yu-Jehn protocol is analyzed against different privacy attacks. It is shown that how our modification on the Yu-Jehn protocol can fix all mentioned weaknesses and increase its privacy.

Traceability Attack: In Section 4.1, it is shown that the adversary can trace the tag via two different methods. In our proposed protocol, in order to prevent these two, we make two changes in the exchanged messages between the Tag and the Reader. First, we change transmitted PID_i from the Tag to the Reader with $PID_{add} = PID_i \oplus r_3$, where r_3 is a random number that is generated by the tag in each session. Therefore, since in each session the value of PID_{add} changes, even if the adversary intercepts the protocol, he/she cannot trace the tag using PID_i. Also in order to prevent the second attack, we change generating $M_1 = N_i \oplus r_2$ into $M_1 = PRNG(N_i \oplus r_3) \oplus r_2$. As a result, the adversary cannot obtain N_i and r_2 and consequently he/she cannot calculate the value of PID_{i+1} to trace the tag.

Backward and Forward Traceability Attacks: In the proposed protocol, in order to prevent backward traceability and forward traceability attacks, we change updating procedure of $N_{i+1} = P(N_i \oplus r_2)$ into $N_{i+1} = P(N_i \oplus r_2 \oplus r_3)$ and $K_{i+1} = P(K_i \oplus r_2)$ into $K_{i+1} = P(K_i \oplus r_2 \oplus r_3)$. Since the values of r_2 and r_3 are generated in each session, thus the adversary cannot trace the target tag even if he/she corrupts the tag and obtains the secret key K_i, N_i, and EPC_i.

The privacy of our proposed protocol is compared with the analyzed protocol and Chien and Chen's protocol in Table 2. As it can be seen, our proposed protocols can provide user privacy.

6. Conclusion

In this paper, we analyzed the privacy of a recently proposed RFID authentication protocol under the standard of EPC C1G2 by Yu-Jehn in 2015. We showed that Yu-Jehn protocol does not provide privacy immunity and it is susceptible to different traceability attacks such as forward traceability attack and traceability attack. Then, in order to improve the performance of the analyzed protocol, an improved version is proposed that eliminates the mentioned attacks.

References

[1] Yu-C. Huang, and Jehn-R. Jiang, "Ultralightweight RFID Reader-Tag Mutual Authentication Revisted," *in Proc. of IEEE Mobile Services Conference (IEEE MS 2015)*, 2015.

[2] D. He, 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, pp. 72-83, 2015.

[3] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381 - 394, 2006.

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

[5] H.-Y. Chien, "SASI: a newultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, pp. 337–340, 2007.

[6] B. Abdolmaleki, K. Baghery, B. Akhbari, and M. R. Aref, "Attacks and improvements on two new-found RFID authentication protocols," *in 7th International Symposium on Telecommunications (IST), Tehran*, 2014.

[7] 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, pp. 51-56, 2014.

[8] 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.

[9] Y. C. Lee, "Two Ultralightweight Authentication Protocols for Low-Cost RFID Tags," *Applied Mathematics & Information Sciences*, pp. 425-431, 2012.

[10] S. Abdolmaleky, S. Atapoor, M. Hajighasemlou and H. Sharini, "A Strengthened Version of a Hash-based RFID Server-less Security Scheme," *Advances in Computer Science: an International Journal*, vol. 4, pp. 18-23, 2015.

[11] M. Mohammadi, M. Hosseinzadeh and M. Esmaeildoust, "Analysis and improvement of the lightweight mutual authentication protocol under EPC

C-1 G-2 standard," *Journal of Advances in Computer Science (ACSIJ)*, vol. 3, pp. 10-16, 2014.

[12]S.M. Alavi, K. Baghery, B. Abdolmaleki, and M. R. Aref, "Traceability analysis of recent RFID authentication protocols," *Wireless Personal Communications*, pp. 1-20, 2015.

[13]M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, J. C Hernandez-Castro, "Weaknesses in another Gen2-based RFID authentication protocol," *in IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, 2012.

[14]U. Mujahid, M. Islam, M. A. Shami, "RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash," *International Journal of Distributed Sensor Networks*, vol. Volume 2015, Article ID 642180, 8 pages, 2015.

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

[16]K. Baghery, B. Abdolmaleki, B. Akhbari, M.R. Aref, "Untraceable RFID authentication protocols for EPC compliant tags," *in 23rd Iranian Conference on Electrical Engineering (ICEE)*, pp. 426-431, 2015.

[17]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, pp. 799-805, 2014.

[18]H. Martin, E. Millan, P. Peris-Lopez, and J. E. Tapiador, "Efficient ASIC implementation and analysis of two EPC-C1G2 RFID authentication protocols," *Sensors Journal, IEEE*, vol. 13, pp. 3537-3547, 2013.

[19]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, pp. 605-612, 2013.

[20]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, pp. 254-259, 2007.

[21]P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, "Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard," *Computer Standards & Interfaces*, vol. 31, pp. 372-380, 2009.

[22]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.