Security Improvement in Authentication Protocol for Gen-2 Based RFID System

Liangmin WANG, Xiaoluo YI, Chao LV, Yuanbo GUO

School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China

School of Communication Engineering, Xidian University, Xi’an, 710071, China

School of Electronic Technology, Information Engineering University of PLA, Zhengzhou, 450004, China

doi:10.4156/jcit.vol6.issue1.18

Abstract

The EPC Class-1 Generation-2 specification (Gen-2 in brief) is widely accepted as the standard for RFID tags under grant number ISO18000-6c. However, there are two problems in view of its security authentication protocols. First of all, there is no unified standard for the security requirements, such as which threats should be protected against. Secondly, there is no widely acceptable means to guarantee the security, for the provable security methods are not applicable without using encryption function or hash function. In this paper, we study the security requirements presented in the current Gen-2 based RFID authentication protocols, and summarize an Enhancing Security Standard that contains all 10 security characteristics discussed in literatures [10-17]. We point out the security drawbacks of Chien’s mutual authentication protocol [10], and improve the protocol based on the 10 security requirements. Our improved protocol merely uses CRC and PRNG operations supported by Gen-2 that require very low communication and computation loads. We also develop two methods based on BAN logic and AVISTA to prove the security of RFID protocol. BAN logic is used to give the proof of protocol correctness, and AVISTA is used to affirm the authentication and secrecy properties.

Keywords: RFID System, Authentication Protocol, BAN Logic, Formal Verification

1. Introduction

Radio Frequency Identification (RFID) is a technology which is used to identify remote objects embedded with RFID tags by wireless scanning without manual intervention. RFID has attracted attentions in the past few years and such technology has been deployed in supply chains management systems of some major department stores. To promote the adoption of RFID technology and to support interoperability, EPCglobal proposed one of the most important standards EPCglobal Class-1 Gen-2 RFID specification (Gen-2 in brief) [1], and soon Gen-2 is ratified by ISO and published as an amendment to its 18000-6 standard. The increased functionality of Gen-2 is making this standard a de facto specification for inexpensive tags in the RFID industry. Unfortunately, the Gen-2 pays little attention to the security and privacy issues. Duc [2] has pointed out that Gen-2 is inherently vulnerable to eavesdropping under wireless communication environment. Moreover, the Gen-2 based EPC code is fixed and sent out unscrambled that make the tags easily be tracked.

User privacy may be violated when RFID systems are susceptible to unauthorized attackers [3]. In order to prevent RFID tags from leaking messages, some improved physically and cryptographically schemes are proposed [3-17]. Physical improved schemes, such as tag killing, Faraday cage, active jamming and blocker tag, etc. [3], are too expensive to large-scale use in practice [3]. In cryptographic schemes, the protocol using public-key operations [4-8] is not suitable for low-cost tags due to the limited resource. Hash function can be efficiently implemented in low-power hardware, but it is still beyond current capability of the Gen-2 tag. In particular, Gen-2 merely provides an on-chip 16-bit pseudo-random number generator (PRNG) and a 16-bit cyclic redundancy code (CRC). It does not accept cryptographic Hash function like MD5 and SHA-1. Yksel [9] presented a novel Hash solution with around 1.7K gates, but it doesn’t pass the strict security analysis until now.
Generally speaking, Gen-2 does not support public-key and Hash operations. So Gen-2 based RFID security authentication protocols cannot employ encryption function or hash function. Only lightweight algorithms supported by Gen-2 can be used, such as bitwise operations, CRC operation, or PRNG operation.

We focus on schemes that merely take use of the available algorithms [10-17]. But there is a common problem in these schemes. As we know, provable secure methods cannot be used in Gen-2 based protocols for encryption or hash functions are not supported. Then the problem is how to prove the security of the presented schemes. To solve this problem, the authors [10-17] argued that their protocols protect against the threats in the RFID systems by qualitative analysis. However, two other problems are brought out: which threats should be protected against and how to judge the correctness of the analysis. In this paper, we summarize all the security requirements threats mentioned in the existing Gen-2 based authentication protocols [10-17] as an enhancing standard, and introduce BAN logic based proof and AVISTA verification method as the formal proofs to support the security analysis.

The rest of the paper is organized as follows. Section II introduces the enhanced security standard and reviews current Gen-2 based RFID protocols [12-17]. In Section III, we give a short review of Chien’s protocol [10] and then point out its drawbacks. In Section IV, we improve Chien’s protocol to meet the Enhanced Security Standard. Section V analyses the improved protocol and time complexity. And proves its correctness by using BAN logic, verifies its authentication and secrecy by formal verification toolkit AVISPA. Finally, we conclude the paper in section VI.

2. Related Work and Enhancing Security Standard

In this section, we first investigate the security properties that existing Gen-2 based authentication protocols have discussed. Chien’s protocol [10] was the first protocol conforming to Gen-2 specification. He believed security protocol should have these properties: ① Privacy, ② Anonymity, ③ Resist to reply attack, ④ Resist to DOS attack and ⑤ forward secrecy. Then Wu [11] thought it should have the ability of resisting to ⑥ Backward Security. Besides, Pedro [12] has proposed an 8 security indicators in 2009 which contains ①②③④⑤ in Chien’s protocol and supplement 4 requirements: ⑦ Data Confidentiality, ⑧ Mutual Authentication, ⑨ Forgery Resistance and ⑩ Data Recovery. These 10 security properties contain all the requirements discussed in the related papers [13-17]. Therefore, we think that these 10 security indicators are required in the security protocol for RFID system, and we denote it as Enhancing Security Standard.

Enhancing Security Standard: The Gen-2 based authentication protocol should meet the following 10 security requirements: ① Privacy, ② Anonymity, ③ Resist to reply attack, ④ Resist to DOS attack, ⑤ forward secrecy, ⑥ Backward Security, ⑦ Data Confidentiality, ⑧ Mutual Authentication, ⑨ Forgery Resistance and ⑩ Data Recovery.

<table>
<thead>
<tr>
<th>Tabal 1. Security Properties of Existing Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
</tr>
<tr>
<td>Anonymity</td>
</tr>
<tr>
<td>Resist to reply attack</td>
</tr>
<tr>
<td>Resist to DOS attack</td>
</tr>
<tr>
<td>Forward Secrecy</td>
</tr>
<tr>
<td>Backward Security</td>
</tr>
<tr>
<td>Data Confidentiality</td>
</tr>
<tr>
<td>Mutual Authentication</td>
</tr>
<tr>
<td>Tag Forgery Resist</td>
</tr>
<tr>
<td>Server Forgery Resist</td>
</tr>
<tr>
<td>Data Recovery</td>
</tr>
</tbody>
</table>

Notation: ×: not provided; O: provided; <: partially provided
Secondly, we analyze current Gen-2 based RFID protocols conforming to Enhancing Security Standard in Tab.1. Because the Forgery Resistance is divided to Tag Forgery Resistance and Server Forgery Resistance, we have two in ran 10 and ran 11. The security properties of the related schemes listed in Table 1 were abstracted from the existing publication, in which they reported their own work and discussed the others’ properties. But there are two exceptions. First, security properties in Chien’s Protocol are not met as he claimed and the difference will be illustrated in Section 3. Second, Choi[16] has shown that his scheme is good at Tag Forgery Resist while he doesn’t discuss the Forward Secrecy, Forgery Resist and Anonymity in his paper. And we didn’t find the analysis of Choi[16] in existing publications. So we analyze the protocol in the following phase.

**Analysis of Choi’s Protocol**[16]: Each tag T shares three private values with the server S in Choi[16]: a kill password $PW_{kill}$, an access password $PW_{access}$ and a serial number $sn_T$. Let $R$ denote Reader. The protocol with four communications is shown in Fig. 1. Server Forgery attack could be happened as follows: If an attacker eavesdrops a certain session, he can obtain $M_1, M_2, M_3$ and $M_4$. When T sends a new $M_1'$, the attacker calculates $M_2'$ by formula (1):

$$M_2' = M_1 \oplus M_1' \oplus M_2 = R_{i} \oplus (R_{i} \oplus R_{r}) \oplus PW_{access}$$

$M_3 = M_3$, he sends $M_2', M_3'$ to T. After receiving $M_2', M_3'$, T will compute and obtain $R_{i} = R_{i} \oplus (R_{i} \oplus R_{r})$. Thus, $RNG(R_{i} \oplus R_{r}) = RNG(R_{i} \oplus R_{r})$ holds. Therefore, the attacker forges Server successfully.

Now, knowing $RNG(R_{i} \oplus R_{r}) = RNG(R_{i} \oplus R_{r})$ by Server Forgery attack, and the fact that the plaintext $M_4$ is a constant, attackers can track the tag, then get user location. Thus, tag anonymous is not guaranteed.

In addition, Forward Secrecy and Backward Security are not guaranteed since the key updating is not fulfilled after the mutual authentication, a security breach of an RFID tag will reveal data previously or later transmitted.

---

3. Chien’s Protocol and Security Analysis

In this Section we analyze Chien’s protocol[10] and take the analysis as a preparation for designing protocol with enhancing security. Chien’s protocol is Forward Secrecy in the phase of keys update, but it does not consider the Forward Secrecy in the response phase when messages transmitted from tag to reader. As an earliest Gen-2 based mutual authentication protocol, Chien[10] did not also consider Data Confidentiality, Forgery Resistance and Backward Security. In the following, briefly reviews Chien’s RFID mutual authentication scheme at first.

![Figure 1. Choi’s RFID Authentication Protocol](image-url)
3.1. Initial Setup and Authentication Process

Before being put into use, each RFID tag is assigned a global unique identifier, such as production name, production date, and so on. Chien’s Protocol uses symmetric key to achieve mutual authentication between tags and the server and the symmetric cryptograph system should be initialized. Thus, the protocol consists of two phases: the initialization phase and the authentication phase.

For every tag $Tag_x$, the server randomly selects an initial authentication key $K_{x,0}$ and initial access key $P_{x,0}$. $Tag_x$ initially shares three values ($EPC_x, K_{x,0}, P_{x,0}$) with server $S$, where $EPC_x$ is the EPC code of the tag. $K_{x,0}$ and $P_{x,0}$ will be updated after each successful authentication, and those after the $i$-th successful session are denoted by $K_{x,i}$ and $P_{x,i}$, respectively. $S$ stores ($newK, newP, oldK, oldP, EPC_x, DATA$), where $oldK$ and $oldP$ are the most recent ‘old’ values of $newK$ and $newP$, and $newK$, $newP$, both are initially set to $K_{x,0}$, $P_{x,0}$, respectively. DATA is all other information about the tagged object. Chien’s protocol has four passes shown in Fig. 2. The detailed scenarios are described as follows:

1. $R \rightarrow Tag_x$: $1N_1$, where $N_1$ is a random nonce.

   $Tag_x$: Compute $M_1 = CRC(EPC_x || N_1 || N_2) \oplus K_{x,j}$, where $N_2$ is a random nonce.

2. $Tag_x \rightarrow R$: $M_1$. $R \rightarrow S$: $M_1, N_1$

   $S$: Search all ($newK, oldK, EPC_x$) and compute $I_{old} = M_1 \oplus oldK$, $I_{new} = M_1 \oplus newK$, then verify the tag by checking whether $I_{new}$ or $I_{old} = CRC(EPC_x || N_1 || N_2)$.

3. $S \rightarrow R$: $M_2$, DATA

   $S$: Compute $M_2 = CRC(EPC_x || N_2) \oplus newP$ or $M_2 = CRC(EPC_x || N_2) \oplus oldP$ depending on which value ($newK$ or $oldK$) satisfies the verification equation in the previous step. Then update:

   $oldK \leftarrow newK$, $oldP \leftarrow newP$, $newK \leftarrow PRNG(oldK)$, $newP \leftarrow PRNG(oldP)$.

4. $R \rightarrow Tag_x$: $M_2$

   $Tag_x$: Verify $R$ by checking whether $M_2 \oplus P_{x,j} = CRC(EPC_x || N_2)$. If $R$ satisfies this verification equation, update $K_{x,j} \leftarrow PRNG(K_{x,j})$, $P_{x,j} \leftarrow PRNG(P_{x,j})$.

Figure 2. Chien’s protocol

3.2. Security Analysis
Chien assumed that the channel between server and reader is secure, while the channel between reader and tags is insecure and subject to eavesdropping or modification. When considering the Enhancing Security Standard, we will find that Chien’s protocol does not meet Tag Forgery Resistance, Anonymity, Data Confidentiality, Forward Secrecy and Backward Security. The details are shown in Proposition 1~5 as follows:

**Proposition 1.** The leakage of the value of \( \text{CRC}(EPC_{\text{sec2I}}) \oplus K_{x,i} \) causes Tag Forgery Resistance not guaranteed.

**Proof:** From the assumptions of Chien’s protocol, we know that reader and tag communicate via an insecure channel. Thus, the exchanged plaintext \( M_1 \) can be obtained by an attacker. By using the lemma of CRC:[18](where \( n \) is the bit length of B):

\[
\text{CRC}(A \| B) = \text{CRC}(A \oplus B) = \text{CRC}(A_{\text{sec8}}) \oplus \text{CRC}(B)
\]

and \( M_1 \), the attacker gets Eq.(2):

\[
\text{CRC}(EPC_{\text{sec2I}}) \oplus K_{x,i} = M_1 \oplus \text{CRC}(N_{1(\cdot)}) \oplus \text{CRC}(N_{2(\cdot)})
\]  

(2)

Since he knows \( N_1 \) and \( N_2 \), he calculates \( \text{CRC}(N_{1(\cdot)}) \) and \( \text{CRC}(N_{2(\cdot)}) \), then obtains the value of \( \text{CRC}(EPC_{\text{sec2I}}) \oplus K_{x,i} \) by Eq.(2).

Therefore, the attacker can pre-compute the value \( M_1' \) before the next successful authentication as follows:

\[
M_1' = \text{CRC}(EPC_{\cdot} \| N_1 \| N_2') \oplus K_{x,i}
\]

Then S will be spoofed successfully when verifying. Hence the protocol does not guarantee Tag Forgery Resistance.

**Proved #**

**Proposition 2.** Tag Anonymity of Chien’s protocol not guaranteed due to a constant value.

**Proof:** From Proposition 1, we know an attacker can obtain the value of \( \text{CRC}(EPC_{\text{sec2I}}) \oplus K_{x,i} \).

Note that the value of \( \text{CRC}(EPC_{\text{sec2I}}) \oplus K_{x,i} \) is a constant, that is, the message \( M_1 \) can be transformed into a constant. When the attacker traces the constant, tag tracing happens, and user location is revealed. Therefore, Anonymity is not guaranteed.

**Proved #**

**Proposition 3.** Chien’s protocol has no Data Confidentiality, Forward Secrecy and Backward Security.

**Proof:** From two continuous sessions eavesdropped, the attacker can obtain the following four values:

\[
M_{1i} = \text{CRC}(EPC_{\cdot} \| N_{1i} \| N_{2i}) \oplus K_{x,i}
\]

(3)

\[
M_{2i} = \text{CRC}(EPC_{\cdot} \| N_{2i}) \oplus P_{x,i}
\]

(4)

\[
M_{1(i+1)} = \text{CRC}(EPC_{\cdot} \| N_{1(i+1)} \| N_{2(i+1)}) \oplus K_{x,i+1}
\]

(5)

\[
M_{2(i+1)} = \text{CRC}(EPC_{\cdot} \| N_{2(i+1)}) \oplus P_{x,i+1}
\]

(6)

By using the lemma of CRC in Proposition 1, the attacker calculates (3) \( \oplus \) (5), Thus

\[
K_{x,i} \oplus K_{x,i+1} = M_{1i} \oplus M_{1(i+1)} \oplus \text{CRC}(N_{1i} \| N_{2i}) \oplus \text{CRC}(N_{1(i+1)} \| N_{2(i+1)})
\]

(7)
holds. Since he knows $M_{li}$, $M_{li+1}$, $N_{li}$, $N_{li+1}$, and $N_{2li+1}$, he obtains the value of $K_{s,j} \oplus K_{r,li}$, then the length $l$ of $K_{s,j}$ is revealed.

The attacker can obtain a $K$ by $PRNG(K) = K \oplus C$. At least, $K_{s,j}$ satisfies. Thus, we may regard that $K_{s,j}$ is revealed. Now, by using $K_{s,j}$, Eq.(3) and Eq.(5), he obtains $CRC(EPC_{s \oplus j})$. Likewise, he obtains $P_{x,i}$ and $CRC(EPC_{s \oplus i})$ from Eq.(4) and Eq.(6).

By using $K_{s,i} = PRNG(K_{s,i})$, the attacker calculates $K_{s,j}$ ($j \geq i+1$). Then he can pre-compute the value $M_{ik}^*$ when receiving a new $N_i$ in the $(k+1)$-th $(k \geq i+3)$ session as follows:

$$M_{ik}^* = CRC(EPC_i \| N_1 \| N_{2i} \| x_{s,k}) \oplus K_{s,k}$$

and tag-to-reader authentication can be performed successfully. The protocol hence does not meet Tag Forgery Resistance.

Similarly, the attacker gets $P_{x,k}$ by using $P_{x,i} = PRNG(P_{x,i})$, and pre-computes the value $M_{2k}^*$ in $(k+1)$-th session as follows:

$$M_{2k}^* = CRC(EPC_k \| N_2 \| P_{s,k})$$

Then reader-to-tag authentication will be performed successfully. Hence Server Forgery Resistance is not met. Furthermore, this attack will make authentication key and access key update illegally. As a result, Data Confidentiality is not guaranteed.

**Proposition 4.** If the value of $K_{s,j}$ and $P_{x,i}$ reveals, it will make Forward Secrecy not guaranteed.

**Proof:** From Proposition 3, the attacker can know $K_{s,j}$ and $P_{x,i}$ by two continuous session. Besides, when EPC code is revealed, the attack can also obtain $K_{s,j}$ and $P_{x,i}$ as follows:

By using Eq.(8):

$$K_{s,j} = CRC(EPC_i \| N_1 \| N_{2i}) \oplus M_{li}$$

which is changed from Eq.(3), and the plaintext $N_{1i}$, $N_{2i}$ and $M_{li}$, the attacker obtains $K_{s,j}$; Likewise, he obtains $P_{x,i}$ by changing Eq.(4).

When knowing $K_{s,j}$ and $P_{x,i}$, he could decrypt the messages transmitted in the $(i+1)$-th session. Thus, Forward Secrecy is not guaranteed.

**Proposition 5.** Backward Secrecy is not guaranteed in Chien’s protocol.

**Proof:** If a tag is compromised after $i$-th session, an attacker obtains $EPC_i$, $K_{s,j}$ and $P_{x,i}$. Then he obtains $K_{s,j}$ and $P_{x,i}$ ($i \geq i+1$) by using $K_{s,i+1} = PRNG(K_{s,i+1})$ and $P_{x,i} = PRNG(P_{x,i})$. Thus, the messages transmitted in the $(i+1)$-th session can be decrypted. Therefore, the protocol does not meet Backward Secrecy.

**4. Improved Chien’s Protocol**

From the analysis in section III, we find that Chien’s protocol did not well satisfy the Enhancing Security Standard. To solve the problem, in this section we presents an improved version which is shown in Fig.3. The details are as follows.

1. $R \rightarrow Tag_{s,i} : N_1$, where $N_1$ is a random nonce.

   $Tag_{s,i} : Compute : M_1 = N_2 \oplus K_{s,j}$, $M_2 = CRC(K_{s,j} \| EPC_i \| N_1 \| N_{2i}) \oplus K_{s,j}$, where $N_2$ is a random nonce.

2. $Tag_{s,i} \rightarrow R : M_1 \rightarrow S : M_1, N_1$
5. Analysis of the Improved Protocol and the Formals

We present a detailed security analysis to show that the improved protocol meets the Enhancing Security Standard. Then we prove the correctness of the improved protocol by formal method based on BAN logic. Moreover, we verify the authentication and secrecy by formal verification with AVISPA toolkit.

5.1. Analysis of the Improved Protocol

In Section IV, we analyze Chien’s protocol and show that the protocol does not meet 5 properties. Now we show the improved protocol basically meets these 5 properties.

Tag Anonymity: The location privacy of tag holders can be revealed when the tag’s answers are constant. Specifically, location privacy can be more significant when a certain tag is exposed to long-term tracking. It is therefore crucial to make all the information sent by the tag anonymous. As we have seen, in the mutual-authentication stage, the tag generates a nonce, by which all the transmitted messages are encrypted. In addition, the attack like that in Proposition 2 can not succeed without the nonce. Tag anonymity is guaranteed and privacy location of the tag owner is not compromised.
Forward Secrecy: Forward security is the property that guarantees the security of messages sent in this session will be valid in the next session. Since the key updating is fulfilled after the mutual authentication, and the attacker can not obtain $K_{i,j}$ or $P_{s,i}$ by using the method in Proposition 4, a security breach of an RFID tag will not reveal data previously transmitted.

Backward Security: Backward Security is the property that guarantees the security of messages sent in future session when the tag is compromised in current session. In Chien’s protocol, an attacker is prone to update $K_{i,j}$ and $P_{s,i}$ after compromising a tag shown in Proposition 3. The improved scheme provides Backward Security if an attacker misses $N_z$ just once in a single successful authentication session after compromising the tag’s secret. That is, if the attacker does not have access to the value of $N_z$ once that is needed to refresh $K_{i,j}$ and $P_{s,i}$, then he cannot compute the new keys and know future transactions.

Tag Forgery Resistance: If a weak attacker intend to forge the tag, it must be able to pre-compute a valid response $(M_1, M_2)$ to a reader query. However, it is hard to compute such a valid pair without knowledge of $N_z$, so the situation in Proposition 1 will not happen. When an attacker obtains two continuous sessions like that in Proposition 3, he will not get the value of $K_{i,j} \oplus K_{s,i}$ or $P_{s,i} \oplus P_{s,i}$ because of the unknown $N_z$. Thus, $K_{i,j}$ and $P_{s,i}$ are unknown to the attacker. Therefore, the improved protocol can provide Tag Forgery Resistance. Of course, a strong attacker is able to clone a tag.

Server Forgery Resist: A legitimate server responds with a message $M_3$ to a tag in order to enable the tag to authenticate the server. A strong attacker cannot create a valid $M_3$ without knowing $P_{s,i}$. Actually, $P_{s,i}$ is shared between Tag and S and not yet exchanged in this $(i+1)$-th session. Additionally, it’s not revealed in the prior $i$ times which has been discussed when analyzing Tag Forgery Resistance. Hence, our protocol resists such an attack.

Data Integrity: A portion of the tag’s memory is rewritable, so modifications are possible. In this part of the memory, the tag stores the EPC code $EPC_i$, authentication key $K_{i,j}$ and access key $P_{s,i}$. If an attacker does succeed in modifying this part of the memory, the reader will not recognize the tag. Except physical attacks, Server Forgery attack will result in such modification by illegally updating $K_{i,j}$ and $P_{s,i}$. However, the improved protocol can resist this attack shown above. Therefore, Data Integrity is guaranteed.

From analysis with respect to these 5 properties above, we find that the improved protocol have 5 properties which are not satisfied in Chien’s protocol. Next, we show that the improved protocol also has the properties which are obtained in Chien’s protocol.

Privacy: EPC code must be kept secure to guarantee user privacy. The messages containing the code are $M_1$ and $M_3$ which can be eavesdropped by an attacker. However, EPC code is encrypted by a nonce $N_z$ or $K_{s,i}$ or $P_{s,i}$, and an attacker will not obtain these three values which were discussed above. Therefore, only an authorized server and reader are able to access the information associated with the tag.

Resist to Reply attack: An eavesdropper could store all the messages exchanged between the reader and the tag. Then he could try to impersonate a reader, and re-send the messages seen in any of the previous protocol. It may seem that this could cause loss of synchronization between sever and tag, but this is not the case due to the challenge-response technology and the freshness of the random number $N_1$ and $N_z$ per session.

Resist to DOS attack: If an attacker prevents the fourth flow from reaching the tag, the shared secrets of the server and tag might be out of synchronization, because the server will update the shared secrets while the tag will not. However, in the improved protocol, the server maintains both the old and new values of $K_{i,j}$ and $P_{s,i}$ for Tag in its database, so the server can resynchronize with the tag in such situation. Additionally, although Server Forgery attack can also desynchronize the shared keys, the improved protocol can resist this attack.
Data Recovery: The interception or blocking of messages is a DoS attack which prevents tag identification. When dismissing messages, S can still recover the message thanks to the storage of $K_{old}$ and $P_{old}$ in its database.

Mutual Authentication: In the improved protocol, server identifies tag by verifying $\_2_{\text{ki}}N$ in $M_1$, $M_2$, and tag authenticates server by verifying $\_2{}_{x_i}P$ in $M_3$, which will be analyzed in AVISPA tool in the next subsection.

From the analysis above, we can see that the improved protocol basically meets all the 10 requirements in the Enhancing Security Standard. And with the consideration of Tab.1, we think the protocol may be the first protocol with these 10 security properties. Moreover, the improved protocol is very low in the communication and computation loads. Compared with the original protocol, the improved protocol has the same time of communication, CRC operation and PRNG operation, and only 3 times XOR operation and 1 time Concatenation operation increased in the tag, $3n$ and $n$ increased in the sever correspondingly, where $n$ is the tag amount in the RFID system.

5.2. Formal Proof of Correctness

It’s very difficult to ensure the security of a protocol. Non-formal analysis, such as the security analysis in 5.1, can only discover whether the known threats existed, rather than analyze cryptographic protocols comprehensively and objectively. As a kind of formal analysis methods, BAN logic[19] can not only discover the current attacks in cryptographic protocols, but also find out flaws comprehensively and profoundly. Therefore, the formal proof of correctness of the improved protocol based on BAN logic is shown in this subsection.

There are four phases in BAN logic, including Establishment of Idealized Model, Initiative Assumptions, Establishment of Security Goals and Protocol Analysis. BAN logic consists of 19 logical rules. The only six rules used in the paper are as follows:

1. **Message-meaning rule:**
   
   $P \models Q \iff P, P \models \{X\}_k$  
   
   $P \models Q \iff P \models \neg X$  
   
   $P \models Q \iff P \models \neg X$  

2. **Nonce-verification rule:**
   
   $P \models Q \iff P \models P \models \neg X$  

3. **Jurisdiction rule:**
   
   $P \models Q \iff X, P \models Q \models X$  

4. **Belief rule:**
   
   $P \models (X, Y)$  

5. **Freshness rule:**
   
   $P \models \#(X)$  

First phase: Idealized the improved protocol

The purpose of this step is to transform the improved protocol into an ideal one for the following proof. Due to the secure channel between sever and reader, we regard that they have the same security level. Let B donate sever and reader. Ignoring the plaintext transmitted, the protocol can be idealized as follows:

**Message 1:**

$\text{Tag}_s \rightarrow B: \{N_2\}_{k_s} \rightarrow \{\text{Tag}_s \rightarrow EPC_s, N_2\}_{k_s}$

**Message 2:**

$B \rightarrow \text{Tag}_s: \{EPC_s, N_2, \text{Tag}_s \rightarrow B\}_{k_s}$

Second phase: Initiative Assumptions

This step is to abstract the initial assumptions from the improved protocol, which is the premise of the success of each protocol. Assumptions about the initial state are written below.

$A_1$: $\text{Tag}_s \models \text{Tag}_s \rightarrow B$  

$A_2$: $B \models \text{Tag}_s \rightarrow B$
A1: \( B \vdash \text{Tag}_x \Rightarrow \text{EPC}_x \) \hspace{1cm} A4: \( \text{Tag}_x \vdash B \Rightarrow \text{EPC}_x \) 

A2: \( \text{Tag}_x \equiv (N_2) \) \hspace{1cm} A5: \( B \equiv (N_1) \)

The first two assumptions, A1 and A2, are for the shared secrets. A3 means that B believes \( \text{Tag}_x \) has jurisdiction over \( \text{tEPC} \) and A4 means that \( \text{Tag}_x \) believes B has jurisdiction over \( \text{sEPC} \). The last two mean that \( \text{Tag}_x \) believes \( N_2 \) is fresh and B believes \( N_1 \) is fresh.

**Third phase: Establishment of security goals**

The goals of the protocol are \( B \vdash \text{EPC}_x \) and \( \text{Tag}_x \vdash \text{EPC}_x \). The actual meaning is that they ensure each other’s legality through mutual authentication.

**Fourth phase: Protocol Analysis**

The logic rules and the assumptions will be used by the messages in the first phase to discover the final beliefs held by the parties in the protocol. If the final beliefs contain the goals of the protocol, the protocol is integrated; else, the protocol has flaws. The proof is as follows:

1) \( B \vdash (\text{Tag}_x \leftarrow \text{EPC}_x, N_2) \) \hspace{1cm} /*For Message 1*/

2) \( B \vdash (\text{Tag}_x \leftarrow \text{EPC}_x, N_2) \) \hspace{1cm} /*For 1), by A2, (P1)*/

3) \( B \equiv (\text{Tag}_x \leftarrow \text{EPC}_x, N_2) \) \hspace{1cm} /*By A6, (P6)*/

4) \( B \vdash (\text{Tag}_x \leftarrow \text{EPC}_x, N_2) \) \hspace{1cm} /*For 2), 3), by (P3)*/

5) \( B \vdash (\text{Tag}_x \leftarrow \text{EPC}_x) \) \hspace{1cm} /*For 4), by (P3)*/

6) \( B \vdash (\text{Tag}_x \leftarrow \text{EPC}_x) \) \hspace{1cm} /*For 4), (P3)*/

7) \( B \vdash (\text{Tag}_x \leftarrow \text{EPC}_x) \) \hspace{1cm} /*For 5), by A3, (P3)*/

By the same token, we can obtain \( \text{Tag}_x \equiv \text{EPC}_x \) and \( \text{Tag}_x \equiv \text{EPC}_x \) from Message 2.

As shown above, the final beliefs contain the proof goals \( B \equiv \text{EPC}_x \) and \( \text{Tag}_x \equiv \text{EPC}_x \). Thus, the improved protocol can effectively achieve the correctness of mutual authentication between B and \( \text{Tag}_x \).

**5.3. Formal Verification with AVISPA**

The AVISPA (Automated Validation of Internet Security Protocols and Applications) \(^{[20]}\) is a toolkit for the automated validation of security-sensitive protocols and applications. It provides a modular and expressive formal language for specifying protocols and their security properties, and integrates different back-ends that implement a variety of state-of-the-art automatic analysis techniques. The security protocols specifications are written in the AVISPA’s High-Level Protocol Specification Language (HLPSL) \(^{[21]}\). We validate standard authentication and secrecy goals of the improved protocol by using AVISPA model.

1) **Specifying the protocol:** In our protocol model described in HLPSL, there are three basic roles gen_R, gen_T and gen_S which represent the participant Reader, Tag and Server respectively. In this place, we only present one of the basic roles S shown in Fig. 4 as an example. S waits to receive \( M_1, M_3 \) and \( N_1 \) from R and then sends \( M_1, DATA \) to R. The \( DATA \) is omitted in the HLPSL module. At the same time the state St of S will be changed from 0 to 1. Here, the type declaration channel (dy) stands for the Dolev-Yao intruder model. Under this model, the intruder has full control over the network, such that all messages sent by the agents will go to the intruder. The intruder may intercept, analyze, and/or modify messages as far as he knows the required keys, and send any message he composes to whoever he pleases, posing as any other agent.
Security Improvement in Authentication Protocol for Gen-2 Based RFID System
Liangmin WANG, Xiaoluo YI, Chao LV, Yuanbo GUO
Journal of Convergence Information Technology, Volume 6, Number 1. January 2011

role gen_S(R, T, S : agent, 
   Snd, Rcv : channel (dy), 
   Kxi : symmetric_key, 
   EPC : text, 
   CRC : hash_func)
   played_by S def= 
   local St               : nat, 
   RcN2             : message, 
   RcM2             : message, 
   RcN1, P             : text
init St := 0
transition 
   rcv_from_reader. St  = 0 /\ 
   Rcv(R.S.xor(RcN2'.EPC). 
   RcM2'.RcN1') =|>
   St':= 1 /\ P' := new() /\ 
   Snd(S.R.xor(CRC(EPC.RcN2'),P')) /\ 
   request(S,T,auth_s_t_n1,RcN1') /\ 
   witness(S,T,auth_t_s_n2,RcN2')
end role

Figure 4. Role of S

We analyze following properties which are in the goal section as shown in Fig. 5. The current version of HLPSL supports the standard authentication and secrecy goals. This is, however, sufficient to specify a large number of problems. For our protocol, we verify two weak authentications. S and T have the mutual authentication property through the authentication of S on T and T on S.

goal
   weak_authentication_on auth_t_s_n2
   weak_authentication_on auth_s_t_n1
   secrecy_of sec_s_t_epc
end goal

Figure 5. Analysis goals of the model

2) Analysis of results: The back-end OFMC is chose for an execution test and a bounded number of sessions model checking. The depth for the search is eight and output of model checking results are shown in Fig. 6. From Fig. 6, we can conclude that the proposed protocol is secure under the test of AVISPA using the OFMC back-end with bounded number of sessions.

% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/abc/avispa-1.1/testsuite/results/gen2.if
GOAL

as_specified
BACKEND
OFMC
COMMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 32.93s
visitedNodes: 20490 nodes
depth: 8 plies

Figure 6. Results reported by the OFMC back-end

6. Concluding Remarks

We point out there are two problems of security protocol in Gen-2 based RFID system: which security properties should be required and how to prove the properties claimed by the schemes. In this paper, firstly, we propose an Enhancing Security Standard including 10 security indicators presented in current Gen-2 based RFID authentication protocols. Secondly, we analyze Chien’s protocol, and then present an improved protocol, which is up to the Enhancing Security Standard. The improved protocol still uses CRC operation and PRNG operation supported by Class-1 Generation-2 standard. Analysis shows that the improved protocol basically meets the Enhancing Security Standard. Thirdly, we introduce two types of formal proofs of correctness, mutual authentication and secrecy of the improved protocol. In short, we proposed a security standard, present a scheme, then argue that the scheme is up to the standard by qualitative analysis, formal proving and verification. Obviously, our attribution is limited to a practical solution. We wish the paper will attract the attention of these two problems, and
then some general contents, such as the sufficiency of the security standard, the theories of formal proofs and the verification toolkit specially developed for RFID, will be studied in the future.

The work of this paper is supported by National Natural Science Foundation of China(NSFC: 60703115, 60633020), China Postdoctoral Science Foundation (CPSF: 20070420955), Natural Science Foundation of Jiangsu Province(BK2007560) and Postdoctoral Science Foundation of Jiangsu Province(0702003B), and the author Liang-min WANG is supported by China Scholarship for visiting scholarship under grant 200832053, Special Funding Scheme of China Postdoctoral Science Foundation under No.200801357, "Qing Lan Project" for Excellent Youth Scholars of Jiangsu Province and Talents Foundation of Jiangsu University under No.07JDG080. And the code was programmed by LV Chao, a PHD student at School of Electrical & Electronic Engineering, Nanyang Technological University.

10. References

Security Improvement in Authentication Protocol for Gen-2 Based RFID System
Liangmin WANG, Xiaoluo YI, Chao LV, Yuanbo GUO
Journal of Convergence Information Technology, Volume 6, Number 1. January 2011


Liang-min WANG received his B. S. degree in computational mathematics in Jilin University, Changchun, China, in 1999, and the Ph.D degree in Cryptology from Xidian University, Xi’an, China, in 2007. He has also worked with Prof. Alex KOT for a year in the School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore. Currently, he is an associate professor in the School of Computer Science and Communication Engineer, Jiangsu University, Zhenjiang, China. Now his research interests include security protocols and wireless sensor networks. Dr. WANG is a senior member of Chinese Computer Federation and a member of Chinese Cryptology Federation. He is also a member of AICIT Conference.

Xiaoluo Yi received his B.S. degree in Information and Computing Science from Jiangsu University, China, 2008/06. His interests include RFID security and application, and sensor network security. Currently, he is studying as a Master student in Computer Science and Its application in the School of Computer Science and Communication Engineering, Jiangsu University, China.