Journal of Computing and Security

July 2016, Volume 3, Number 3 (pp. 163–174)

http://www.jcomsec.org

Security Analysis of an EPC Class-1 Generation-2 Compliant RFID Authentication Protocol

Fereidoun Moradi [a,*], Hamid Mala [a], Behrouz Tork Ladani [a], Fariba Moradi [b]

[a] *Faculty of Computer Engineering, University of Isfahan, Hezar Jerib Avenue, Isfahan 81746-73441, Iran.*
[b] *Faculty of Computer Engineering, Hamedan University of Technology, Hamedan, Iran.*

ARTICLE INFO.

Article history:
Received: 16 March 2016
Revised: 04 December 2016
Accepted: 29 October 2017
Published Online: 10 February 2018

Keywords:
RFID, EPC-C1G2 Standard,
Mutual Authentication,
Impersonation,
De-Synchronization.

ABSTRACT

Design of secure authentication solutions for low-cost RFID tags is still an open and quite challenging problem, though many protocols have been published in the last decade. In 2013, Wei and Zhang proposed a new lightweight RFID authentication protocol that conforms to the EPC-C1G2 standard and claimed that the protocol would be immune against all known attacks on RFID systems. In this paper, we consider the security of this protocol and show that it cannot provide secure authentication for RFID users. An attacker, by following our suggested approach, will be able to impersonate server/reader, and destroy synchronization between the back-end server and the tag. Finally, we enhance this protocol, and by using formal and informal security analysis we show that the enhanced protocol strongly inhibits the security flaws of its predecessor.

1 Introduction

Radio Frequency Identification (RFID) is a promising new technology that is widely deployed for supply chain and inventory management, retail operations and more generally, automatic identification. An RFID tag is small and low-cost, and a large number of RFID tags can be simultaneously recognized with radio frequency communication. Therefore, the RFID system is expected to replace the current barcode system. Generally, the advantage of RFID over barcode technology is that it does not require direct line of sight reading. Furthermore, compared with barcode readers, RFID readers can interrogate tags concurrently, faster and at greater distances [1, 2].

However, RFID system has two fatal security risks; the privacy problem [1] and the forgery problem [2, 3]. These problems are results of hardware specifications of this system, characteristics of the tag information, method used to transfer the information from the tag to reader, and communication attributes. They can be easily solved if the proper cryptographic algorithms are applied during communication between the tag and the reader [3, 4]. However, as a tag is small and low-cost, its hardware resources are inadequate to implement traditional cryptographic algorithms on RFID tags [1]. There are many researches aiming to solve the privacy and forgery problems with RFID system characteristics [5–7].

EPCglobal is an organization set up to achieve worldwide adoption and standardization of Electronic Product Code (EPC) technology. Currently, its main focus is to both create a worldwide standard for RFID and to facilitate using the internet to share data via the EPCglobal network. It has recently approved

[*] Corresponding author.

Email addresses: fereidoun.moradi@eng.ui.ac.ir (F. Moradi), h.mala@eng.ui.ac.ir (H. Mala), ladani@eng.ui.ac.ir(B. Tork Ladani), fariba.mrd@gmail.com(F. Moradi)

ISSN: 2322-4460 © 2016 JComSec. All rights reserved.

the EPC Class 1 Gen 2 (EPC-C1G2) standard for RFID deployments [8]. This standard defines the functionality of a passive RFID tag, and supports basic reliability guarantees, provided by an on-chip 16-bit pseudo-random number generator ($PRNG$) and a 16-bit Cyclic Redundancy Code (CRC). This standard is designed to strike a balance between cost and functionality, with less attention paid to security.

The security level of EPC-C1G2 standard is very weak. Aiming to increase this security level, many proposals have been published [9–12]. However, almost all of them were soon followed by cryptanalysis attacks [13–16]. In this paper, we show how Wei and Zhang's scheme [17] suffers the same fate as previous proposals. We will call this protocol WZ-LRAP (Wei and Zhang's Lightweight RFID Authentication Protocol).

The rest of the paper is organized as follows. The related works is reviewed in Section 2. Wei and Zhang's protocol is briefly described in Section 3. The properties of CRC functions are studied in Section 4. We present our attacks in Section 5. In Section 6, we propose a modification to WZ-LRAP and its security is formally verified using BAN logic. Finally, the paper is concluded in Section 7.

2 Related Works

In this section, we briefly review some attempts to raise the security level of authentication schemes related to EPC-C1G2 authentication protocols.

In 2007, Chien et al. proposed an authentication solution which heavily relied on the abuse of CRC [18]. However, Peris-Lopez et al. showed that the protocol cannot resist to tag impersonation, de-synchronization attacking and location tracking [19]. This way, their protocol not only is vulnerable to such attacks, but also does not provide tag privacy.

Duc et al. proposed an RFID authentication protocol in EPC platform [20]. The security of Duc et al.'s protocol is based on key synchronization between tags and back-end server. The last message of the protocol is comprised of an *EndSession* command, which is sent to both tags and readers. Interception of one of these messages will cause a synchronization loss between the tag and the server. This situation allows an attacker to trace back all past communications.

Chen and Deng proposed a mutual authentication scheme by using $PRNG$ and CRC functions. Their protocol tried to apply CRC as a cryptographic hash function for message authentication [21]. However, Peris-Lopez et al. exploited the linearity of CRC function to show that the protocol fails to provide its security objectives [13].

Yeh et al. proposed an RFID mutual authentication protocol conforming to the EPC-C1G2 standard [9]. The information transmitted between reader and back-end server may also be eavesdropped and intercepted by the attacker in actual environment. Thus, the protocol applied a one-way hash function to guarantee the communication security between reader and back-end server. However, it was pointed out that the protocol has data integrity problem and forward secrecy problem [22].

In 2012, Yi et al. analyzed the security of Chien's authentication protocol [18] and proposed an improved design based on a set of clear security requirements [11]. But, Safkhani et al. scrutinized the protocol and showed a simple approach to de-synchronize protocol's parties. Moreover, they presented a tag and reader impersonation attack with negligible associated computational requirements [14].

In 2015, Yu-Jehn studied Chien and Chen's protocol and proposed a new mutual authentication scheme for EPC-C1G2 RFID tags [23]. But, Yu-Jehn missed these notes including definition of a new and randomized quantity as a secret value and wiping the similarity between the transmitted messages. Soon after in 2016, Ghaemmaghami et al. [24] showed that the proposed protocol does not provide privacy and the scheme is susceptible to traceability attack. Then, in order to enhance the privacy of the protocol, they presented an improved version to prevent the mentioned attack.

In 2016, Abdolmaleki et al. [25] cryptanalyzed an RFID mutual authentication scheme which had been proposed by Xiao et al. [26]. They first presented four attacks against this protocol including secret parameters reveal, tag impersonation, backward traceability and forward traceability. Then, they proposed an efficient and secure RFID authentication protocol.

In 2017, through applying the Ouafi-Phan privacy model [27] Abdolmaleki et al. [28] revealed some weaknesses and presented various traceability attacks on the privacy of three RFID authentication protocols proposed by Wang et al. [29], Safkhani et al. [30], and Sun-Zhong [31]. Abdolmaleki et al. pointed out that these protocols suffer from two main problems of dependency between tag's responses and updating procedure. Then, in order to overcome the existing weaknesses of these protocols, they applied some modifications and proposed an improved version of each one.

Eyad Taqieddin [32] provided a new investigation of the improper use of CRC function for cryptographic purposes in RFID systems which presents full disclosure attacks against Gao et al. scheme [33] and then offers suggestions for designing more secure protocols.

3 Wei and Zhang's Protocol

In 2013, Wei and Zhang [17] proposed WZ-LRAP as an EPC-C1G2 authentication protocol. We will outline the WZ-LRAP in brief, which consists of two phases: the initialization phase and the authentication phase. The definitions of notations used by authors are shown in Table 1 and Figure 1 depicts the protocol steps.

***Initialization Phase*:** For each tag T_i the back-end server randomly selects $metaID_i$, K_i^1, K_i^2. The back-end server maintains a record of $(metaID_{iold}, K^2_{iold}, metaID_{inew}, K^2_{inew})$. A $Flag$ value is used to indicate whether the old or the new secret parameters are used. The value K_i^1 is sent to the reader cache, and it is the same for all tags.

***Authentication Phase*:** The authentication between the tag (T_i), the back-end server (S) and the reader (R) is described as follows.

(1) $R \rightarrow T_i : Query, N_r$
The reader generates a random number N_r and sends a request message to the tag.

(2) $T_i \rightarrow R : M_1, N||(N_t \oplus [K_i^1]_L)$
The tag T_i generates the random number N_t, computes $N = CRC([K_i^1]_R||N_r) \oplus N_t$ and $M_1 = [CRC(K_i^2||(N_r \oplus N_t))||CRC(K_i^2||N_t)] \oplus metaID_i$ and sends the message $M_1, N||(N_t \oplus [K_i^1]_L)$ to the reader R.

(3) $R \rightarrow S : M_1, N_t, N_r$
After receiving the message by the reader, it decrypts $N_t \oplus [K_i^1]_L$ to obtain N_t, and computes the value $N' = CRC([K_i^1]_R||N_r) \oplus N_t$ and checks whether $N' = N$ or not. If it holds, the reader transmits the message (M_1, N_t, N_r) to the back-end server, otherwise the authentication process is stopped.

(4) $S \rightarrow R : M_2$
The back-end server gets (M_1, N_t, N_r), then iteratively picks up an entry $(metaID_{iold}, K^2_{iold}, metaID_{inew}, K^2_{inew})$ from its database, computes the value M_1' and checks whether it equals to the received M_1 or not. The process is repeated until a match is found in the database, thus implying a successful authentication of the tag. If no match is found, the authentication fails. The back-end server performs the following steps at the same time.

- If $Flag$=1, the match record is $(metaID_{inew}, K^2_{inew})$. Then it computes $M_2 = [CRC(K^2_{inew}||N_t)|| CRC(K^2_{inew}||N_r)] \oplus metaID_{inew}$, and updates the secret parameters of tag T_i as follows:

  $-metaID_{iold} \leftarrow metaID_{inew}$
  $-K^2_{iold} \leftarrow K^2_{inew}$
  $-K^2_{inew} \leftarrow PRNG(K^2_{inew}) \oplus N_t$
  $-metaID_{inew} \leftarrow PRNG(metaID_{inew})|| CRC(metaID_{inew}) \oplus N_t \oplus N_r$

- If $Flag$=0, it does not change $(metaID_{iold}, K^2_{iold})$, computes M_2 and updates $(K^2_{inew}, metaID_{inew})$ of tag T_i.

  $-K^2_{inew} \leftarrow PRNG(K^2_{inew}) \oplus N_t$
  $-metaID_{inew} \leftarrow PRNG(metaID_{inew})|| CRC(metaID_{inew}) \oplus N_t \oplus N_r$

Finally, the back-end server sends the message M_2 to the reader.

(5) $R \rightarrow T_i : M_2$
Upon receiving M_2, the tag verifies whether the equation $M_2 \oplus metaID_i = [CRC(K_i^2||N_t)||CRC(K_i^2||N_r)]$ holds. If so, it updates K_i^2 and $metaID_i$.

4 Cyclic Redundancy Codes (CRCs)

CRCs are error-detecting codes that check (non-malicious) errors caused by faults during transmission. They are additive operators with strong linearity aspects (the modulo operator is homomorphic), and therefore its use as a cryptographic tool is not appropriate [34].

Definitions and Notations.

Let A be an m-bit string in $\{0,1\}^m, A = A_{m-1}||A_{m-2}||\ldots||A_0$. We define $A_{\ll n}$ as the $m+n$ bit string A' resulting from left-shift of A by n-bits and inserting n zeros from the right [13, 35].

$$A'_i = \begin{cases} 0 & for \quad 0 \leq i \leq n-1 \\ A_{i-n} & for \;\; n \leq i \leq n+m-1 \end{cases}$$

Let B be an n-bit string in $\{0,1\}^n$, where $n \leq m$. We define the exclusive-OR operation $A \oplus B = B \oplus A$ as follows:

$$(A \oplus B)_i = \begin{cases} A_i \oplus B_i & for \;\; 0 \leq i \leq n-1 \\ A_i & for \;\; n \leq i \leq m-1 \end{cases}$$

Table 1. Notations

Symbol	Description
N_r	16-bit random number generated by the reader.
N_t	16-bit random number generated by the tag.
K^1	32-bit key shared by the reader and the tag.
K^2	16-bit key shared by the tag and the back-end server.
$metaID$	32-bit ID pseudonym shared by the tag and the back-end server.
$metaID_{old}, K^2_{old}$	The previous values of $metaID$ and K^2 before update.
$metaID_{new}, K^2_{new}$	The values of $metaID$ and K^2 after update.
$\oplus$	The bitwise XOR operation.
$\|\|$	The concatenation operation.
$B \leftarrow A$	Assigning the value of A to B.
$[x]_{L/R}$	The left/right half part of the string x.
$CRC()$	The Cyclic Redundancy Code (CRC) function with 16-bit output length.
$PRNG()$	The pseudo random number generator with 16-bit output length.

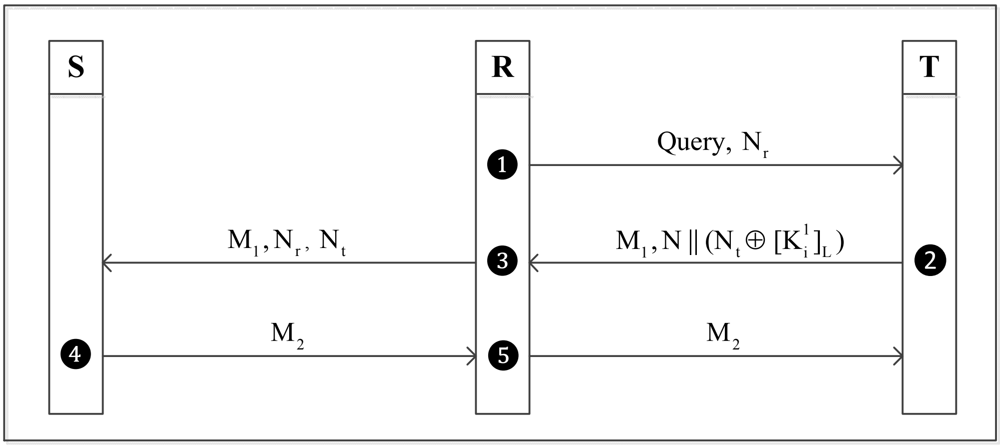

Figure 1. Wei and Zhang's Lightweight RFID Authentication Protocol

Due to the linearity, $CRCs$ have the following properties. Let A be any bit string and B be n-bit string. Then, as proved in [13, 35], CRC satisfies the following properties.

$$CRC(A \oplus B) = CRC(A) \oplus CRC(B) \qquad (1)$$

$$CRC(A||B) = CRC(A_{\ll n}) \oplus CRC(B) \qquad (2)$$

We will take advantage of these properties for attacking WZ-LRAP.

5 Vulnerabilities of Wei and Zhang's Protocol

In this section, we present concrete attacks to WZ-LRAP. We use the standard Dolev-Yao intruder model [36], in which the adversary controls the "network". In this model, the adversary can eavesdrop, block, modify, and inject messages in any communication between reader and tag. However, the channel between back-end server and reader is assumed to be secure, which can be guaranteed by using full-fledged cryptographic technologies.

5.1 Server/Reader Impersonation Attack

We show that an active adversary can impersonate a legitimate server/reader to a tag in WZ-LRAP even when the adversary has no access to any of the tag's secrets. The detail of this attack is given below. In this case we focus on message M_2, generated by the back-end server. The adversary should be able to generate this message in order to impersonate the legitimate server/reader. For the adversary, it is enough to listen an iteration between a legitimate tag and the reader in order to exploit this vulnerability.

(1) $R \rightarrow T_i : Query, N_r$
(2) $T_i \rightarrow R : M_1, N||(N_t \oplus [K_i^1]_L)$
(3) $R \rightarrow S : M_1, N_t, N_r$
(4) $S \rightarrow R : M_2$
(5) $R \rightarrow T_i : M_2$

The adversary has to block or disturb radio channel to obstruct the correct reception of message 5. The objective of this is to prevent the legitimate tag from updating its K_i^2 and $metaID_i$. At this moment, the adversary could supplant the back-end server without knowing its private information. It chooses the random number N_r from previous session, and sends it to the tag. The tag generates a random number N_t' and replies with $M_1', N'||(N_t' \oplus [K_i^1]_L)$. Then, the adversary using the eavesdropped values (N_r, M_1', M_2), calculates a new value $M_2' = [M_1']_L \oplus CRC(N_r)||[M_2]_R$, and sends it to the tag. Finally, the tag accepts M_2' and authenticates the adversary.

We now prove that the tag will accept M_2' and the adversary will impersonate as a legitimate server/reader. The adversary knows the following values,

$$\begin{aligned} M_1' &= [CRC(K_i^2||(N_r \oplus N_t'))||CRC(K_i^2||N_t')] \\ &\quad \oplus metaID_i \\ M_2 &= [CRC(K_i^2||N_t)||CRC(K_i^2||N_r)] \oplus metaID_i \end{aligned}$$

Thus, by using CRC properties shown in previous section iteratively, the following equations hold. From property (2), we can observe that

$$\begin{aligned} M_1' = [&CRC(K^2_{i\ll 16}) \oplus CRC\,(N_r \oplus N_t') \\ &||CRC(K^2_{i\ll 16}) \oplus CRC(N_t')] \oplus metaID_i \end{aligned}$$

and, using the property (1), it is easy to see

$$\begin{aligned} M_1' = [&CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus CRC(N_t') \\ &||CRC(K^2_{i\ll 16}) \oplus CRC(N_t')] \oplus metaID_i. \end{aligned}$$

Furthermore, the following result can be achieved by separating the $metaID_i$ into two parts.

$$\begin{aligned} M_1' = [&CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus CRC(N_t') \\ &\oplus [metaID_i]_L||CRC(K^2_{i\ll 16}) \oplus CRC(N_t') \\ &\oplus [metaID_i]_R] \end{aligned}$$

In the same as above via the property (1) and (2), we can rewrite M_2 equation as follows.

$$\begin{aligned} M_2 = [&CRC(K^2_{i\ll 16}) \oplus CRC(N_t) \oplus [metaID_i]_L \\ &||CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus [metaID_i]_R] \end{aligned}$$

Since adversary knows N_r, it can calculate $CRC(N_r)$ by definition of CRC. From this value and following equations,

$$\begin{aligned} [M_1']_L &= CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus CRC(N_t') \\ &\quad \oplus [metaID_i]_L \\ [M_1']_R &= CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus [metaID_i]_R \\ [M_2]_L &= CRC(K^2_{i\ll 16}) \oplus CRC(N_t) \oplus [metaID_i]_L \\ [M_2]_R &= CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus [metaID_i]_R \end{aligned}$$

it can calculate

$$\begin{aligned} M_2' &= [M_1']_L \oplus CRC(N_r)||[M_2]_R \\ &= [CRC(K^2_{i\ll 16}) \oplus CRC(N_t') \oplus [metaID_i]_L \\ &\quad ||CRC(K^2_{i\ll 16}) \oplus CRC(N_r) \oplus [metaID_i]_R] \\ &= [CRC(K_i^2||N_t')||CRC(K_i^2||N_r)] \oplus metaID_i \end{aligned}$$

which is the exact value a legitimate server/reader was expected to send to the tag. Therefore, the adversary can successfully impersonate the server/reader.

5.2 De-synchronization Attack

Wei and Zhang propose that the back-end server maintains old and new values $\{metaID_i, K_i^2\}$ for each tag to defend against a de-synchronization. This assumption allows the back-end server to authenticate tags and re-synchronize these tags each time they suffer a de-synchronization. However, our impersonation attack described in Section 5.1. results in synchronization loss between the back-end server and the tag due to update of the secret information of the tag.

The adversary forces the tag to update its secret value such that it does not match the value that back-end server has stored in its database. The tag uses N_t' to update K_i^2 and $metaID_i$ as follows.

$$\begin{aligned} &K_i^2 \leftarrow PRNG(K_i^2) \oplus N_t' \\ &metaID_i \leftarrow PRNG(metaID_i)||CRC(metaID_i) \\ &\qquad \oplus N_t' \oplus N_r \end{aligned}$$

Therefore, after the tag updates its secret parameters, the updated values K_i^2 and $metaID_i$ of the tag will be different to the corresponding parameters stored in the database of the back-end server. Thus, de-synchronization happens, and the tag and the back-end server will not authenticate each other anymore.

6 Countermeasure for the Security Vulnerabilities on WZ-LRAP

We now describe a countermeasure for WZ-LRAP to overcome the flaws mentioned in the previous sections and other attacks in the context. The main weakness of the protocol is that the computational similarity between $M_1' = [CRC(K_i^2|| (N_r \oplus N_t'))||CRC(K_i^2||N_t')] \oplus metaID_i$ and $M_2 =$

$[CRC(K_i^2||N_t)||CRC(K_i^2||N_r)] \oplus metaID_i$ gives the adversary an opportunity to forge a valid M_2' without knowing the secret values K_i^2 and $metaID_i$.

The structure of messages should be altered in order to switch the complexity over the reader and the back-end server which is equipped with stronger processors and also to provide quick and reasonable assurance of the integrity of messages delivered. CRC is an easily reversible function, which makes it unsuitable for use in cryptographic operations. Following this fact, we should try to reduce the number of calls to this function on the tag side and change the construction to protect secret values from revealing.

To prevent the given de-synchronization and server/reader impersonation attacks, we make some changes in generating message M_1, that is generated by the tag. First, the structure of this message is changed to apply $PRNG$ function in the places where the CRC functions are used. This alteration eliminates the messages similarity in authentication process but still it is feasible for an adversary to mount exhaustive key search on this construction. Therefore, for inhibition of this weakness we consider second operational change to supplant inner concatenation operations with the exclusive-OR. Mainly, using $PRNG$ function with exclusive-OR as its input operation does not contradict with each other. $PRNG$ function does not have linearity properties so it can be used as a one-way function, therefore the following definition of M_1 can wipe out the aforementioned attacks.

$$M_1 = [PRNG(K_i^2 \oplus N_r)||PRNG(K_i^2 \oplus N_t)] \\ \oplus metaID_i$$

6.1 Security Analysis

Here, we present a detailed security analysis of the proposed modifications to show that it meets resistance against the attacks presented in this paper and the other known active and passive attacks in the context. Our security proof is carried out based on informal method relying on the heuristic opinions of security experts and also the formal method relying on the mathematical rules to draw a conclusion.

Informal method mainly relies on intelligence of analyst. Since the analyst may forget or ignore some points during the analysis, so there is no way to understand if the analysis is complete or not. However, due to its simplicity and lack of need for sophisticated tools, the informal methods are widely used in the protocol security analysis.

In the formal method, the target protocol and its features are modeled based on algebra and logic. Several logic tools exist to prove the security correctness of a cryptographic authentication protocol, for example, BAN logic [37], GNY logic [38], AVISPA tool [39], and ProVerif tool [40].

Furthermore, there are limitations in formalizing security notions of cryptographic protocols which are practical and useful in real-life setting. For example, de-synchronization is needed for practical sense for cryptographic protocols, while we cannot easily formalize this property. Thus, we combine these two informal and formal methods to prove the security correctness.

In this subsection, first we argue the security improvement through informal method then we use BAN logic for modeling to prove the security correctness of the revised protocol.

Resistance against Replay Attack.

In the revised scheme, the message M_1 like other the authentication messages (*i.e.* M_2, and N) is computed with the random numbers, which provides freshness and resistance against replay attack.

Resistance against Tag Impersonation Attack.

The resistance of WZ-LRAP against tag impersonation attack arises from this fact that the tag's information ($metaID$ and K^2) is stored in the back-end server, which is assumed to be secure, and this assumption that the communication channel between the back-end server and the reader is secure. Therefore, an adversary is not able to access the information of a tag which is stored in the back-end server.

On the other hand, the adversary, who wants to impersonate the valid tag, must be able to complete the authentication steps successfully. It needs to respond to the reader with a valid M_1 which is computed on the basis of the shared secret keys K^2 and $metaID$. Thus, it is not possible for the attacker to compute a valid M_1 without knowing secret values of K^2 and $metaID$.

Resistance against Server/Reader Impersonation Attack.

In the revised scheme, through message transformation ($PRNG$ generated message) such as M_1 or transmitting scrambled bits (XOR-ed) the revised scheme data security is achieved. In addition, M_1 and M_2 involve at least two secret values ($metaID$ and K^2) that are well protected against eavesdroppers. Among the mutual communication period, anonymity of the tags can be provided since only transformed messages and valid random numbers are broadcasted. Hence, adversary cannot easily impersonate the server/reader. The best strategy for the adversary to impersonate the server/reader could be sending a random value to the tag. However, since the tag has only one record of the secret parameter, the adversary's success probability in each try is bounded by 2^{-16}.

Resistance Against De-synchronization Attack.

De-synchronization attack against WZ-LRAP happened after the adversary succeeded to impose invalid random number on the tag for updating parameters. This flaw is based on the linear property of CRC function which is fixed by using $PRNG$ function in using M_1.

Moreover, employment of a combined process oriented mechanism ($flag = 0$ or $flag = 1$) in updating the shared secret keys makes parties remain in synchronized state even if the previous session is not safely terminated. This design allows a tag with non-synchronized keys due to de-synchronization attack, to be still authenticated by the back-end server and re-synchronize its secret data with the server database.

Resistance Against Traceability Attack.

Traceability attack against WZ-LRAP is accomplished based on this fact that an adversary can link two different sessions of a tag. WZ-LRAP guarantees tag privacy by refreshing the secret and the random number in tag for each session. Hence, adversary cannot easily trace a specific tag since there are no consistent clues revealed in each tag response. Furthermore, due to the freshness of random numbers N_r and N_t per session, our scheme can resist the replay attack.

6.2 Formal Logic Proof

Following, we use BAN logic to prove the security correctness of the revised scheme. We formally show that after one run of the protocol, the tag, the reader, and the server believe the received messages are from the expected sender, and these messages are fresh. Hence, they can be authenticated by each other properly. To prove the security of a protocol formally with BAN logic, the following four steps should be followed [37]:

a) The messages and the actions of the protocol parties should be represented by mathematical relations.

b) The messages and the actions of the protocol parties should be converted into BAN logic formulas and dropping the plain text messages from protocol messages. In this step, the resulting protocol messages are called idealized messages.

c) The protocol initial assumptions and security goals should be explained as BAN logic formulas.

d) Finally, the protocol security goals should be deduced. In this step, using BAN logic rules, it is evaluated whether protocol security goals are satisfied or not.
We present only principle rules and notations in Table 2 which are used in our proof.

a) *Expression of the revised scheme messages as mathematical relations.*

$$
\begin{aligned}
&\mathit{M1}: R \rightarrow T_i : Query, N_r\\
&\mathit{M2}: T_i \rightarrow R : [PRNG(K_i^2 \oplus N_r)||\, PRNG(K_i^2 \oplus N_t)]\\
&\qquad \oplus metaID_i,\\
&\qquad [CRC([K_i^1]_R||N_r) \oplus N_t]||(N_t \oplus [K_i^1]_L)]\\
&\mathit{M3}: R \rightarrow S : [PRNG(K_i^2 \oplus N_r)||PRNG(K_i^2 \oplus N_t)]\\
&\qquad \oplus metaID_i,\ N_t, N_r\\
&\mathit{M4}: S \rightarrow R : [CRC(K_i^2||N_t)||CRC(K_i^2||N_r)]\\
&\qquad \oplus metaID_i\\
&\mathit{M5}: R \rightarrow T_i : [CRC(K_i^2||N_t)||CRC(K_i^2||N_r)]\\
&\qquad \oplus metaID_i
\end{aligned}
$$

b) *Messages idealization.*
In this step, we transform each message into an idealized message, such as plaintexts are omitted from protocol messages, and only encrypted message contents are relevant to this step. We also use BAN logic notations for representing these idealized messages as follows.

$$
\begin{aligned}
&\mathit{IM1}: R \lhd \{\{N_r\}_{K_i^2}, \{N_t\}_{K_i^2}\}_{metaID_i}\\
&\mathit{IM2}: R \lhd \{N_t\}_{[K_i^1]_L}\\
&\mathit{IM3}: S \lhd \{\{N_r\}_{K_i^2}, \{N_t\}_{K_i^2}\}_{metaID_i}\\
&\mathit{IM4}: T_i \lhd \{N_r, N_t, K_i^2\}_{metaID_i}
\end{aligned}
$$

c) *Initial assumptions and security goals.*
The explicit assumptions of the revised protocol are shown in the succeeding text.

$$
\begin{aligned}
&\mathit{A1}: S| \equiv T_i \overset{K_i^2}{\longleftrightarrow} S\\
&\mathit{A2}: T_i| \equiv S \overset{K_i^2}{\longleftrightarrow} T_i\\
&\mathit{A3}: T_i| \equiv R \overset{K_i^1}{\longleftrightarrow} T_i\\
&\mathit{A4}: R| \equiv T_i \overset{K_i^1}{\longleftrightarrow} R\\
&\mathit{A5}: S| \equiv T_i \overset{metaID_i}{\longleftrightarrow} S\\
&\mathit{A6}: T_i| \equiv S \overset{metaID_i}{\longleftrightarrow} T_i\\
&\mathit{A7}: T_i| \equiv \#(N_t)\\
&\mathit{A8}: R| \equiv \#(N_r)
\end{aligned}
$$

The assumptions *A1* to *A6* are related to secrets which are shared between the protocol parties and the assumptions *A7* and *A8* are related to freshness of

Table 2. Principles and Notations

Principles and Notations	Meaning
$P \triangleleft MSG1:$	P receives $MSG1$ (possibly after doing some decryption).
$P\| \sim MSG1:$	P sends $MSG1$.
$\#(X):$	X is fresh.
$P\| \equiv \#(MSG1):$	P believes the freshness of $MSG1$.
$\{X\}_K:$	Message X is encrypted with the key of K.
$P\| \equiv P \overset{K}{\leftrightarrow} Q:$	P believes the secret K is shared between P and Q.
$R1: \dfrac{P\| \equiv P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P\| \equiv Q\| \sim X}$	: The message meaning rule of BAN logic that means if P believes that it shares a secret key K with and if P receives a message X encrypted with K, then P is entitled to believe that Q once said X. In this paper we called this rule $R1$.
$R2: \dfrac{P\| \equiv Q\| \sim \{X,Y\}}{P\| \equiv Q\| \sim \{X\}}:$	This is one rule of BAN logic that means if P believes Q has sent X, Y then P is entitled to believe that Q has sent X. In this paper we called this rule $R2$.

random numbers which are generated by the reader and the tag respectively. The goals of the proposed scheme are as below.

G1 : $S| \equiv T_i| \sim N_t$
G2 : $T_i| \equiv S| \sim N_r$

In the above, *G1* means that the server believes the tag T_i has sent the random number N_t. This goal shows that the adversary does not have any control on this random number, which was generated by the tag and sent through the reader to the server. Therefore, the adversary cannot apply any attack on the protocol that requires any change on the random number.

G2 means that the tag believes that N_r, which is generated by the reader, is transmitted to the tag without any modification. In other words, at the end of the last step of this protocol run, this random number reach to the tag without any tampering by the adversary.

d) Goals deductions.
In this step, we combine idealized messages and the assumptions to construct numerator expressions of BAN logic rules. If such relations are corresponded to the numerator expressions of BAN logic rules, it can be concluded that the denominator expressions of BAN logic rules are correct. We show these deductions as below.

D1:IM3, A5, R1 $\Rightarrow S| \equiv T_i| \sim \{\{N_r\}_{K_i^2}, \{N_t\}_{K_i^2}\}$
D2:D1, R2 $\Rightarrow S| \equiv T_i| \sim \{N_t\}_{K_i^2}$

As the *IM1* and *IM3* show, the encrypted messages are delivered directly to the server through the reader in the secure communication channel. Therefore, the final result of *D2* is $S \triangleleft \{N_t\}_{K_i^2}$.

D3:D2, A1, R1 $\Rightarrow S| \equiv T_i| \sim N_t$

It is obvious that *D3* is equals to *G1*. Similarly, we have following deductions to reach *G2*.

D4: IM4, A6, R1 $\Rightarrow T_i| \equiv S| \sim \{N_r, N_t, K_i^2\}$
D5:D4, R2 $\Rightarrow T_i| \equiv S| \sim N_r$

Finally, it also deduced that *D5* is equals to *G2*. Hence, the security goals of the revised scheme, are satisfied.

6.3 Performance Analysis

The proposed modification does not increase computational cost of the protocol extensively while it provides much better security. It has only one more exclusive-OR operation on the both side because of reducing the number of concatenation operation. The only increased cost is two calls of $PRNG$ function instead of CRC function. Table 3 shows performance comparison between WZ-LRAP and revised scheme in detail.

Now, we analyze the efficiency of our revised scheme through comparing it with Ghaemmaghami et al. [24] and Abdolmaleki et al. [25, 28] protocols which are based on the same framework. They succeeded in omitting the vulnerability of likeness between the transmitted messages and removed drawbacks in the updating procedure.

As shown in Table 4, Ghaemmaghami et al. [24] and Abdolmaleki et al. [25, 28] protocols store $4n$ and $3n$ parameters in the tag memories. Our revised scheme stores $3n$ parameters that is an efficient value in storage areas. It is also shown that our countermeasure impacts the protocol to involve CRC besides $PRNG$ function on the tag side. On the point of implementation, these functions can employ LFSR-based operations in the same hardware.

Table 3. Performance Comparison

Server/Tag of Protocols	$\#PRNG$	$\#\oplus$	$\#CRC$	$\#\|\|$	#Transfered bits
Server of WZ-LRAP	2	$6n$	5	7	n
Server of Revised Scheme	4	$7n$	3	5	n
Tag of WZ-LRAP	2	$8n$	6	9	$2n$
Tag of Revised Scheme	4	$9n$	4	7	$2n$

n denotes the bit length of parameters.

Table 4. Comparison of Revised Scheme With Similar Ones

Protocols	Comp. of Tag	Comp. of Server/Reader	Storage of Tag	Storage of Server/Reader	Rounds of Communication
[24]	$6P$	$7P + 2H$	$4n$	$9n$	5
[25]	$7P$	$7P + 4H$	$4n$	$9n$	5
[28]	$6P$	$7P$	$3n$	$5n$	3
This scheme	$4P + 4CRC$	$4P + 3CRC$	$3n$	$4n$	4

n denotes the bit length of parameters. H: Hash function. P: $PRNG$ function.

Indeed, the idea of using linear feedback shift registers (LFSR) in the construction of cost-effective operations for RFID tags is widely suggested [41].

LFSR functions are fast and efficient in hardware implementations as well as simple in terms of computational requirements. Therefore, the main functions of the revised scheme are able to execute LFSR-based functions in the same hardware and are suitable for RFID applications.

The required hardware complexity of low-cost tags is considered by its number of equivalent logic gates (GEs). Based on the measurements presented by [42, 43], the number of GEs for LFSR-based $PRNG$ is about 453 because of implementing polynomial selector and decoding logic modules. In addition, LFSR can be measured with approximately 73 GEs. LFSR along with a few logic gates are used to obtain CRC. This scheme versus the similar protocols holds four calls of CRC rather than $PRNG$. Hence, the energy consumption for operating functions of this scheme is almost 1.5 times lower than other comparing protocols.

In terms of communication rounds, our revision assures a secure performance without increasing rounds rather than WZ-LRAP scheme. In all mentioned protocols, three of these rounds are related to connection between the reader and the tag, while others are associated to connection between the reader and the back-end server. Reducing the computational cost of the tag is the goal for designing improved authentication protocols. Therefore, this scheme has low communication complexity and computational cost.

7 Conclusions

In this paper we investigated the security of a lightweight RFID authentication protocol compliant with EPC-C1G2 which has been proposed by Wei and Zhang [17]. We proved that, in contrary to the designers claim, this protocol does not provide resistance against server/reader impersonation and de-synchronization attacks. We showed that the security weaknesses are due to the abuse of the CRC included in protocol and computational similarity between transferred messages. In addition, we proposed a modification of this protocol to withstand the attacks presented in this paper. We also analyzed the security properties of the proposed protocol as well as its efficiency. The proposed scheme also was compared with the original WZ-LRAP and two other similar protocols.

References

[1] Ari Juels. RFID security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006. doi:10.1109/JSAC.2005.861395. URL `https://doi.org/10.1109/JSAC.2005.861395`.

[2] Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks.

In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pages 59–66. IEEE, 2005.

[3] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim. Mutual authentication protocol. In *Workshop on RFID and lightweight crypto*, 2005.

[4] Sanjay E Sarma, Stephen A Weis, Daniel W Engels, et al. RFID systems and security and privacy implications. In *CHES*, volume 2, pages 454–469. Springer, 2002.

[5] Yung-Chin Chen, Wei-Lin Wang, and Min-Shiang Hwang. RFID authentication protocol for anti-counterfeiting and privacy protection. In *Advanced Communication Technology, The 9th International Conference on*, volume 1, pages 255–259. IEEE, 2007.

[6] Y-C Lee, Y-C Hsieh, P-S You, and T-C Chen. An improvement on RFID authentication protocol with privacy protection. In *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, volume 2, pages 569–573. IEEE, 2008.

[7] Jung-Sik Cho, Sang-Soo Yeo, and Sung Kwon Kim. An analysis of RFID tag authentication protocols using secret value. In *Future Generation Communication and Networking (FGCN 2007)*, volume 1, pages 482–487. IEEE, 2007.

[8] EPCglobal Ratified Standard. EPC Radio Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.0. 9. *EPCglobal, US*, 2005.

[9] 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.

[10] 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.

[11] Xiaoluo Yi, Liangmin Wang, Dongmei Mao, and Yongzhao Zhan. An gen2 based security authentication protocol for RFID system. *Physics Procedia*, 24:1385–1391, 2012.

[12] Jing Huey Khor, Widad Ismail, Mohammed I Younis, MK Sulaiman, and Mohammad Ghulam Rahman. Security problems in an RFID system. *Wireless Personal Communications*, 59(1):17–26, 2011.

[13] Pedro Peris-Lopez, Julio C Hernandez-Castro, Juan ME Tapiador, and Jan CA Van der Lubbe. Cryptanalysis of an EPC class-1 generation-2 standard compliant authentication protocol. *Engineering Applications of Artificial Intelligence*, 24(6):1061–1069, 2011.

[14] 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.

[15] Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Lopez, and Nasour Bagheri. Weaknesses of fingerprint-based mutual authentication protocol. *Security and Communication Networks*, 8(12): 2124–2134, 2015.

[16] Fereidoun Moradi, Hamid Mala, and Behrouz Tork Ladani. Security analysis and strengthening of an RFID lightweight authentication protocol suitable for VANETs. *Wireless Personal Communications*, 83(4): 2607–2621, 2015.

[17] Guoheng Wei and Huanguo Zhang. A lightweight authentication protocol scheme for RFID security. *Wuhan University Journal of Natural Sciences*, 18(6):504–510, 2013.

[18] 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.

[19] Pedro Peris-Lopez, Tieyan Li, Julio C Hernandez-Castro, and Juan ME Tapiador. Practical attacks on a mutual authentication scheme under the EPC Class-1 Generation-2 standard. *Computer Communications*, 32(7): 1185–1193, 2009.

[20] Dang Nguyen Duc, Hyunrok Lee, and Kwangjo Kim. Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning. *Auto-ID Labs Information and Communication University, White Paper*, 2006.

[21] Chin-Ling Chen and Yong-Yuan Deng. Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection. *Engineering Applications of Artificial Intelligence*, 22(8):1284–1291, 2009.

[22] Masoumeh Safkhani, Nasour Bagheri, Somitra Kumar Sanadhya, and Majid Naderi. Cryptanalysis of improved Yeh et al.'s authentication Protocol: An EPC Class-1 Generation-2 standard compliant protocol. *IACR Cryptology ePrint Archive*, 2011:426, 2011.

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

[24] Seyed Salman Sajjadi Ghaemmaghami, Afrooz Haghbin, and Mahtab Mirmohseni. Traceability improvements of a new RFID protocol based on EPC C1 G2. *The ISC International Journal of Information Security*, 8(2):105–115, 2016.

[25] Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari, and Mohammad Reza Aref. Analysis of Xiao et al.'s authentication protocol conforming to EPC C1 G2 standard. In *Telecommunications (IST), 2016 8th International Symposium on*, pages 111–116. IEEE, 2016.

[26] Feng Xiao, Yajian Zhou, Jingxian Zhou, Hongliang Zhu, and Xinxin Niu. Security Protocol for RFID System Conforming to EPC-C1G2 Standard. *JCP*, 8(3):605–612, 2013.

[27] Khaled Ouafi and Raphael CW Phan. Privacy of recent rfid authentication protocols. *Lecture Notes in Computer Science*, 4991:263–277, 2008.

[28] Behzad Abdolmaleki, Karim Baghery, Shahram Khazaei, and Mohammad Reza Aref. Game-Based Privacy Analysis of RFID Security Schemes for Confident Authentication in IoT. *Wireless Personal Communications*, 95(4): 5057–5080, 2017.

[29] Shaohui Wang, Sujuan Liu, and Danwei Chen. Security analysis and improvement on two RFID authentication protocols. *Wireless Personal Communications*, 82(1):21–33, 2015.

[30] Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. On the designing of a tamper resistant prescription rfid access control system. *Journal of medical systems*, 36(6):3995–4004, 2012.

[31] Da-Zhi Sun and Ji-Dong Zhong. A hash-based RFID security protocol for strong privacy protection. *IEEE Transactions on Consumer Electronics*, 58(4), 2012.

[32] Eyad Taqieddin. On the Improper Use of CRC for Cryptographic Purposes in RFID Mutual Authentication Protocols. *International Journal of Communication Networks and Information Security*, 9(2):230, 2017.

[33] Lijun Gao, Maode Ma, Yantai Shu, and Yuhua Wei. An ultralightweight RFID authentication protocol with CRC and permutation. *Journal of Network and Computer Applications*, 41:37–46, 2014.

[34] B Westerbaan. Reversing CRC. *Intrepid Blog, Posted Jul*, 15, 2005.

[35] Daewan Han and Daesung Kwon. Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards. *Computer Standards & Interfaces*, 31(4):648–652, 2009.

[36] Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208, 1983.

[37] Michael Burrows, Martín Abadi, and Roger M. Needham. A Logic of Authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, 1990. doi:10.1145/77648.77649.

[38] Li Gong, Roger Needham, and Raphael Yahalom. Reasoning about belief in cryptographic protocols. In *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on*, pages 234–248. IEEE, 1990.

[39] AVISPA. avispa tool. *Available from*, 1th November 2016. URL `www.avispa-project.org`.

[40] Bruno Blanchet and Avik Chaudhuri. Automated formal analysis of a protocol for secure file sharing on untrusted storage. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 417–431. IEEE, 2008.

[41] Peng-yu Cui. An Improved Ownership Transfer and Mutual Authentication for Lightweight RFID Protocols. *IJ Network Security*, 18(6):1173–1179, 2016.

[42] Jiageng Chen, Atsuko Miyaj, Hiroyuki Sato, and Chunhua Su. Improved lightweight pseudo-random number generators for the low-cost rfid tags. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 17–24. IEEE, 2015.

[43] Joan Melià-Seguí, Joaquin Garcia-Alfaro, and Jordi Herrera-Joancomartí. Multiple-polynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags. In *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, pages 3820–3825. IEEE, 2011.

Fereidoun Moradi received his B.Sc. degree in Information Technology from Payame Noor University of Hamedan in 2012 and he received the M.Sc. degree in Information Security at University of Isfahan in 2015. His main research interests include lightweight cryptography and cryptanalysis, RFID security, RFID authentication protocols, IoT security and Data Center Infrastructure Management.

Hamid Mala received his B.Sc., M.Sc. and Ph.D. degrees in Electrical Engineering from Isfahan University of Technology (IUT) in 2003, 2006 and 2011, respectively. He joined University of Isfahan (UI) in September 2011 as an Assistant Professor in the Department of Information Technology Engineering. His Research interests include the design and cryptanalysis of block ciphers, cryptographic protocols and secure multiparty computation.

Behrouz Tork Ladani holds a bachelor in Computer Engineering from University of Isfahan, M.Sc. in Software Engineering from Amir Kabir University of Technology and a Ph.D. in Software Engineering from the University of Tarbiat Modarres. Dr. Tork Ladani joined University of Isfahan in 2005. His research interests are in the areas of Cryptographic Protocols, Access Control, Trust, and Formal verification. He is currently member of executive council of Iranian Society of Cryptology (ISC).

Fariba Moradi currently is a B.Sc. student in Information Technology at Hamedan University of Technology. His research interests include IoT Systems and RFID Security.