A Secure Mutual Authentication Protocol for Low-cost RFID System

N.W. Lo, Tzu-Li Yang and Kuo-Hui Yeh
*National Taiwan University of Science and Technology
Taiwan, R.O.C.*

1. Introduction

With extended data storage space and advanced wireless transmission capability, Radio Frequency IDentification (RFID) is rapidly deployed to replace barcode position in our daily lives and considered as the next generation identification technology in ubiquitous communication environment. The most important key factor of RFID technology is to enable systems with the ability to automatically identify labeled objects without the constraint of line of sight. RFID technology is a well known AIDC (Automatic Identification and Data Capture) technology to provide the benefits including contactless read, long transmission range and transaction time saving (Garfinkel & Rosenberg, 2005). Most of innovative applications designed for RFID system can be divided into following classes such as asset management, tracking, authenticity verification, matching, process control, access control, automated payment and supply chain management (Karygiannis et al., 2007).

In spite that the adoption of RFID technology becomes popular in a board range of applications, the cost of a RFID tag is still too expensive to be fully adopted by logistic and retailer industries. Even though from the logistic and retailer industries point of view, to label RFID tags on all sale items is still cost-prohibitive under the current price of a passive RFID tag. Nevertheless, the convenience of RFID technology still has a great attraction for inventory management. For example, in 2005, Wal-Mart which is the biggest retailer in America declared a new policy to force its top 500 suppliers to adopt RFID technology for inventory management; otherwise, Wal-Mart will deny new transaction contracts from those who do not comply this new policy. Because of this policy, all top 500 suppliers start to apply RFID tags onto their merchandises by spending and absorbing extra RFID cost. In contrary, the introduction of RFID technology can provide great benefits for Wal-Mart to control logistic process accurately, replenish empty stock efficiently and lower space requirement for goods storage.

Although the widespread use of RFID technology makes human life better than past, the security invasion and user privacy disclosure are still concerned by individuals and organizations. For example, in 2006, Metro AG which is the biggest supermarket chain store in Germany used the RFID technology to not only automatically manage production and stock but also help customers search their target items quickly. Metro AG gave VIP cards to the top 10% customers and based on the historical shopping behaviors of a VIP customer to recommend products nearby the customer's current location. However, Metro AG did not notify VIP customers that the VIP card is embedded with RFID. Three months later, a VIP

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

member curiously disassembled his card and recognized the RFID secret of the VIP card. About ten thousand members' location privacy is at risk of disclosure because the unique customer number stored in each VIP card can be easily read by a malicious stalker using a handheld RFID reader.

As we mentioned above, the RFID technology faces serious security threats and privacy concern (Juels et al., 2005; Weis, 2003). Wireless communication and cost-down consideration on RFID systems are the two main factors that cause these security threats. In RFID operation environment, a passive RFID tag must be powered and triggered by a broadcast signal through the forward channel from a RFID reader, and the reader receives the response from the tag via the backscatter channel. An adversary may capture transmitted messages between reader and tag easily with wireless eavesdropping device. Furthermore, an adversary can utilize the captured messages to invoke other attacks such as object tracking, tag compromise and tag impersonation. In short, the concerns on information security and privacy protection will impede the future development of RFID technology. In order to secure data integrity, data confidentiality, non-repudiation, and availability of a RFID system, a straight forward thought is to apply existing authentication protocols on wireless networks. However, due to the nature of restricted computation ability and limited memory storage of a low-cost passive RFID tag, it is difficult to implement a secure or robust RFID system with powerful cryptographic operations such as RSA, DES, and AES (Datasheet Helion Technology, 2005) as existing authentication protocols did.

In the past five years, many researchers had proposed ideas to protect data security and user privacy (Weis et al., 2003; Lo & Yeh, 2007) on RFID systems. These researches use powerful cryptographic operations (Feldhofer et al., 2004; Kumar & Paar, 2006) such as symmetric key encryption, public key infrastructure and one-way hash function to prevent information leakage. Although those operations can provide strong protection to defend against malicious attacks, low-cost RFID tags with highly constrained resource are not able to carry out expensive cryptographic primitives to perform strong authentication. In fact, a passive tag can only contain 5K – 10K gates; on the contrary, a cryptographic primitive requires 250 – 3K gates. Hence, powerful encryptions are hardly possible to be built in a passive tag in the near future. In order to comply with the resource constraint, a few new authentication protocols with lightweight encryptions (Peris-Lopez et al., 2006; Chien, 2007; Yu et al., 2007; Juels, 2005) are invented to fit the physical limitation of a passive tag. However, those proposed schemes cannot provide enough security level in general; more specifically, they cannot prevent all major or general attacks such as eavesdropping, tracking, replay attack and Denial of Service, and preserve the forward secrecy of tagged object at the same time. Therefore, in order to successfully defend against those security threats, we propose a new secure mutual authentication protocol for low-cost RFID systems, named as SMAP-LRS, to achieve higher security level and be compatible with the hardware restriction of passive RFID tag at the same time. The design of SMAP-LRS protocol adopts simple cryptographic operations to comply with existing RFID standards. In addition, a bit flag mechanism is introduced in our scheme to resolve the Denial of Service attack and save the memory space for protocol implementation at backend server.

The rest of this chapter is organized as follows. Section 2 reviews previous work on RFID authentication protocol. Next, we propose a new authentication scheme for low-cost RFID system in section 3. The security analysis of our scheme is presented in section 4. Finally, we summarize our conclusion in section 5.

2. Related work

In recent years, the vast literatures have addressed the security and privacy concerns on the use of RFID tags. Based on the type of encryption primitive used on RFID system, we classify RFID authentication protocols into four classes. The first class of RFID authentication protocol is hash-based. Most of those schemes only use hash function for data encryption. In 2003, Weis et al. (Weis et al., 2003) proposed a new authentication protocol for RFID system using hash function to achieve data security and user privacy. In their hash-based access control mechanism, the tag does not change its identification in authentication sessions. An adversary can easily trace his target RFID object by eavesdropping the same ID transmitted through air interface. Ohkubo et al. (Ohkubo et al., 2003) developed a secure authentication protocol based on hash chain mechanism. This scheme provides indistinguishability and forward security. Through their scheme, a RFID tag can generate a responding message whose content is indistinguishable from truly random value to achieve indistinguishability. At the same time, the property of forward security is preserved because even if an adversary gathers information from transmitted messages during authentication sessions and the secret data stored in a compromised tag, the adversary still cannot derive the secret information of the tag before it is compromised. However, this scheme cannot resist replay attack. Henrici & Müller (Henrici & Müller, 2004) proposed a novel authentication which is based on hash function to provide anonymity and location privacy by updating tag identification in each session. Nevertheless, the tag always responds reader query with the same hashed value of identification before the tag successfully updates its current identification at the end of authentication session. This security flaw allows an attacker to track a specific tag by eavesdropping.

The second class of RFID authentication protocol utilizes hash function and random-number generator. Weis et al. also proposed another authentication protocol in their paper (Weis et al., 2003) by using randomized access control and hash function. The advanced scheme certainly provides stronger anonymity property than the previous hash-based scheme they derived. However, the backend server does not update the database information at all after authentication. An adversary can eavesdrop the transmitted messages between a reader and tags, as well as injecting arbitrary messages into the communication channel. In other words, the adversary can impersonate the original tags and send arbitrary message to backend server until the next authentication session. An and Oh (An & Oh, 2005) developed a new authentication protocol which is based on hash function and random number generator. Although authors claimed that their scheme provide data security in different databases, this scheme cannot prevent replay attack and tag tracking. Rhee et al. (Rhee et al., 2005) proposed a challenge-response protocol for authentication to enhance the anonymity and resist replay attack via hash function and pseudo-random number generator. Unfortunately this scheme cannot efficiently support forward secrecy when it encounters adversary attacks. Once the tag is compromised, the adversary can derive or identify the past transmitted messages through revealed secret information from the tag. Kim et al. (Kim et al., 2006) proposed a new scheme which generates stream blocks to update the shared secret information between tag and backend server in an authentication process. Their scheme supports tag anonymity and relay attack resistance. However, the identification of tag can be calculated by using XOR operation with the transmitted message consisting of E_{ID} and random value R2′; the adversary can use the specific characteristic to track a tag virtually anywhere. A new authentication protocol which is based on AES encryption primitive is designed by Feldhofer et al. (Feldhofer et al., 2004). Although the scheme reaches the strongest level of security requirement, it is not suitable for systems using low-cost RFID tags since the computing capability of a passive tag at present cannot support such large computation workload as the AES encryption process requires.

The third class of RFID authentication protocol adopts lightweight encryption primitive. Those schemes utilize the common bit-wise arithmetic operations to perform data encryption task. By doing so, both the low-cost requirement and security robustness for a passive RFID tag can be achieved simultaneously. In 2006, Peris-Lopez et al. (Peris-Lopez et al., 2006) proposed a series of authentication protocols which involve simple bit-wise operations such as AND, OR, XOR and addition mod 2^m. These schemes are very cost-effective and attractive to RFID systems with resource-constrained tags. Nevertheless, Li et al. (Li & Wang, 2007; Li & Deng, 2007; Li, 2008) showed that there are two vulnerabilites, de-synchronization and full-disclosure attack, in these schemes proposed by Peris-Lopez et al. However, Li-Wang's enhancement scheme still cannot successfully remedy these two security weaknesses as shown by Chien and Hwang (Chien & Huang, 2007). In 2007, Chien (Chien, 2007) proposed a new lightweight authentication protocol and corrected the drawback of Peris-Lopez's schemes by applying bit-rotation function. Even though Chien claimed his scheme can provide more robust security features than Peris-Lopez's schemes, the Chien's scheme still is vulnerable in subtle situations. For example, if the *IDS* value of Chien's scheme does not update in a period of time, the tag sent the same *IDS* response to reader might be tracked by adversary.

The forth class of RFID authentication protocol complies with the EPCglobal standard. Sarma et al. (Sarma & Engels, 2003) developed a mutual authentication scheme using pseudo-random number generator only. Although the scheme meets the implementation requirements of the EPCglobal standard, it suffers the problem of tag identification disclosure. Chien and Chen (Chien & Chen, 2007) proposed an enhanced EPCglobal complied authentication protocol. However, Lo and Yeh (Lo & Yeh, 2007) showed that Chien and Chen's scheme cannot provide forward security and suffer heavy computation workload at the backend server. Correspondingly, Lo and Yeh proposed a new authentication scheme to improve user privacy and data security.

3. Proposed SMAP-LRS protocol

As we mentioned above, the research in the past does not guarantee enough security for RFID system; previously proposed schemes only prevent a few specific types of security attacks. To implement encryption module in a passive RFID tag still requires lots of gates and space. In consequence, the cost of tag becomes more expensive and the tag needs more power to drive. Strong encryption operations, as more computing time required, might also delay tag response time. Most of passive tags cannot afford the resource demand from strong encryption primitive at present. The EPCglobal Class1 Gen2 tag standard only defines CRC function and pseudo-random number generator for tag to operate. Although some lightweight encryption primitives for RFID tags are introduced and claim that they are adaptive to the resource constraint of RFID tag (Duc et al., 2006; Juels, 2005; Karthikeyan & Nesterenko, 2005), most of them have not demonstrated that these schemes can really work on passive tags to achieve security requirement. Poschmann et al. (Poschmann et al., 2007; Poschmann et al., 2006) had proposed a new hash function requiring less number of gates to supply the need of lightweight encryption primitives for RFID authentication. Although this method seems to be lightweight enough to fit in a low-cost RFID tag, the security strength of this hash function still remains as an open question. In the following, we introduce a newly designed authentication protocol, which uses simple bit-wise arithmetic operations such as AND, OR, XOR and ROT (bit rotation) to achieve the security and privacy requirements of low-cost RFID system.

3.1 System assumption

We assume that tag is vulnerable to be compromised. When the tag was compromised, the secret information of tag which contains shared symmetric key and tag identification can be retrieved by adversary. The system assumption of our scheme is described below. Our protocol has three main components: tag, reader and the backend server. Tags are passive tags, reader is the equipment to collect data from tags, and the backend server is to analyze the collected data. The communication channel between tag and reader are classified into two categories, forward channel and backscatter channel. The backscatter channel is namely as back channel and reverse channel. The communication channel between reader and backend database is a well protected and trusted system, so that transmitted message cannot be violated or eavesdropped by adversary. In other word, it cannot get any secret information from backend server. Each tag contains four filed data including ID, T_{key}, t and *flag*. ID is the identification of RFID tag. According to EPC global standard, the length of tag identification can be 64bits, 96bits and 128bits and 256bits. Accordingly, we assume a reasonable length of tag identification is 96 bits. Sometimes, it has the probability of $1/2^{96}$ to generate the same identification because the length of tag identification has only 96 bits. Many researchers also provide complete solution for tag collision (Shih et al., 2006; Lee et al., 2004). Hence, we think that tag collision is almost impossible happened for RFID tag. T_{key} is the shared secret information in RFID tags as well as an encryption key. t is the counter value represented as total query times. The database includes two data, ID and T_{key}. We assume the length of T_{key} and t is the 96 bits as ID. Finally, we present the system notation in the following. Note that the flag mechanism design at backend server is used for solving *DoS* attack.

- S: random generator number is generated by reader for each session.
- *flag*: the value is used to indicate the tag is normal state(*flag*=0) or exceptional state(*flag*=1).
- i : the i th session
- ID_i, ID_i': the identification of tag at tag and backend server.
- ID_{iL}, ID_{iL}': the left half of tag identification at tag and backend server.
- ID_{iR}, ID_{iR}': the right half of tag identification at tag and backend server.
- T_{key} , T_{key}': the secret symmetric key of tag at tag and backend server.
- T_{keyL}, T_{keyL}': the left half of secret symmetric key of tag at tag and backend server.
- T_{keyR}, T_{keyR}': the right half of secret symmetric key of tag at tag and backend server.
- t: a counter value of tag, when flag is one, it generates a value to encrypt the message.
- M_1, M_2, M_3, M_4, M_1', M_2', M_3' and M_4': the encrypted message at tag and backend server.
- K_1, K_2, K_1' and K_2': the symmetric secret keys of tag which update for each session at tag and backend server.
- R, R': the certificated message at tag and backend server.
- R_L, R_L': the left half of certificated message R at tag and backend server.
- R_R, R_R': the right half of certificated message R of tag at tag and backend server.

- ID_{i+1}, $ID_{i+1'}$: the updated identification of tag at tag and backend server.
- ID_x: the identification of tag in any session
- ⊕: XOR
- /\: AND
- \/: OR
- ‖: Concatenation
- +: ADD
- $Rot(x, y)$: left rotate the value of x with y bits

3.2 Mutual authentication protocol

In this section, we propose a new mutual authentication protocol namely SMAP-LRS. SMAP-LRS is based on two conditions, the first one is normal state (flag is zero) and second one is exceptional state (flag is one). After the authentication is successfully completed, the protocol switches to normal state and the flag of tag will be changed from one to zero.

The proposed scheme consists of two different conditions based on previous authentication session is safely terminated (*flag* = 0) or not (*flag* =1). The condition of normal state is illustrated as Fig. 1.

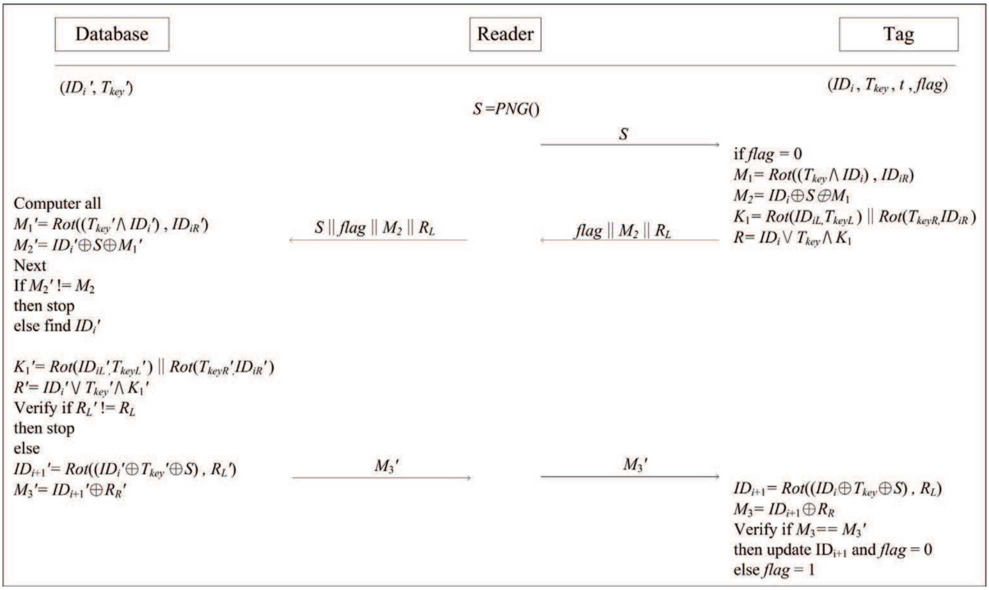

Database
Reader
Tag
(ID_i', T_{key}')
$S = PNG()$
$(ID_i, T_{key}, t, flag)$
S
if $flag = 0$
$M_1 = Rot((T_{key} \wedge ID_i), ID_{iR})$
$M_2 = ID_i \oplus S \oplus M_1$
$K_1 = Rot(ID_{iL}, T_{keyL}) \,\|\, Rot(T_{keyR}, ID_{iR})$
$R = ID_i \vee T_{key} \wedge K_1$
$flag \,\|\, M_2 \,\|\, R_L$
$S \,\|\, flag \,\|\, M_2 \,\|\, R_L$
Computer all
$M_1' = Rot((T_{key}' \wedge ID_i'), ID_{iR}')$
$M_2' = ID_i' \oplus S \oplus M_1'$
Next
If $M_2' != M_2$
then stop
else find ID_i'
$K_1' = Rot(ID_{iL}', T_{keyL}') \,\|\, Rot(T_{keyR}', ID_{iR}')$
$R' = ID_i' \vee T_{key}' \wedge K_1'$
Verify if $R_L' != R_L$
then stop
else
$ID_{i+1}' = Rot((ID_i' \oplus T_{key}' \oplus S), R_L')$
$M_3' = ID_{i+1}' \oplus R_R'$
M_3'
M_3'
$ID_{i+1} = Rot((ID_i \oplus T_{key} \oplus S), R_L)$
$M_3 = ID_{i+1} \oplus R_R$
Verify if $M_3 == M_3'$
then update ID_{i+1} and $flag = 0$
else $flag = 1$

Fig. 1. The normal state of mutual authentication protocol

Condition 1: previous authentication session is safely terminated (*flag* = 0)

Step1: *Reader → Tag: Query*

The reader generates random number S and sends it as a query command to tag.

Step2: *Tag → Reader: flag*, M_2, R_L

When tag receives the query S from reader, it checks the flag state to decide the protocol is normal state. First, tag computes M_1=$Rot((T_{key}$ /\ $ID_i)$, $ID_{iR})$ and response value

M_2=ID_i⊕S⊕M_1 which protect ID to avoid from eavesdropping. Second, tag computes T_{keyL}, T_{keyR} and K_1=$Rot(ID_{iL,}T_{keyL}) \| Rot(T_{keyR,}ID_{iR})$ to generate certificated message R=$ID_i \vee T_{key} \wedge K_1$. The certificated message R will be used to authenticate the tag and reader. Finally, the tag will send these response value *flag*, M_2, R_L to reader.

Step3: *Reader → Backend Server: S, flag,* M_2, R_L

After the reader receives the response from tags, it appends the number S and forwards to backend server.

Step4: *Backend Server → Reader:* M_3'

When backend server receives the authentication request (*flag*, M_2, $R_{L,}$ S) from reader, server computers all M_1'=$Rot((T_{key}' \wedge ID_i') , ID_{iR}')$. Next, the server reuses M_1' to creates the M_2'=ID_i'⊕S⊕M_1' to verify the M_2. If M_2' is the same as M_2, it finds the corresponding record form the database. Otherwise, it terminates the authentication immediately.

After retrieving the value of relative field in the corresponding record, the server computes the K_1'=$Rot(ID_{iL}',T_{keyL}') \| Rot(T_{keyR}',ID_{iR}')$. Next, the backend server keeps to create the certificated message R'=$ID_i' \vee T_{key}' \wedge K_1'$. The server uses the left half of certificated message R', called R_L' to verify whether R_L' is equal the R_L or not. This verification process can ensure the data integrity; otherwise it will terminate the process and respond anything. In order to avoid the tracking attack, the server updates the identification of tag ID_{i+1}=$Rot((ID_i \oplus T_{key} \oplus S) , R_L)$ for each session. With new identification, the server can calculates the certificated message M_3'=ID_{i+1}'⊕R_R and transmits it to tag though reader.

Step5: *Reader → Tag :* M_3'

When tag receives M_3', it computes the new identification of tag and uses the updated identification of tag ID_{i+1} to generate the certificated message M_3. If the M_3 is equal to M_3', the tag updates the old identification ID with new identification ID_{i+1}. Until the process is successful finished, the tag also resets the flag value to zero.

When the authentication between tag and reader is not completely finished, the flag value will be changed from zero to one. For example, when the authentication is proceeding, once tag does not receive any response from original reader in a period time or the response is invalid, the tag which still receives the query from reader may change its condition to exceptional state. The condition of exceptional state is illustrated as Fig. 2.

Condition 2: previous authentication session is not safely terminated (*flag* = 1)

Step1: *Reader → Tag: Query*

The reader generates random number S and sends it as a query command to tag.

Step2: *Tag → Reader: flag,* M_2, M_3, R_L

When tag receives the query again and not terminates safely, it means that it is an exceptional state. So, the tag will calculate the t = $(t+2^t+T_{keyL})$ *mod length* (ID_i) value by using T_{key} and mod function. By using t value, the tag generates the another identification, namely as M_1=$Rot(ID_i , t)$ and computes the M_2=S⊕T_{key}⊕M_1 with S and T_{key}. In order to use the t value to resolve the M_2, we must send the t value to the backend server. The only way is to protect t value by using T_{key} and M_1. Thus, the M_3=$(T_{key} \wedge M_1) \oplus t$ is a ciphertext to protect the t value. At the same time, the tag computes the K_1=$Rot(T_{keyL,}T_{keyR}+t) \| Rot(T_{keyR,}T_{keyL}-t)$ to generate the message R=$T_{key} \vee M_1 \wedge K_1$. The certificated message R value will be utilized to conform whether the tag is legal or not. Finally, the tag responds *flag*, M_2, M_3 and R_L to reader.

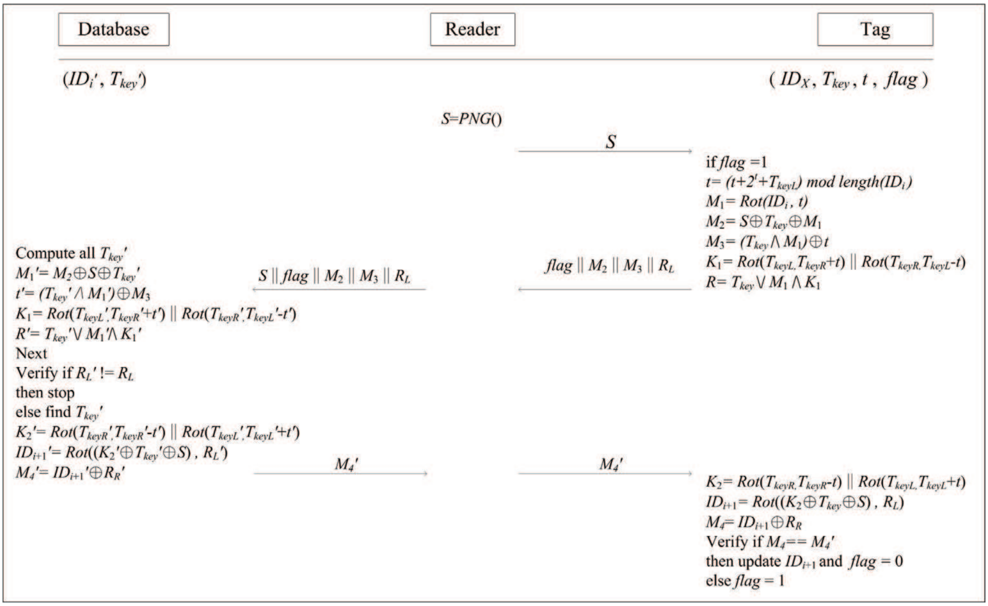


Fig. 2. The exceptional state of mutual authentication protocol

Step3: Reader → *Backend Server: S, flag,* M_2, M_3, R_L

When reader receives the response from tag, it appends S and forwards to the backend server.

Step4: *Backend Server→ Reader:* M_4'

When backend server collects a round of message from reader, it retrieves the $M_1'=M_2'\oplus S\oplus T_{key}'$ by using S, T_{key}' and M_2'. M_2' value is the same as M_2 which sends from tag. then, the backend server decrypts the M_3 with T_{key}' and M_1' to obtain the $t'=(T_{key}'\ /\backslash\ M_1')\oplus M_3$ value. By using t' value, we can calculate $K_1= Rot(T_{keyL,}T_{keyR}+t')\|Rot(T_{keyR,}T_{keyL}-t')$ to generate the certificated message $R'=T_{key}\ \backslash/\ M_1'/\backslash\ K_1'$. Next, backend server verifies whether the R_L' is equal to R_L or not. If the pair of values is not match, the authentication process will be terminated immediately. Otherwise, it means that the backend server can identify correctly the corresponding tuple of database. Finally, it computes the $K_2'=Rot(T_{keyR}',\ T_{keyR}'-t')\|Rot(T_{keyL}',\ T_{keyL}'+t')$ with T_{keyR}', T_{keyL}'. By using the updated identification of tag $ID_{i+1}'=Rot((K_2'\oplus T_{key}\oplus S),\ R_L')$ and the right half of R' to create the certificated message $M_4'=ID_{i+1}'\oplus R_R$, the certificated message M_4' provides a proof for tag to verify the reality of reader.

Step5: *Reader → Tag :* M_4'

while the tag receives the message M_4' from backend server, it calculates the new tag identification $ID_{i+1}=Rot((K_2\oplus T_{key}\oplus S)\ ,\ R_L)$. By using the right half of R and ID_{i+1}, the backend server can create the certificated message $M_4=ID_{i+1}\oplus R_R$ to compare whether the M_4' is equal to M_4 or not. if M_4' is the same as M_4, the identification of tag will change to ID_{i+1} and reset the flag to zero.

4. Security and performance analysis

For the sake of clarity, the aim of this section is to analyze our authentication scheme and compare it with related literature based on following security and performance criterions. First of all, we explain that how to ensure that the protocol is well protected. We illustrate each security analysis in section 4.1. Secondly, we have a comparison for our scheme in storage, operation and communication in section 4.2.

4.1 Security analysis

In this section, we conduct security analysis to proposed authentication scheme.

- Data security

The transmitted message between tag and reader is a ciphertext by using AND, OR, XOR and ROT function. The encrypted message for each session is encrypted by random-generated one time valid numbers to perform beneficial computation. Even if the ciphertext can be modified or eavesdropped, the transmitted messages which provide the security robustness of meaningful data will not be compromised. So we believe that the transmitted message is secure enough to ensure the confidentiality of the transmitted data.

- Anonymity

For each tag, the information of tag is changed dynamically in each session. Even if the authentication process between tag and reader is failure, the tag still has its mechanism to keep the responded message different. In normal state, the transmitted messages are encrypted by different *S* and *ID*. In exceptional state, the transmitted message still keeps being changed by using updated *t* value. Generally speaking, no matter the authentication is success or not, the tag will modify its own data in every session. Hence, the attacker cannot find consistent clues of each tag response to track a specific tag easily.

- Replay attack resistance

SAMP-RLS is a challenge-response protocol using pseudo-random number to prevent replay attack. The message M_1, M_2 and M_3 are refreshing by using *S* and *ID* in each section. Hence, the malicious attack cannot reuse the original message to pass the authentication.

- Denial of Service resistance

As we noted above, *DoS* attack have two different definition. By using a flag mechanism, our scheme allows the tag with constant secret key can still be authentication by backend server and re-synchronize its data with databases. Additionally, comparing other schema against Dos attack, our schema can replace dual tuple of secret information values (*new* and *old*) to save lots of storage space in backend server.

- Forward security

If the adversary collects a series of past transmitted messages and get the secret information of tag in a period. The adversary infers transmitted messages to obtain previous relationship of data. Because the identification *(ID)* of tag is dynamically changed for each session, the adversary is unable to obtain the previous data by using the current secret information of tag and have no co relationship between messages transmitted in consecutive session. The adversary cannot generate new identification and track further recorder. However, if the adversary try to compromise tag to know all data stored in, the attacker still could not trace back the trajectory of compromised tag in our scheme.

- Mutual authentication

SAMP-RLS provides both tag to reader and reader to tag authentications. The R_L is the certificated code to verify the tag. On the contrary, the R_R is the certificated code to verify the reader. Hence, our scheme indeed reaches the aim of mutual authentication.

Introducing the security analysis in our scheme provides the well protection for command attacks. A simple comparison of recent authentication protocols is listed in Table 1. We compare the similar operations of authentication protocols such as EMAP, M2AP, LAMP, SASI, etc.

According to the Table 1 above, our scheme use simple operation to secure message to achieve the requirement of security. It also provides strong security against all kinds of command attacks.

	SMAP-LRS	EMAP	M2AP	LAMP	SASI
Data security	Y	N	N	N	Y
Anonymity	Y	N	N	N	N
Replay attack resistant	Y	N	N	N	Y
DoS resistant	Y	N	N	N	Y
Forward security	Y	N	N	N	Y
Mutual authentication	Y	N	N	N	Y

Table 1. Comparison of other simple operation scheme

4.2 Performance analysis

Our protocol also compares the performance analysis, including storage, operation and communication. In our research, we know that the memory space of our scheme decrease 5*L* of storage and 0.5*L* of communication for the SASI mechanism which is the most low-cost scheme currently. Hence, our scheme reduced about fifty percent of memory space is less than other scheme at present.

In our scheme, we assume that the lengths of the identification or key are 96 bit as *L* bits. First, storage is separated into two parts, one is the memory of tag and the other is the memory of database. The database memory of our scheme contains *ID* and T_{key} are 2*L* bits. Because the memory space of *flag* is one bit, the tag memory of our scheme contained *ID*, T_{key}, *t* and *flag* are about 3*L* bits. Second, the recent papers in designing the authentication protocol usually use hash, Pseudo-random number generator and CRC to protection their protocol. However, our scheme only uses simple operations that fit the requirement of passive tag such as AND, XOR, OR and Rot function. Hence, we believe that simple operation can ensure not only security requirement but also low-cost demanded, especially for EPC global standard. Third, the communication between reader and tag also should be considered because the energy of passive tag comes from reader. The length of message decides the consumption of energy to transmit range. It is an important factor to dispatch the power energy and control the communication. The total communications of our scheme including *flag*, M_2, M_3' and R_L is 2.5*L* bits when our scheme is a normal state. Even if our scheme is exceptional state, the communication of our scheme including *flag*, M_2, M_3, M_4' and R_L is only 3.5*L* bits. We believe that our communication is less 0.5*L* than SASI at least. We list a comparison summary of various schemes in Table 2. We also count the number of simple operation in detail to compare with other low cost authentication protocols in Table 3.

	Memory storage		Operation	Communication
	Tag	Backend Server		
EMAP (Peris-Lopez et al., 2006)	6L	6L	⊕, /\ , \/	5L
M2AP (Peris-Lopez et al., 2006)	6L	6L	⊕, /\ , \/ , +	5L
LMAP (Peris-Lopez et al., 2006)	6L	6L	⊕, /\ , \/ , +	4L
SASI (Chien, 2007)	4L	7L	⊕, /\ , \/ , + , Rot	4L
SMAP-LRS	3L	2L	⊕, /\ , \/ , Rot, mod	3.5L

Table 2. The comparison of required memory, operation and communication

	LMAP		M2AP		EMAP		SASI		SMAP-LRS		SMAP-LRS	
Authentication state									Flag = 0		Flag =1	
	T	R+B	T	R+B	T	R+B	T	R+B	T	R+B	T	R+B
AND	0	0	1	1	2	2	0	0	2	2	2	2
OR	0	1	1	1	1	1	2	2	1	1	1	1
XOR	2	2	1	2	6	5	6	6	3	3	4	4
ADD	1	3	1	2	0	0	3	3	0	0	0	0
ROT	0	0	0	0	0	0	0	0	1	1	1	1
Update state									Flag = 0		Flag = 1	
AND	0	0	0	0	0	0	0	0	0	0	0	0
OR	0	0	0	0	0	0	0	0	0	0	0	0
XOR	10	10	10	10	10	10	4	4	2	2	2	2
ADD	5	5	5	5	0	0	1	1	0	0	0	0
ROT	0	0	0	0	0	0	2	2	3	3	5	5
Total	18	21	19	21	19	18	18	18	12	12	15	15

Table 3. The counter of simple operation

5. Conclusion

In this chapter, we present a secure mutual authentication protocol for low-cost resource-constrained RFID tag system under insecure wireless communication environment. The introduction of three security-enhanced designs in our scheme provides a more robust RFID authentication process. First, a flag state mechanism is proposed to prevent DoS attack and reduce the data storage space at the backend server by eliminating the need of storing dual tuples in database. Second, simple operations such as AND, XOR, OR, bit addition (mod 2^m) and bit rotation function are introduced to be compatible with EPCglobal Class1 Gen2 standard and to fit in the computation limitation of resource-constrained tag. Third, the proposed scheme SAMP-RLS provides data security to defend against major security threats such as replay attack and eavesdropping. In addition, SAMP-RLS possesses privacy protection features such as anonymity and forward secrecy. In terms of resource utilization, the required memory space of our scheme for a RFID system decreases about 45% to 50% in comparison with other existing mutual authentication protocols. In summary, our mutual authentication protocol offers data security enhancement, privacy protection ability and better resource utilization in comparison with other RFID authentication protocols.

6. Acknowledgments

The authors gratefully acknowledge the support from TWISC projects sponsored by the National Science Council, Taiwan, under the Grants No NSC 96-2219-E-001-001 and NSC 96-2219-E-011-008.

7. References

An, Y. & Oh, S. (2005). RFID System for User's Privacy Protection, In 2005 Asia-Pacific Conference on Communications, pp. 516-519.

Chien, H. (2007). SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, *IEEE Transactions on Dependable and Secure Computing*, vol. 4, pp. 337–340.

Chien, H.Y. & Chen, C.H. (2007). Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standard, *Computer Standards & Interfaces*, Vol. 29, Issue 2, pp. 254-259.

Chien, H.Y. & Huang, C.W. (2007). Security of ultra-lightweight RFID authentication protocols and its improvements, in *ACM SIGOPS Operating Systems Review* Vol. 41 New York, NY, USA.

Datasheet Helion Technology. (2005). MD5, SHA-1, SHA-256 hash core for Asic, http://www.heliontech.com .

Duc, D.N.; Park, J.; Lee, H. & Kim, K. (2006). Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning, Proceedings of the 2006 Symposium on Cryptography and Information Security.

Feldhofer, M.; Dominikus, S. & Wolkerstorfer, J. (2004). Strong authentication for RFID systems using the AES algorithm, Workshop on Cryptographic Hardware and Embedded Systems–CHES, vol. 3156, pp. 357–370.

Garfinkel, S. & Rosenberg, B. (2005). *RFID: Applications, Security, and Privacy*, Addison-Wesley Professional.

Henrici, D. & Müller, P. (2004). Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, in Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, Florida, pp. 149-153.

Juels, A. (2005). Strengthening EPC tags against cloning, in Proceedings of the 4th ACM workshop on Wireless Security, pp. 67-76.

Juels, A.; Molnar, D. & Wagner, D. (2005). Security and privacy issues in e-passports, in *IEEE Secure Comm.* Vol. 5.

Karthikeyan, S. & Nesterenko, M. (2005). RFID security without extensive cryptography, in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, ACM, pp. 63-67.

Karygiannis, T.; Eydt, B.; Barber, G. & Bunn, L. (2007). *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, in National Institute of Standards and Technology, April.

Kim, H.W.; Lim, S.Y. & Lee, H. J. (2006). Symmetric Encryption in RFID Authentication Protocol for Strong Location Privacy and Forward-Security, in Proceedings of the 2006 International Conference on Hybrid Information Technology Vol. 02, pp. 718-723.

Kumar, S. & Paar, C. (2006). Are standards compliant elliptic curve cryptosystems feasible on RFID, in Proceedings of Workshop on RFID Security, Austria, July.

Lee, J.; Kwon, T.; Choi, Y.; Das, S.K. & Kim, K. (2004). Analysis of RFID anti-collision algorithms using smart antennas, in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, pp. 265-266.

Li, T. & Deng, R.H. (2007). Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol, in the Proceedings of the Second International Conference on Availability, Reliability and Security-AReS, pp. 10-13.

Li, T. & Wang, G. (2007). Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols, IFIP SEC.

Li, T. (2008). Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols, *JOURNAL OF SOFTWARE*, vol. 3, p. 1.

Lo, N.W. & Yeh, K.H. (2007). An Efficient Mutual Authentication Scheme for EPCglobal Class-1 Generation-2 RFID System, in the 2nd International Workshop on Trustworthiness, Reliability and services in Ubiquitous and Sensor networks, TRUST. Vol. 7, LNCS.

Ohkubo, M.; Suzuki, K. & Kinoshita, S. (2003). Cryptographic approach to "privacy-friendly" tags, in RFID Privacy Workshop, MIT, MA, USA, pp. 624-654.

Peris-Lopez, P.; Hernandez-Castro, J.C.; Estevez-Tapiador, J.M. & Ribagorda, A. (2006). EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags, OTM Federated Conferences and Workshop, IS Workshop.

Peris-Lopez, P.; Hernandez-Castro, J.C.; Estevez-Tapiador, J.M. & Ribagorda, A. (2006). LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags, in Proc. of 2nd Workshop on RFID Security.

Peris-Lopez, P.; Hernandez-Castro, J.C.; Estevez-Tapiador, J.M. & Ribagorda, A. (2006). M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags, in Proc. of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923.

Poschmann, A.; Leander, G.; Schramm, K. & Paar, C. (2006). A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications, in Workshop on RFID Security–RFIDSec. Vol. 6.

Poschmann, A.; Leander, G.; Schramm, K. & Paar, C. (2007). New Light-Weight Crypto Algorithms for RFID, in Proceedings of The IEEE International Symposium on Circuits and Systems, ISCAS.

Rhee, K.; Kwak, J.; Kim, S. & Won, D. (2005). Challenge-response based RFID authentication protocol for distributed database environment, in International Conference on Security in Pervasive Computing–SPC. Vol. 3450, pp. 70–84.

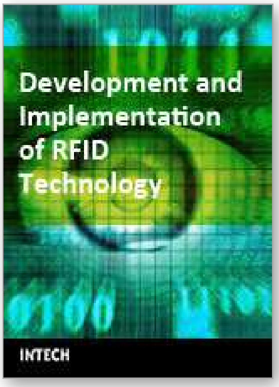
Sarma, S.E. & Engels, D.W. (2003). On the Future of RFID Tags and Protocols, in white paper, Auto-ID Center, Massachusetts Institute of Technology.

Shih, D.H.; Sun, P.L.; Yen, D.C. & Huang, S.M. (2006). Taxonomy and survey of RFID anti-collision protocols, *Computer Communications*, Vol. 29, pp. 2150-2166, Elsevier.

Weis, S.A. (2003). Security and Privacy in Radio-Frequency Identification Devices, Massachusetts Institute of Technology.

Weis, S.A.; Sarma, S.E.; Rivest, R.L. & Engels, D.W. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, in Security in Pervasive Computing, pp. 201–212.

Yu, S.; Ren, K. & Lou, W. (2007). A Privacy-preserving Lightweight Authentication Protocol for Low-Cost RFID Tags, in IEEE Military Communications Conference, MILCOM, pp. 1-7.



Development and Implementation of RFID Technology
Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821