The ISC Int'l Journal of
Information Security
ISeCure

July 2016, Volume 8, Number 2 (pp. 105–114)
http://www.isecure-journal.org

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

Seyed Salman Sajjadi Ghaemmaghami [1,*], Afrooz Haghbin [1], and Mahtab Mirmohseni [2]
[1] *Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*
[2] *Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 11 January 2016
Revised: 7 June 2016
Accepted: 27 June 2016
Published Online: 15 July 2016

Keywords:
RFID Authentication Protocols,
Privacy, Traceability Attack,
Forward Traceability Attack,
Ouafi-Phan Privacy Model.

ABSTRACT

Radio Frequency Identification (RFID) applications have spread all over the world. In order to provide their security and privacy, researchers proposed different kinds of protocols. In this paper, we analyze 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 to secret parameter reveal attack, traceability attacks, forward traceability attack and it also does not provide the privacy of RFID users. 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.

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 [1–3]. 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 Figure 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. The reader is placed between the tag and the back-end server. Depending on the protocol,readers are allowed 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 [3, 5–9]. According to the structure of the protocols and their deployed cryptographic func-

---

[*] Corresponding author.

Email addresses: `salman.ghaemmaghami@srbiau.ac.ir` (S.S. Sajjadi GhaemMaghami), `no`(A. Haghbin), `no` (M. Mirmohseni)

ISSN: 2008-2045 © 2016 ISC. All rights reserved.

tions, these protocols are classified into four main groups [10]. The first class, called full-fledged, contains the protocols that apply ordinary cryptographic functions, such as one-way hash functions, public or private key cryptography systems, and so forth [11]. The second class contains the protocols that use Random Number Generators (RNG) and one-way hash functions. Lightweight is the name of the third class that is relevant to those protocols which apply RNG and Cyclic Redundancy Code (CRC) checksum [12, 13]. The last class are the Ultra Lightweight protocols which are only allowed to use simple bitwise operators such as OR, AND, XOR and it means that they are not even permitted for using RNG on the tag's side [14, 15].

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 [1, 6, 16–19]. Electronic Product Code Class 1 Generation 2 (EPC C1 G2) [20] 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 [3, 5, 14, 21–25].

In 2007, Chien and Chen [26] proposed an improved mutual authentication protocol for RFID systems that is related to the standard of EPC C1 G2. Peris-Lopez *et al.* in [27] showed that Chien and Chen's scheme cannot resist against the tracking, forged-server, DoS, forged tag, and forward secrecy attacks. In 2010, Yeh *et al.* [23] investigated the Chien and Chen's protocol and showed that it is vulnerable against DOS attack. Moreover, they improved it and proposed a new protocol based on EPC C1 G2 standard. They claimed that their protocol provides sufficient security and privacy. However, in 2013, Yoon *et al.* [22] declared that there are still weaknesses with Yeh *et al.* protocol [23] in providing data integrity and secrecy. In 2015, Yu-Jehn [14] studied Chien and Chen's protocol and proposed a new mutual authentication protocol for EPC C1 G2 RFID tags. This protocol only used ultra-lightweight operations, such as RNG, PRNG and XOR. In [14], the security and the privacy of the proposed protocol are analyzed and it is claimed that the protocol is immune against existing security and privacy attacks.

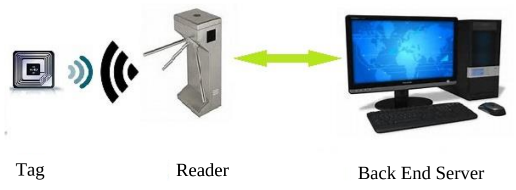


Figure 1. A System model of RFID systems

In this paper, we study the privacy of Yu-Jehn protocol [14] 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. Yu-Jehn [14] missed these notes in designing their their protocol, hence it is possible for 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 these weaknesses by performing two different traceability attacks, forward traceability attack and secret parameter reveal 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: in Section 2, privacy concerns in RFID protocol are highlighted and the model of *Ouafi* and *Phan* is described. 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 Privacy in RFID Protocol

Providing privacy in an RFID system is the main goal of protocol proposers. These protocols are always at risk of different types of attacks and threats.

2.1 Traceability

Traceability issue is one of the greatest challenges in every authentication protocol which plays an important role in providing the privacy of RFID users. Traceability topic from the perspective of privacy is categorized in one of the following three section [28]:

Untraceability: It means that, after the transaction between the tag T_0 and the reader at the moment t, there should not be any relation between the messages created at time t', $t' > t$, with the stored values in the last session.

Forward untraceability: If an adversary $\mathcal{A}$ has

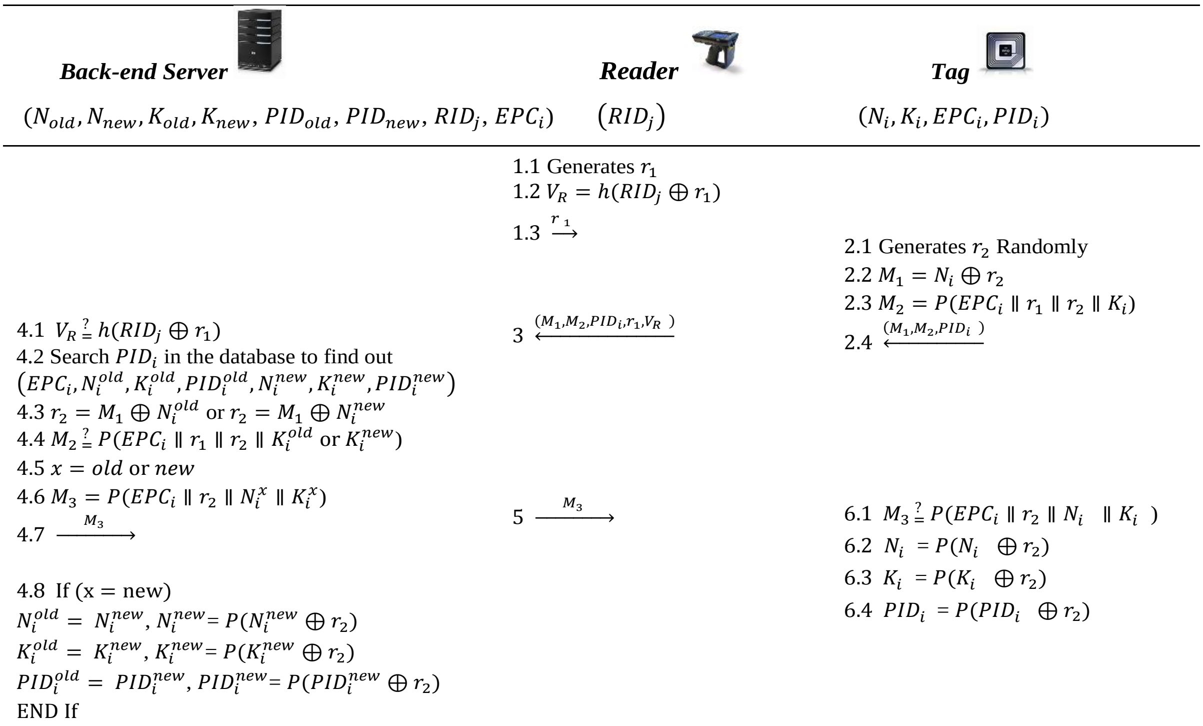


Figure 2. The Yu-Jehn Protocol [14]

access to the secret values of the tag T_0 at t, he/she will not be able to recognize the messages produced by the tag T_0 at the time t'', when $t'' > t'$, after a successful session between the tag T_0 and the reader at time t', with $t' > t$.

Backward untraceability: If the attacker has access to the secret values of the tag T_0 at time t', he/she will not be able to distinguish the transactions of the tag T_0 at time t'' with $t'' < t'$.

2.2 Ouafi and Phan Privacy model

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 [28] 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 i^{th} 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 privacy (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. 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 $Adv_A{}^{UPriv}\ (k)$, where k is the security parameter.

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{UPriv}}(\kappa) = |\,\Pr[b' = b] - \frac{1}{2}|\ .$$

where $0 \leq Adv_{\mathcal{A}}^{UPriv}(k) \leq \frac{1}{2}$. if$Adv_{\mathcal{A}}^{UPriv}(k) \ll \varepsilon(k)$, the protocol is traceable with negligible probability.

3 The Yu-Jehn Protocol

In [14], *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 barcode [3]. The structure of Yu-Jehn protocol is illustrated in Figure 2. It should be noted that the connection between the tag and the reader is insecure, while the back-end server and the reader communicate in a secure connection. The notation that are used in Yu-Jehn protocol are listed in Table 1.

Table 1. The notation that are used in Yu-Jehn protocol.

Symbol	Definition
EPC_i	Electronic Product Code of the i^{th} tag
K_i	Authentication key
PID_i	Pseudonym identification code of the i^{th} tag
$PID_i^{T_k}$	PID of the k^{th} tag during the i^{th} session
RID_j	Pseudonym identification code of the j^{th} reader
r_i	A random number
N_i	Secret parameter updated at the end of each round. For the first time it is pre-defined in the tag and the back-end server
$M_{l,i}^{T_k}$	The l^{th} message generated by the k^{th} tag during the i^{th} session
x	Shows that the received messages are the old or new ones which are stored in the back-end server
$h(\cdot)$	Hash function
$P(\cdot)$	Pseudo Random Number Generator
$\parallel$	Concatenation operation
$\oplus$	Bitwise XOR

3.1 Review of Yu-Jehn RFID Tag Authentication Protocol

The Yu-Jehn protocol is organized in six phases which are described as follows:

In the first phase, the reader generates a random number r_1 and sends a request query through transmission of r_1 to the tag. Besides, the reader computes $V_R = h(RID_j \oplus r_1)$ in this session. In the second phase, the tag generates a random number r_2 after receiving the request from the reader. Moreover, it computes $M_1 = N_i \oplus r_2$ and $M_2 = P(EPC_i \parallel r_1 \parallel r_2 \parallel k_i)$ messages and sends (M_1, M_2, PID_i) to the reader. The reader puts r_2 and V_R beside the received messages and sends $(M_1, M_2, PID_i, r_1, V_R)$ to the back-end server in the third phase. In the fourth phase, the back-end server validates the reader as a legal one, by calculating $V_R = h(RID_j \oplus r_1)$ and comparing it with the received V_R. Considering the stored PID_i is in the database, the back-end server compares them with the received PID_i to obtain the appropriate set of $(EPC_i, N_i^{old}, k_i^{old}, PID_i^{old}, N_i^{new}, , k_i^{new}, PID_i^{new})$. As the back-end server stores the last two k_i, PID_i and N_i, it computes r_2 with both $M_1 \oplus N_i^{old}$ and $M_1 \oplus N_i^{new}$ equations. Implementing results for r_2 and the stored values of k_i^{new} and k_i^{old}, the back-end server computes M_2 which result in four values. Comparing these four values with the received message M_2, clarifies that the transmitted messages of the tag are the old or new ones (it is referred by x in this paper). After choosing the correct tag, the back-end server computes $M_3 = P(EPC_i \parallel r_2 \parallel N_i^x \parallel K_i^x)$ and sends it to the reader. Now, if the transmitted messages of the tag are the new ones, it will update its stored values. The reader sends the received M_3 to the tag, in the fifth phase. In the last phase, the tag computes $P(EPC_i \parallel r_2 \parallel N_i \parallel K_i)$ and compares it with the received M_3. If they are equal, the authentication process is performed successfully. Finally, the tag updates its stored values.

4 Analysis of Yu-Jehn Protocol

4.1 Secret Parameter Reveal

Protocols should provide private communication besides preventing from reveal of secret parameters implemented in their structure. Although, Yu-Jehn protocol [14] assures the immunity of secret parameters, we find their protocol vulnerable to secrecy attack which is described below,

Learning phase: In sessions (i) the adversary $\mathcal{A}$ sends an Execute query (R, T_0, j) to the tag T_0 and receives $M_{1,i}^{T_0}$, $PID_i^{T_0}$, $M_{2,i}^{T_0}$.

Attack phase: The attacker sends an Execute query $(R, T_0, i+1)$ in the $(i+1)$th session of the protocol which results in obtaining $M_{1,i+1}^{T_0}, PID_{i+1}^{T_0}, M_{2,i+1}^{T_0}$. Now, the attacker finds the secret value N_{i+1} with the probability of "1", through usage of stored values during the last session: $N_{i+1} = P(N_i \oplus r_{2,i}) = P(M_{1,i})$. Therefore, it is shown that the Yu-Jehn protocol reveals the secret parameter N_{i+1}, after eavesdropping one session of the protocol which leads to the other privacy and security attacks.

4.2 Traceability Attack

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

Learning phase: In the sessions (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 $b' \in \{0,1\}$ as a guess of bit b as follows,

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

As a result, we have, $ADV_{\mathcal{A}}^{uprive}(k) = |pr(b' = b) - \frac{1}{2}| = |1 - \frac{1}{2}| = \frac{1}{2} \gg \varepsilon$

Proof: According to the Figure 2 we can write,

$$\begin{aligned} \text{If} \quad T_b = T_0 \Longrightarrow & P(PID_{i+1}^{T_0} \oplus \gamma) \\ &= P(PID_{i+1}^{T_0} \oplus M_{1,i+1}^{T_0} \oplus \lambda) \\ &= P(PID_{i+1}^{T_0} \oplus M_{1,i+1}^{T_0} \oplus P(N_i^{T_0} \oplus r_{2,i})) \\ &= P(PID_{i+1}^{T_0} \oplus M_{1,i+1}^{T_0} \oplus N_{i+1}^{T_0}) \\ &= P(PID_{i+1}^{T_b} \oplus M_{1,i+1}^{T_b} \oplus N_{i+1}^{T_b}) \\ &= P(PID_{i+1}^{T_b} \oplus r_{2,i+1}) = PID_{i+2}^{T_b} \end{aligned}$$

Hence, $ADV_{\mathcal{A}}^{uprive}(k) = \frac{1}{2} \gg \varepsilon$ and the tag is traceable. Note that, the notion $ADV_{\mathcal{A}}^{uprive}(k)$ is defined in [28]. Moreover, the Yu-Jehn protocol is again vulnerable to traceability attack. 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_i', and obtains M_1', M_2' and PID_i'.

Challenge phase: The attacker $\mathcal{A}$ selects two fresh tags T_0 and T_1 for test, and sends a Test query $(T_0, T_1, i+1)$. According to the randomly chosen bit $b \in \{0,1\}$, the attacker is given a tag $T_b \in \{T_0, T_1\}$. 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 $b' \in \{0,1\}$ as a guess of bit b as follows,

$$b' = \begin{cases} 0 & \text{if} \quad PID_i' = PID_i'' \\ 1 & \text{otherwise} \end{cases} .$$

As a result, we get:

$$ADV_{\mathcal{A}}^{uprive}(k) = |pr(b' = b) - \frac{1}{2}| = |1 - \frac{1}{2}| = \frac{1}{2} \gg \varepsilon$$

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. Therefore, the adversary can perform traceability attack on the Yu-Jehn protocol with the success probability of "1".

4.3 Forward Traceability Attack

In addition to the mentioned privacy disquiets, it can be shown that Yu-Jehn protocol does not assure forward untraceability. 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 $(K_i^{T_0}, N_i^{T_0}, EPC_i^{T_0})$ from Tag T_0. It also sends an Execute query (R, T_0, i) and obtains $(r_{1,i}^{T_0}, M_{1,i}^{T_0})$. 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 and as follows:

$$A = P(N_i^{T_0} \oplus r_{2,i})$$

$$B = P(K_i^{T_0} \oplus r_{2,i})$$

Challenge phase: The adversary $\mathcal{A}$ selects two fresh tags T_0 and T_1 for test, , and sends a Test query $(T_0, T_1, i+1)$. According to the randomly chosen bit $b \in \{0,1\}$, the adversary is given a tag $T_b \in \{T_0, T_1\}$. 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 $(M_{1,i+1}^{T_b}, M_{2,i+1}^{T_b})$. 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 $b' \in \{0,1\}$ as a guess of bit b using the following rule: bit $b' \in \{0,1\}$ as a guess of bit b as follows,

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

As a result, it can be written that,

$$ADV_{\mathcal{A}}^{uprive}(k) = |pr(b' = b) - \frac{1}{2}| = |1 - \frac{1}{2}| = \frac{1}{2} \gg \varepsilon$$

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:

$$\begin{aligned} (1)If \quad T_b = T_0 \Longrightarrow N_{i+1}^{T_b} &= P(N_i^{T_b} \oplus r_{2,i}) \\ &= P(N_i^{T_0} \oplus r_{2,i}) = A \\ &= (EPC_i^{T_0} \parallel r_{1,i} \parallel r_{2,i+1} \parallel K_{i+1}^{T_0}) \\ &= (EPC_i^{T_0} \parallel r_{1,i} \parallel r_{2,i+1} \parallel B) \end{aligned}$$

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 illustrate that our proposed protocol is resistant against all of the mentioned traceability attacks. Yu-Jehn protocol has two main weaknesses that makes it vulnerable to traceability attacks. The first one is the structure of generating $M_1 = N_i \oplus r_2$. In their protocol, if the adversary obtains N_i, upon eavesdropping M_i, 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 introduce a new definition for computation of M_1 and the transmitted PID_i as follows:

$$\begin{aligned} (2)\text{If} \quad T_b = T_0 \Longrightarrow K_{i+1}^{T_b} &= P(K_i^{T_b} \oplus r_{2,i}) \\ &= P(K_i^{T_0} \oplus r_{2,i}) = B \\ (1),(2) \Longrightarrow M_{2,i+1}^{T_b} &= P(EPC_i^{T_b} r_{1,i} \parallel r_{2,i+1} \parallel K_{i+1}^{T_b}) \\ M_1 &= P(N_i \oplus r_3) \oplus r_2 \\ PID_{add} &= PID_i \oplus r_3 \end{aligned}$$

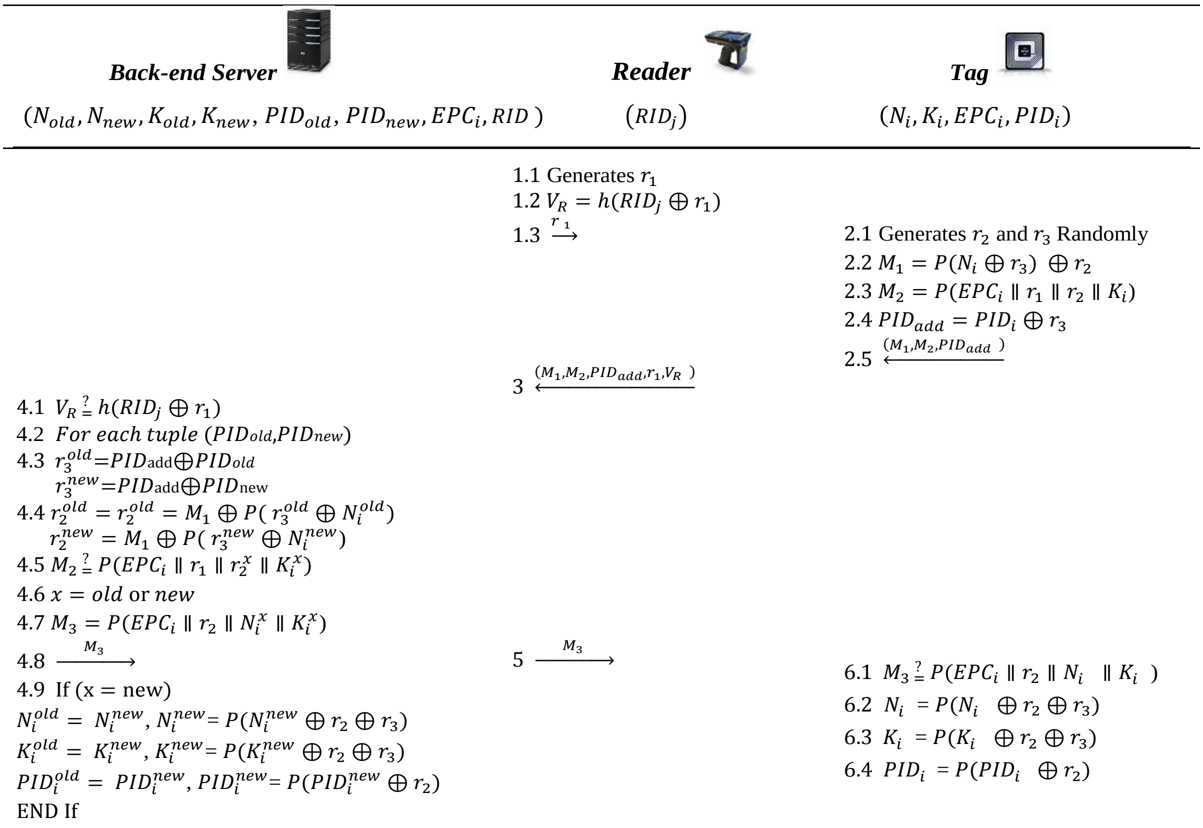
where we define a new random number r_3 which is generated in the tag. Furthermore, we change the updated messages of n_i and K_i by, $N_{i+1} = P(N_i \oplus r_2 \oplus r_3)$. The improved protocol is shown in Figure 3 in details.

Although, the amount of computation and complexity are limiting factors in an RFID protocol, it should be considered that this limitation is so serious in the tag [2], [4]. One of the most important issues that plays the role of impediment for developing RFID system is the cost of RFID tags. Decreasing the tag's price is directly related to reducing its amount of complication and complexity [4]. On the other hand, great developments in electronic devices permit the reader and the back-end server to use a powerful processor. Therefore, an authentication protocol must include as much simplicity as it is possible in the tag, besides providing adequate privacy and security. Moreover, it should switch the complexity over the reader and the back-end server which are equipped with potent processors. In our proposed protocol the connection between the reader and the back-end server is secure. In order to omit weaknesses of the Yu-Jehn's protocol [14] we make changes in the back-end server messages. Although this improvement increases the amount of computation in the back-end server, as we discussed above, this is not so serious in the performance of the RFID system.

5.1 Analysis of our proposed protocol

The improved protocol avoids traceability attack, by preventing transmission of PID_i explicitly and replace it with PID_{add} which increases the amount of computation in the back-end server side, but as we mentioned before, the presence of processor in back-end server will make this issue ignorable [21, 29, 30]. In the rest of this section, the privacy of improved Yu-Jehn protocol is analyzed. It is shown that how our modification on the Yu-Jehn protocol can fix all mentioned weaknesses and increase its privacy.

DoS attack resistance: Preventing access to services and resources for legal users in an RFID system is called Denial of Service (DoS) attack. These attacks usually take place through creating artificial traffic, temporarily interrupt or averting connection. Sometimes an attacker uses the eavesdropped messages during last session and sends them as a query or response which yields in detecting the attacker as a legal user and updating stored values. Since we implement a new random variable r_3 in our proposed protocol, the generated PID_{add} always differs with the value in previous session. Moreover, the structure of the $M_1 = P(N_i \oplus r_3) \oplus r_2$ is related on both r_2 and r_3 random variables. It makes it impossible for an adversary to perform interruption in service. Although the connection between the reader and the back-end server is secure, the manner of generating messages and their dependency via this connection to random variables, prevents an attacker to perform DoS attacks.



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 $V_R \overset{?}{=} h(RID_j \oplus r_1)$ 4.2 *For each tuple* (PID_{old}, PID_{new}) 4.3 $r_3^{old} = PID_{add} \oplus PID_{old}$ $r_3^{new} = PID_{add} \oplus PID_{new}$ 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 $M_2 \overset{?}{=} P(EPC_i \parallel r_1 \parallel r_2^x \parallel K_i^x)$ 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 $M_3 \overset{?}{=} P(EPC_i \parallel r_2 \parallel N_i \parallel K_i)$ 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 $PID_i = P(PID_i \oplus r_2)$

Figure 3. Improved version of Yu-Jehn Protocol.

Secret parameter reveal resistance: Different types of attacks are result of revealing the secret parameters used in an authentication protocol. As described in Section 4.1, the similarity between the transmitted messages and updating procedure results in secret parameter reveal attack. Our improved protocol prevents this attack by defining new messages and implementing fresh random parameters. Here we show that our proposed protocol is secure against revealing the secret parameter:

Learning phase: In session (i), the adversary $\mathcal{A}$ sends an Execute query $(R, T_0, i)$to the tag T_0 and receives $M_{1,i}^{T_0}$, $PID_{i,add}^{T_0}$, $M_{2,i}^{T_0}$.

Attack phase: The attacker sends an Execute query $(R, T_0, i+1)$ in the $(i+1)$th session of the protocol which results in obtaining $M_{1,i+1}^{T_0}$, $PID_{add,i+1}^{T_0}$, $M_{2,i+1}^{T_0}$. There is not any relation between $M_1 = P(N_i \oplus r_3) \oplus r_2$ and the updating description for the secret parameter $N_i = P(N_i \oplus r_2 \oplus r_3)$. Therefore, an attacker is not able to find the correct value for the secret parameter N_i, even if he/she eavesdrops any session of the protocol.

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 the transmitted PID_i from the tag to the reader with $PID_{add} = PID_i \oplus r_3$, where r_3 is a random number 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. As it is described below, an adversary is not able to trace the tag which is proved with *Ouafi* and *Phan* model: 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'. Then he/she let the protocol unfinished. In session $(i+1)$, the attacker sends an Execute query $(R, T_0, i+1)$ to the tag which result in obtaining M_1'', M_2'', PID_{add}. Presenting a new definition for PID_{add} and implementing a new random number r_3, makes it impossible for the attacker to find any similarity between PID_{add}'' and PID_{add}'.

$$PID_i' \oplus r_3' \neq PID_i \oplus r_3$$

In order to provide an immunity against the second traceability attack, we introduce a new definition for M_1 as $M_1 = P(N_i \oplus r_3) \oplus r_2$. Therefore, the adversary cannot obtain N_i and r_2 and consequently he/she will not be able to calculate the value of PID_{i+1} for tracking the tag. Here we use the *Ouafi* and *Phan* privacy model to show that our proposed protocol is not vulnerable to traceability attack:

Learning phase: An adversary sends an Execute query (R, T_0, i) and Execute query $(R, T_0, i+1)$ in sessions (i) and $(i+1)$, respectively and gets $M_{1,i}^{T_0} = P(N_i^{T_0} \oplus r_{3,i}) \oplus r_2$, $PID_{add,i+1}^{T_0}$, $M_{1,i+1}^{T_0}$. Then, he/she calculates $\lambda = P(M_{1,i}^{T_0}) = P(P(N_i^{T_0} \oplus r_{3,i}) \oplus r_{2,i})$ 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 $PID_{add,i+2}^{T_b}$.

Guess phase: The attacker is not able to trace the target tag cause that $PID_{add,i+2}^{T_b}$ is not equal with $P(PID_{i+1}^{T_0} \oplus \gamma)$. Therefore, our proposed protocol prevents an attacker from tracing a specific 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. Here we describe how our proposed protocol assures resistance against backward traceability attack:

Learning phase: In the i^{th} session, the adversary sends a Corrupt query (T_0, K') and gets $(K_i^{T_0}, N_i^{T_0}, EPC_i^{T_0}, PID_i^{T_0})$. Then, it sends an Execute query(R, T_0, i) and obtains $(r_{1,i}, M_{1,i}^{T_0}, M_{2,i}^{T_0}, PID_{i,add}^{T_0})$. Now, the adversary is able to compute $r_{3,i}$ and $r_{2,i}$ as $r_{3,i} = PID_{i,add} \oplus PID_i$ and $r_{2,i} = M_{1,i}^{T_0} \oplus P(N_i^{T_0} \oplus r_{3,i})$, respectively.

Challenge phase: The adversary $\mathcal{A}$ selects two fresh tags T_0 and T_1 for test, , and sends a Test query $(T_0, T_1, i-1)$. According to the randomly chosen bit $b \in \{0,1\}$, the attacker is given a tag $T_b \in \{T_0, T_1\}$. Now in the $(i-1)$ session, the adversary transmits an Execute query $(R, T_b, i-1)$ by sending a random $r'_{1,i}$ and obtains $(M_{1,i-1}^{T_b}, M_{2,i-1}^{T_b})$. But implementation of additional random number r_3 beside r_2 which are generated at the beginning of each session makes it completely impossible for an adversary to detect messages related to the tag T_0, which results in robustness to backward traceability attack. Similarly, it can be proved that the enhanced protocol is not vulnerable to forward traceability attack via *Ouafi* and *Phan* privacy model.

Now, we analyze the performance of our proposed protocol through comparing it with Yu-Jehn [14], Chien and Chen [26], Yeh *et al.* [23] and Yoon [22] protocols which are based on the same framework. As it is shown in Table 2, Chien and Chen's protocol [26] not only suffers from secrecy reveal, but also does not provide untraceable communications for RFID end users. These vulnerabilities are investigated with more details in [23]. Although Yeh *et al.*'s protocol provides immunity against DoS attack, it has weaknesses against traceability attacks and revealing the secret parameter which are proved in [22]. Yu-Jehn [14] indicated that while Yoon's protocol prevents secret parameter reveal, it is still vulnerable to traceability attack. In Section 4, we showed that Yu-Jehn's protocol suffers from traceability attacks and secret parameter reveal. In Section 5.1, it is proved that our improved authentication protocol solves the drawbacks in the existing ones and provides a private and secure communication in an RFID system. Table 3 compares the computational complexity of our improved protocol and protocols introduced previously.

As we mentioned before in this Section, the greatest restriction in proposing an authentication protocol is implementation of less complication in the tag and switch it to the back-end server. Results show that our proposed protocol uses six PRNG function in the tag. Although there is one more PRNG function in comparison with with the Yu-Jehn protocol [14], but providing privacy issue is the result of this complexity. Moreover, Table 3 shows that *Chien and Chen* [26], Yeh *et al.* [23] and Yoon [22] protocols are more complicated than ours.

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 secret parameter reveal, forward traceability and traceability attacks. Then, in order to advance the performance of the analyzed protocol, an improved version is proposed that eliminates the mentioned attacks.

References

[1] Debiao He and Sherali Zeadally. An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE internet of things journal*, 2 (1):72–83, 2015.

[2] Ari Juels. Rfid security and privacy: A research survey. *IEEE journal on selected areas in communications*, 24(2):381–394, 2006.

Table 2. Comparison of privacy analysis.

Attack \ *Protocol*	Chien & Chen [26]	Yeh *et al.* [23]	Yoon [22]	Yu-Jehn [14]	Our Proposed
Forward Traceability	×	×	×	×	✓
Backward Traceability	×	×	×	×	✓
Traceability	×	×	×	×	✓
Secrecy	×	×	✓	×	✓
DoS attack	×	✓	✓	✓	✓

✓: Secure ×: Insecure

Table 3. Comparison of complexity.

Protocols \ *Part*	Back-end server	Reader	Tag
Chien & Chen [26]	2CRC+2P+1H	1H	2CRC+2P
Yeh *et al.* [23]	2CRC+2P+1H	1H	2CRC+2P
Yoon [22]	9P+2H	2H	6P
Yu-Jehn [14]	5P+1H	1H	5P
Our improved	7P+1H	1H	6P

P: PRNG Function H: Hash Function

[3] Andoni Beriain, Eduardo Entremont, J Gonzalez de Chavarri, Ibon Zalbide, and Roc Berenguer. Epc c1g2 compliant batteryless tire pressure monitoring tag with pressure and tire contact temperature. In *International Workshop on Communication Technologies for Vehicles*, pages 163–172. Springer, 2016.

[4] Gildas Avoine. *Cryptography in radio frequency identification and fair exchange protocols*. PhD thesis, Institut de systemes de communication SECTION DES SYSTEMES DE COMMUNICATION ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE POUR LOBTENTION DU GRADE DE DOCTEURES SCIENCES PAR Gildas AVOINE DEA dintelligence artificielle et algorithmique, université de Caen Basse-Normandie, France, 2005.

[5] Nasour Bagheri, Fatemeh Baghernejhad, and Masoumeh Safkhani. On the designing of epc c1 g2 authentication protocol using akari-1 and akari-2 prngs. *Information Technology And Control*, 44 (1):41–53, 2015.

[6] Seyed Mohammad Alavi, Karim Baghery, Behzad Abdolmaleki, and Mohammad Reza Aref. Traceability analysis of recent rfid authentication protocols. *Wireless Personal Communications*, 83(3):1663–1682, 2015.

[7] Hoda Jannati and Behnam Bahrak. Security analysis of an rfid tag search protocol. *Information Processing Letters*, 2016.

[8] Tassos Dimitriou. Key evolving rfid systems: Forward/backward privacy and ownership transfer of rfid tags. *Ad Hoc Networks*, 37:195–208, 2016.

[9] Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, and Mohammad Reza Aref. Enhancing privacy of recent authentication schemes for low-cost rfid systems. *The ISC International Journal of Information Security*, 7(2):135–149, 2015.

[10] Hung-Yu Chien. Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, 4 (4):337–340, 2007.

[11] Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari, and Mohammad Reza Aref. Attacks and improvements on two new-found rfid authentication protocols. In *Telecommunications (IST), 2014 7th International Symposium on*, pages 895–900. IEEE, 2014.

[12] Zhicai Shi, Yongxiang Xia, Yu Zhang, Yihan Wang, and Jian Dai. A crc-based lightweight authentication protocol for epcglobal class-1 gen-2 tags. In *International Conference on Algorithms and Architectures for Parallel Processing*, pages 632–643. Springer, 2014.

[13] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, and Arturo Ribagorda. Lightweight cryptography for low-cost rfid tags. *Security in RFID and Sensor Networks*, pages 121–150, 2016.

[14] Yu-Chung Huang and Jehn-Ruey Jiang. Ultralightweight rfid reader-tag mutual authentication revisited. In *2015 IEEE International Conference on Mobile Services*, pages 166–173. IEEE, 2015.

[15] Yung-Cheng Lee. Two ultralightweight authentication protocols for low-cost rfid tags. *Applied Mathematics and Information Sciences*, 6(2S): 425–431, 2012.

[16] Shahab Abdolmaleky, Shahla Atapoor, Mohammad Hajighasemlou, and Hamid Sharini. A strengthened version of a hash-based rfid server-less security scheme. *Advances in Computer Science: an International Journal*, 4(3):18–23, 2015.

[17] Masoud Mohammadi, Mehdi Hosseinzadeh, and Mohammad Esmaeildoust. Analysis and improvement of the lightweight mutual authentication

protocol under epc c-1 g-2 standard. *Advances in Computer Science: an International Journal*, 3(2):10–16, 2014.

[18] Masoumeh Safkhani, Nasour Bagheri, Pedro Peris-Lopez, Aikaterini Mitrokotsa, and Julio C Hernandez-Castro. Weaknesses in another gen2-based rfid authentication protocol. In *RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on*, pages 80–84. IEEE, 2012.

[19] Umar Mujahid, M Najam-ul Islam, and M Ali Shami. Rcia: a new ultralightweight rfid authentication protocol using recursive hash. *International Journal of Distributed Sensor Networks*, 2015, 2015.

[20] Epcglobal inc., http://www.epcglobalinc.org.

[21] Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, and Mohammad Reza Aref. Untraceable rfid authentication protocols for epc compliant tags. In *Electrical Engineering (ICEE), 2015 23rd Iranian Conference on*, pages 426–431. IEEE, 2015.

[22] Eun-Jun Yoon. Improvement of the securing rfid systems conforming to epc class 1 generation 2 standard. *Expert Systems with Applications*, 39 (1):1589–1594, 2012.

[23] Tzu-Chang Yeh, Yan-Jun Wang, Tsai-Chi Kuo, and Sheng-Shih Wang. Securing rfid systems conforming to epc class 1 generation 2 standard. *Expert Systems with Applications*, 37(12):7678–7683, 2010.

[24] Smail Hassouni and Hassan Qjidaa. A design of modulator and demodulator for a passive uhf rfid tag using dtmost compatible with c1 g2 epc standard protocol. *International Journal of Wireless Information Networks*, 22(4):407–414, 2015.

[25] Hung-Yu Chien and Che-Hao Chen. Mutual authentication protocol for rfid conforming to epc class 1 generation 2 standards. *Computer Standards & Interfaces*, 29(2):254–259, 2007.

[26] Hung-Yu Chien and Che-Hao Chen. Mutual authentication protocol for rfid conforming to epc class 1 generation 2 standards. *Computer Standards & Interfaces*, 29(2):254–259, 2007.

[27] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, and Arturo Ribagorda. Cryptanalysis of a novel authentication protocol conforming to epc-c1g2 standard. *Computer Standards & Interfaces*, 31(2):372–380, 2009.

[28] Khaled Ouafi and Raphael C-W Phan. Privacy of recent rfid authentication protocols. In *Information Security Practice and Experience*, pages 263–277. Springer, 2008.

[29] Nasour Bagheri, Masoumeh Safkhani, and Majid Naderi. Cryptanalysis of a new epc class-1 generation-2 standard compliant rfid protocol. *Neural Computing and Applications*, 24(3-4):799–805, 2014.

[30] Honorio Martin, Enrique San Millán, Pedro Peris-Lopez, and Juan E Tapiador. Efficient asic implementation and analysis of two epc-c1g2 rfid authentication protocols. *IEEE Sensors Journal*, 13(10):3537–3547, 2013.

Seyed Salman Sajjadi Ghaemmaghami obtained his M.S. degree in electrical engineering communications from Science and Research branch Islamic Azad University, Tehran, Iran in 2015 and B.S. degree in electrical engineering-electronic from Karaj Islamic Azad University, Karaj, Iran, in 2010. His research interests include lightweight cryptography, RFID security and privacy, Internet of Things, and wireless communications.

Afrooz Haghbin obtained her B.S. degree in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2001. She obtained her M.S. degree from Tehran University and her Ph.D. degree from Tarbiat Modares University, Tehran, Iran, all in electrical engineering in 2004 and 2009, respectively. She is currently with the electrical and computer department of Science and Research Branch in Azad University, Tehran, Iran, as assistant professor. Her research interests include MIMO wireless communications, channel coding, precoding, multicarrier modulation and estimation theory.

Mahtab Mirmohseni is an assistant professor at department of electrical engineering, Sharif University of Technology (SUT), since 2014. She is also affiliated with the Information Systems and Security Laboratory (ISSL), Sharif University of Technology, Tehran, Iran. She received the B.S., M.S. and Ph.D. degrees from department of electrical engineering, Sharif University of Technology, Tehran, Iran in the field of communication systems in 2005, 2007 and 2012, respectively. She was a postdoctoral researcher at Royal Institute of Technology (KTH), Stockholm, Sweden, in the School of Electrical Engineering till February 2014. Her current research interests include different aspects of information theory, mostly focusing on molecular communication, secure communication and energy-constrained networks.