This document is downloaded from DR-NTU (https://dr.ntu.edu.sg)
Nanyang Technological University, Singapore.

An ultralightweight RFID authentication protocol with CRC and permutation

Gao, Lijun; Ma, Maode; Shu, Yantai; Wei, Yuhua

2013

Gao, L., Ma, M., Shu, Y., & Wei, Y. (2013). An ultralightweight RFID authentication protocol with CRC and permutation. Journal of Network and Computer Applications, 41, 37-46.

https://hdl.handle.net/10356/100942

https://doi.org/10.1016/j.jnca.2013.10.014

© 2013 Elsevier Ltd. This is the author created version of a work that has been peer reviewed and accepted for publication by Journal of Network and Computer Applications, Elsevier Ltd. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [http://dx.doi.org/10.1016/j.jnca.2013.10.014].

Downloaded on 14 Aug 2022 05:41:47 SGT

An Ultralightweight RFID Authentication Protocol with CRC and Permutation

Lijun Gao[1, 2], Maode Ma[3*], Yantai Shu[1] and Yuhua Wei[2]

[1]School of Computer Science and Technology, Tianjin University, Tianjin
[2]Department of Computer Science and Technology, Shenyang Aerospace University, Shenyang
[3]School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore

Abstract—Radio Frequency Identification (RFID) technology will become one of the most popular technologies to identify objects in the near future. However, the major barrier that the RFID system is facing presently is the security and privacy issue. Recently, an ultralightweight RFID authentication protocol with permutation has been proposed to provide security and prevent all possible attacks. However, it is discovered that a type of desynchronization attack can successfully break the proposed scheme. To overcome the vulnerability under the desynchronization attacks, we propose an approximate ultralightweight RFID authentication protocol which integrates the operation of the XOR operator, build-in CRC-16 function, the permutation and secret key backup technology to improve the security functions without increasing any security cost. We formally verify the security functionality of the proposed scheme by using Simple Promela Interpreter (SPIN). Analysis shows that our proposal has a strong ability to prevent existing possible attacks.

Keywords: RFID; ultralightweight; permutation; desynchronization; SPIN

1. Introduction

Radio frequency identification (RFID) is a technology for automated identification of objects and people [1]. An RFID application contains three key elements: RFID tags, RFID readers, and a back-end database server that has the ability to identify objects with increased speed and accuracy. The reader is used to query the tag identify (TID) and forwards it to the back-end server. Once the tag is found valid, the back-end server will check the information kept by the tag for further processing. RFID tags are classified into three types: active, semi-passive, and passive. Active tags need batteries to operate so that they can actively communicate with the readers. Semi-passive tags also need batteries to work but they have to wait for the reader's query. As for passive tags, the power supply comes from the reader. In a basic RFID system, the information transmitted in the air between the tag and the reader could easily be intercepted and eavesdropped due to its radio transmission nature.

A Generation 2 (Gen2) tag contains a pseudorandom number generator (PRNG) and protects message integrity via Cyclic Redundancy Code (CRC-16). The memory space is separated into four banks: the

reserved memory, Electronic Product Code (EPC) memory, TID memory, and the user memory. It harvests power from the readers through the antenna, and hence, cannot perform complex computations. EPCglobal class-1 generation-2 (Gen2 in brief) was approved as ISO18000-6C in July 2006. It is widely believed that Gen2 tags will be the mainstream for the developing RFID applications because the effective reading range is larger[2].

Currently, the RFID security and privacy protection mechanisms mainly can be classified into two major categories: physical approaches and encryption mechanisms and protocols. The proposals on the physical security mechanisms for the RFID tags mainly include the Faraday Cage [3], kill command mechanism [4], the locker tag [5]. Further research results indicate that although the physical security approaches can achieve some degree of security, it will cause the increase of the cost of an entire RFID system. On the other hand, the encryption technology based security protocols have shown be more attractive to the development of the RFID systems, which will be soon widely adopted. The encryption technology based security protocols can be classified into four classes. The first class called "full-fledged class" refers to those protocols that demand the support of conventional cryptographic functions like symmetric encryption, ryptographic one-way function, or even the public key algorithms. The second class called "simple" refers to those protocols that should support random number generator and one-way hashing function on tags. The third class called "lightweight" protocols refers to those protocols that require a random number generator and simple functions. The fourth class called "ultralightweight" that only nvolve simple bitwise operations (like XOR, AND, OR, etc.) or some built-in function in tags. Analysis shows that simple, lightweight and ultralightweight RFID authentication protocols are more effective and efficient. They have attracted much more attention from researchers because the full-fledged RFID authentication protocols cannot meet the requirement of a low-cost RFID system, although they have strong security functionality [6].

In terms of simple protocols, the hash-Lock scheme has been introduced in [3,7] used $metaID$=H(K) to hide the real ID of a tag, where K is the shared secret between the tag and the back-end server, H is a one-way hash function. Although this scheme offers certain level of reliability at low cost, an adversary can easily track the tag via its *metaID* and thus the transaction secret or privacy would be at risk. Furthermore, since the key shared between the tag and the back-end server is sent in plaintext, even an inactive adversary can easily sniff the channel to spoof the tag later. The hash based ID variation protocol in [8] is similar as the hash chain protocol, which uses a random number to refresh the tag identifier dynamically. The random number increases in every successful authentication session so that this improved protocol can defend against the replay attacks. The protocol can resolves the location attacks by making the ID of a tag randomized in every interrogation. It is reliable to prevent data loss because it can

restore the data from the previous record. Unfortunately, this protocol cannot resist man-in-the-middle attacks. The behaviors of the intermittent position tracing attacks and desynchronization attacks have been defined in [9]. And the vulnerability of the protocol under the desynchronization attacks has been reported in [10] while a novel RFID security protocol (RIPTA-DA) has been designed, which employs a stochastic dynamic multi-key mechanism to encrypt the information and introduces the noise disturbance technology to overcome the vulnerabilities under the both attacks.

On the other hand, in terms of lightweight protocols, Hopper and Blum (HB)、HB+、HB++ protocols have been proposed in [11-14] as a family, which has used Learning Parity in the Presence of Noise (LPN) to provide stronger security functionality. However, it is found that if an aggressor replays challenges on a tag with $O[(1-\eta)/(1-2\eta)^2]$, where η is a noise parameter. Each tag has a noise generator, the probability of generating a noise is $v = \{0, 1 \mid \text{prob}[v = 1] = \eta\}$, $\eta \in (0, 1/2)$, where v is a vector, which is a binary string, η is the probability of the number of "1" in the binary string v times. It is possible to obtain the value of $a \cdot x$, where $\cdot$ is a point multiplication operation, with very high probability. A synchronization-based communication protocol for RFID devices has been presented in [15]. The protocol targets to protect the EPC Global Class-1 Gen-2 RFID tags which support only simple cryptographic primitives like PRNG and CRC. It can prevent the cloned tags and malicious readers from impersonating attacks and abusing legitimate tags, respectively. In addition, the protocol is able to provide that each RFID tag emits a different bit string (pseudonym) when receiving each query from different readers. Therefore, it makes possible for the tracking activities and personal preferences of a tag's owner impractical to provide the user's privacy. It's possible for a malicious reader can get $M_1 = \text{CRC}(\text{TID}\|r_1) \oplus K_i$, and $M_2 = \text{CRC}(\text{TID}\|r_2) \oplus K_i$, where k represents string concatenation and r_1, r_2 are nonce values. In this way, the attacker can identify the tag by the following way $M_1 \oplus M_2 = \text{CRC}(\text{TID}\|r_1) \oplus \text{CRC}(\text{TID}\|r_2)$. Once the tag is queried by a valid reader which causes the key update, the attacker can restart the attack. Although the protocol is defective, the application of CRC function in the design has opened a new way to design a low cost RFID system. In [16-17], three solutions have been proposed for the authentication and privacy in the RFID systems base on the quadratic residues technology. But due to the employment of high cost hash functions and complex encryption algorithms, they are not suitable to the low-cost RFID systems.

In terms of ultralightweight protocols, a minimalist mutual-authentication protocol (M^2AP) for low-cost RFID tags has been proposed in [18] based on some simple operations such as XOR, OR, AND, and sum of modulo. A tag and a reader can share a pseudonym session identifier (SID) and four keys K_1, K_2, K_3, and K_4. During each session, the reader generates two random numbers n_1 and n_2. Let "$\vee$" denote OR operation, "$\wedge$" for AND, and "+" for modular summation. By this protocol, the tag verifies the reader by

checking the n_1 value extracted from the first two messages. The tag then responds to the reader if it is correct. Both SID and four keys must be updated after each session to provide forward secrecy. Recently, an attack to break the M^2AP protocol has been reported in [19]. By this attack, an adversary could discover the tag's identity and some shared secrets in two rounds of eavesdropping. Furthermore, the attacker can undertake desynchronization attacks by using the known key.

An interesting lightweight authentication protocol has been proposed providing strong authentication and strong integrity (SASI) for low-cost RFID tags in [6]. An index-pseudonym (IDS), the tag's private identification (ID), and two keys (k_1/k_2) are stored both on the tag and in the back-end database. Simple operation functions such as bitwise XOR ($\oplus$), bitwise AND ($\wedge$), bitwise OR ($\vee$), addition 2^m and left rotate Rot(x, y) are required on the tag. Additionally, a PRNG is required at the reader. The proposed scheme is ultralightweight, while the active tracking attacks are possible among two valid readers because the IDS in SASI is a static value. It is also shown that a desynchronization attack on the SASI scheme can succeed with at most 96 trials [20]. Gossamer protocol has been introduced in [21], which has a very good security performance to keep the confidentiality and integrity of data in the authentication procedure with a forward security characteristic due to a rotation operation, which is a combined function with circular shift function and the Mixbits function. Gossamer protocol has shown to have an extremely lightweight nature, as only bitwise right shift (>>) and additions have been employed. The abovementioned protocols have certain security functionality equipped with simple operations at a low cost, while they are not able to resist some desynchronization attacks[22].

A new ultralightweight RFID authentication protocol with permutation (UAPP) has been proposed in [23]. It has avoided using unbalanced OR and AND operations and has introduced a new operation named permutation. A tag only involves three operations: bitwise XOR, left rotation and permutation. The performance evaluation illustrates that since the UAPP scheme only uses fewer resources on the tags in terms of computation operation, storage requirement and necessary communication, the total cost of the UAPP scheme is low. The security analysis in [23] has claimed that the UAPP scheme can resist to all possible existing attacks. However, one type of the desynchronization attacks has been found to be able to break the protocol.

It is obvious that the simple authentication protocols can effectively resist to various attacks due to the employment of the complicated hash functions. Then, the security cost of them is high. Although the lightweight authentication protocols have not been equipped with complex hash functions, the security cost is relative higher due to the random number generator introduced. The design of RFID ultralightweight authentication protocols to have high security functionality with a low cost becomes very important and attractive. In this paper, the UAPP scheme, which is the newest ultralightweight protocol,

has been reviewed to explore its vulnerability under one type of the desynchronization attacks. Further, we put forward an improved protocol named as approximate ultralightweight RFID authentication protocol with CRC-16 and permutation (LPCP), which is a proposal to resist the particular desynchronization attacks. The build-in CRC-16 function has been introduced to enhance the security of the ultralightweight protocol without increasing any cost. In addition, the proposed protocol integrates the operation of the XOR operator, permutation and the secret key backup technology to protect the information in the low cost RFID system. We formally verify the security functionality of the proposed scheme by using Simple Promela Interpreter (SPIN) and security analysis, which shows that the proposed solution has a strong ability to prevent all existing possible attacks.

The remainder of the paper is organized as follows. The UAPP scheme is reviewed to explore its vulnerability under one type of the desynchronization attacks in Section 2. In Section 3, the LPCP scheme is proposed to overcome the flaw in the UAPP scheme. The security analysis on the LPCP scheme by theory and SPIN model is presented in Section 4. Then, in Section 5, the logic scheme and the performance evaluation of LPCP is demonstrated in terms of the computation operation, the storage requirement, the communication cost and the capability to resist malicious attacks. Finally, the paper is concluded in Section 6.

2. Security Analysis on the UAPP

This section we review the operation of the UAPP scheme and define a desynchronization attack model to break it.

Table 1 Notations

Symbol	Meaning
$\oplus$	XOR operator
IDS^{old}	The previous serial number
IDS^{new}	The current serial number
n_1	a random number who generated by the back-end server
n_2	a random number who generated by the back-end server
K_1^{old},K_2^{old}, K_3^{old}	secret key storage rooms K_1^{old},K_2^{old}, K_3^{old} which are used to keep the previous secret key in the back-end server
K_1^{new},K_2^{new},K_3^{new}	secret key storage rooms K_1^{new},K_2^{new},K_3^{new} which are used to keep the current secret key in the back-end server
Per(A, B)	The function shown in Figure 1

2.1Review of the UAPP

2.1.1 Notations

We have the symbols used in [23] to describe the UAPP scheme summarized in the Table 1 for the convenience of the understanding.

2.1.2 Operations of the UAPP

1. The RFID reader sends a ”Hello” message to the tag to initiate a protocol session.

2. Upon receiving the reader’s query, the tag transmits *IDS* to the reader.

3. After receiving *IDS*, the reader uses it as an index to search a matched entry in the database. If it is an old *IDS*, the reader will use $\{K_1^{old}, K_2^{old}, K_3^{old}\}$ to computer the messages. If *IDS* is new, $\{K_1^{new}, K_2^{new}, K_3^{new}\}$ will be used. If *IDS* is not in the database, the reader will terminate the session as it may be an invalid tag. Suppose the reader has found $\{K_1, K_2, K_3\}$ as the tag’s entry. It will generate an *L*-bit random number n_1 and compute *A* and *B*. *A* is used to send the random number n_1 with a mask to the tag. The purposes of *B* include the authentication of the reader and the integrity of the messages. Then, *A* and *B* are sent to the tag.

4. The tag extracts n_1 by XOR *A* with Per(K_2,K_1) and computes a local value of *B*. If the local value of *B* is equal to the received *B*, the tag will compute and transmit *C* to the reader. Otherwise, the tag will do nothing because the received messages may be modified or sent by an unauthenticated reader.

5. When receiving *C*, the reader will compare it with the local *C* to authenticate the tag. If the tag is authenticated, the reader will generate another L-bit random number n_2. Both n_1 and n_2 will be used for the key update. The reader computes and sends *D* and *E* to the tag. Then the reader will update the corresponding tag entry.

6. The tag extracts n_2 from *D* and computes a local value of *E*. If the local value of *E* equates to the received *E*, the tag will authenticate the reader and update the pseudonym and the secret keys.

By the UAPP scheme, there are only three operations on the tags, which are bitwise XOR, left rotation and permutation. The storage requirement and the communication cost for the tags by the UAPP are relatively low compared with other ultralightweight authentication protocols. The computation complexity for the tags is quite low because only three effective operations as the abovementioned have been designed on the tags by the UAPP scheme. Corresponding security analysis shows that the UAPP scheme can assure data confidentiality and integrity and has the ability to resistant to most malicious protocol attacks.

2.2 Vulnerability of the UAPP

A desynchronization attack is an active malicious attack with aim to make the attacked RFID system lose desynchronization without an ability to be authenticated as normal. The RFID ultralightweight protocols are mainly used for special circumstances, such as library, warehouse and hospital. By the desynchronization attacks with a “malicious active reader” and several “malicious passive” loggers which is a storage and recording device, an attacker can make the RFID system paralyzed. For example, an equipment of the desynchronization attack can hide around a tag and a reader to launch the attacks and destroy the synchronization. After the attack, the secret keys of the reader will be updated as normal, but the secret key of the tag will be updated according to the forged secret keys which have been tampered by the attacker. The share keys of tag and reader will be not same. So the tag and reader will fail in the next round of authentication process. If lots of tags fail the authentication with the reader, the normal work will be broken.

In this section, we define a desynchronization attack model, which is a new type of desynchronization attack. By this type of desynchronization attacks, it is possible to make the server and tag lose synchronization by bits tampering operation with the probability $P=1/(2^{L-k}*C_{L-k+1}^{k})$. We examine the UAPP scheme to explore and verify that the UAPP scheme cannot resist this particular type of the desynchronization attacks.

2.2.1 Definition of the Desynchronization Attacks

Defines 1: Definition of the desynchronization attacks

An authentication protocol normally works in two steps, which are inquiry and communication. The inquiry has its definition A_{query}, and the communication has its definition $A_{communicate}$. Based on the definitions, an authentication process can be represented as $A= (A_{query}, A_{communicate})$

Experiment $Exp_A[IDS,k_1,k_2,k_3,1n_2, A, B,C, D, E]$

$IDS,k_1, k_2, k_3,n_1,n_2 \leftarrow \{0,1\}^k$

$A, B \leftarrow A_{query}()$

if($A_{reply}(A, B,$ “judge”))

Output(“Trace Attack Success”)

$D', E' \leftarrow A_{communicate}(D, E,$ ”guess”)

if(E'== $Per(K_3,Rot(n_2',n_2')) \oplus Per(n_2,K_3 \oplus K_2)$)

Output(“desynchronization attack success”)

Defines 2: Definition of the variable

Suppose A and B are two l-bit strings, where

$A = a_1a_2 \cdots a_l, a_i \in \{0, 1\}, i = 1, 2, \cdots, l,$

$B = b_1b_2 \cdots b_l, b_i \in \{0, 1\}, j = 1, 2, \cdots, l.$

Moreover, the Hamming weight of B, wt(B),is m($0 \le m \le l$) and $b_{k1} = b_{k2} = \cdots = b_{km} = 1, b_{km+1} = b_{km+2} = \cdots = b_{kl} = 0$, where $1 \le k_1 < k_2 < \cdots < k_m \le l$ and $1 \le k_{m+1} < k_{m+2} < \cdots < k_l \le l$. Then, the permutation of A according to B, denoted as Per(A,B),is Per(A,B)= $a_{k1}\ a_{k2} \cdots a_{km} a_{kl} a_{kl-1}\ a_{km+2}\, a_{km+1}$. Figure1 shows the computation of Per(X, Y).

We assume that

$K_1=\varepsilon_0\varepsilon_1\varepsilon_2\ldots\varepsilon_m\ldots\varepsilon_n\ldots\varepsilon_{l+1}\varepsilon_l$, $K_2=\alpha_0\alpha_1\alpha_2\ldots\alpha_m\ldots\alpha_n\ldots\alpha_{l+1}\alpha_l$,

$K_3=\beta_0\beta_1\beta_2\ldots\beta_m\ldots\beta_n\ldots\beta_{l+1}\beta_l$, $n_2=\gamma_0\gamma_1\gamma_2\ldots\gamma_m\ldots\gamma_n\ldots\gamma_{l+1}\gamma_l$,

$D=\zeta_0\zeta_1\zeta_2\ldots\zeta_m\ldots\zeta_n\ldots\zeta_{l+1}\zeta_l$ and $E=\lambda_0\lambda_1\lambda_2\ldots\lambda_m\ldots\lambda_n\ldots\lambda_{l+1}\lambda_l$.

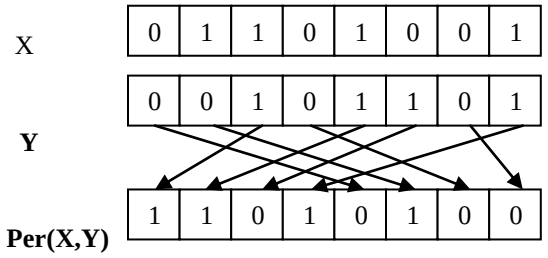


Figure 1 The Computation of the Example

2.2.2 Security Analyses of the UAPP

At the step 6 in the operation of the UAPP scheme, the reader sends D=Per(K_3,K_2)$\oplus n_2$ and E =Per(K_3,$Rot(n_2,n_2)$)) $\oplus$Per(n_1,$K_3 \oplus K_2$) to the tag. We select k bits from the D (k<l), ζ_m, ζ_n, ζ_i, ζ_j…, and flip these k bits as $\zeta_m = \neg\, \zeta_m$, $\zeta_n = \neg\, \zeta_n$, $\zeta_i = \neg\, \zeta_i$, $\zeta_j = \neg\, \zeta_j$…, then $D' = \zeta_0\zeta_1\zeta_2\ldots \neg\, \zeta_m \ldots \neg\, \zeta_n \ldots \neg\, \zeta_i \ldots \neg\, \zeta_j \ldots \zeta_{l+1}\zeta_l$

Because D=Per(K_3,K_2)$\oplus n_2$

$\Rightarrow n_2$= Per(K_3,K_2) $\oplus D$

$\Rightarrow n_2' = \{\gamma_0\gamma_1\gamma_2\ldots \neg\, \gamma_m \ldots \neg\, \gamma_n \ldots \neg\, \gamma_i \ldots \neg\, \gamma_j \ldots \gamma_{l+1}\gamma_l\}$

$\Rightarrow$ Rot(n_2',n_2')= $\gamma_{l-h+1}\gamma_{l-h+2}\ldots \neg\, \gamma_m \ldots \neg\, \gamma_n \ldots \neg\, \gamma_i \ldots \neg\, \gamma_j \ldots \gamma_{l-h-1}\gamma_{l-h}$

h= W(n_2')

$\Rightarrow F'=\mathrm{Per}(K_3,Rot(n_2',n_2'))=\{\sigma_0'\sigma_1'\sigma_2'\ldots\sigma_m'\ldots\sigma_n'\ldots\sigma_i'\ldots\sigma_j'\ldots\sigma_{l+1}'\sigma_l'\}$

$F=\mathrm{Per}(K_3,Rot(n_2,n_2))=\{\sigma_0\sigma_1\sigma_2\ldots\sigma_m\ldots\sigma_n\ldots\sigma_i\ldots\sigma_j\ldots\sigma_{l+1}\sigma_l\}$

$\Rightarrow \bigcup_{i=0}^{l}(\sigma_i)-(\sigma_m\ldots\sigma_n\ldots\sigma_i\ldots\sigma_j)=$

$\bigcup_{i=0}^{l}(\sigma_i')-(\sigma_m'\ldots\sigma_n'\ldots\sigma_i'\ldots\sigma_j')$

The total elements number of $(\sigma_m\ldots\sigma_n\ldots\sigma_i\ldots\sigma_j)$ or $(\sigma_m'\ldots\sigma_n'\ldots\sigma_i'\ldots\sigma_j')$ is k. F will become F' because $(\sigma_m\ldots\sigma_n\ldots\sigma_i\ldots\sigma_j)$ in F' has changed into $(\sigma_m'\ldots\sigma_n'\ldots\sigma_i'\ldots\sigma_j')$. It is clear that the F' will have any k bits different from F if A has been changed with k bits. But It is unclear which k bits have been changed.

$\Rightarrow E=\mathrm{Per}(K_3,Rot(n_2,n_2))\oplus\mathrm{Per}(n_1,K_3\oplus K_2)=\{\tau_0\tau_1\tau_2\ldots\tau_m\ldots\tau_n\ldots\ \tau_i\ldots\tau_j\ldots\tau_{l+1}\tau_l\}$

$E'=\mathrm{Per}(K_3,Rot(n_2',n_2'))\oplus\mathrm{Per}(n_1,K_3\oplus K_2)=\{\tau_0'\tau_1'\tau_2'\ldots\ \tau_m'\ldots\ \tau_n'\ldots\ \tau_i'\ldots\ \tau_j'\ldots\tau_{l+1}'\tau_l'\}$

$\bigcup_{i=0}^{l}(\tau_i)-(\tau_m\ldots\tau_n\ldots\ \tau_i\ldots\tau_j)=$

$\bigcup_{i=0}^{l}(\tau_i')-(\tau_m'\ldots\ \tau_n'\ldots\ \tau_i'\ldots\ \tau_j')$

The total elements number of $(\tau_m\ldots\tau_n\ldots\ \tau_i\ldots\tau_j)$ or $(\tau_m'\ldots\ \tau_n'\ldots\ \tau_i'\ldots\ \tau_j')$ is k. E will become E' because $(\tau_m\ldots\tau_n\ldots\ \tau_i\ldots\tau_j)$ in E' has changed into $(\tau_m'\ldots\ \tau_n'\ldots\ \tau_i'\ldots\ \tau_j')$.

The guess method can be used to detect the probability of the authentication success to be $P=1/(2^k*C_{L-k+1}^{k})$

$\Rightarrow$if $(E'==\mathrm{Per}(K_3,Rot(n_2',n_2'))\oplus\mathrm{Per}(n_1,K_3\oplus K_2))$

Output("desynchronization attack Success")

In normal circumstances, a reader sends the message A to a tag at the step 3. The reader will also send the message E to the tag to pass the authentication at the step 5. The example in the following figure shows that an attacker can change the two bits of the message A at the step 3, then send the guessing message E' which has two bits different from the original message E. It is clear that two bits have been changed on E to make E'. It is uncertain that which two bits have been changed. Finally, the attacker will have a certain probability to guess E' to pass the authentication at the step 5.

For Example:

E

…	**0**	1	0	1	…	1	0	1	1	0	0	1	**1**

m **n**

E'

…	1	0	1	1	…	0	1	**1**	**0**	1	0	0	1

m' n'

2.2.3 Vulnerability Verification

	Input	Output
Tag	K_1=2646 K_2=2982 K_3 =3750	K_1=2033 K_2=1311 K_3 =3703
Tag	TmetaID=149	TmetaID=3807
Server	K_1^{new}=2646 K_2^{new} =2982 K_3^{new} =3750	K_1^{new}=2033 K_2^{new} =1819 K_3^{new} =2809
Server	K_1^{old} = K_2^{old} = K_3^{old} =	K_1^{old} =2646 K_2^{old} =2982 K_3^{old} =3750
Server	$DmetaID^{New}$=149	$DmetaID^{New}$=3807
Server	$DmetaID^{Old}$=	$DmetaID^{Old}$ =149
Mes	n_1=3353 n_2=2413	A =453 B =3647 C=1984 D=1181 E=3609

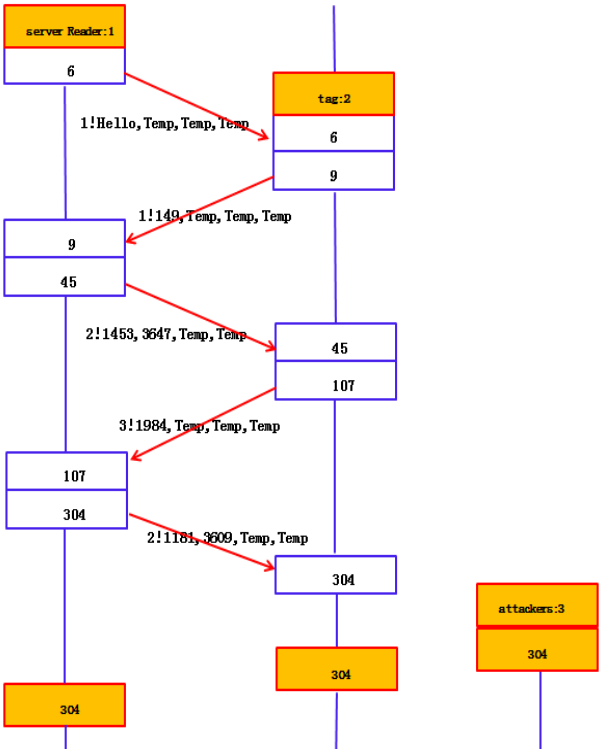


Figure 2 The SPIN Model of the UAPP

Furthermore, we use the formal verification tool, SPIN, to simulate the attack process with setting k = 2 (k< l). It is assumed that the n_2 and n_2' are two bits different, the effects of the E and E' with two bits of permutation order is unobvious. It is assumed that two bits are affected with permutation order are $m' \in (1 \ldots l)$ and $n' \in (1 \ldots l)$. It is divided into $P=1/(2^{L-k}{}_{*}C_{L-k+1}^{k})$ situations to test the two bits of the m' and n'. Finally, the E' will pass the tag's authentication. The m' and n' are the two bits changed to make E becoming E'. $E'=\mathrm{Per}(K_3, Rot(n_2', n_2')) \oplus \mathrm{Per}(n_1, K_3 \oplus K_2)$.

The Figure 2 shows the SPIN model with the values of input and output variables used in the UAPP scheme. The Figure 3 shows the SPIN model of the UAPP scheme under a desynchronization attack. In the process of the attack, an attacker attempts to change k bits of D. Then the k bits of n_2 will be affected by D at the same time. Furthermore， the k bits of D and E will be affected too. The attacker tries to guess the value of k bits of D and E to forge D' and E' to pass the step 6 of the authentication process. The experiments show if the forged D'=1179 and E'=2905 pass the authentication with the tag, the authentication will be desynchronized in the next round of authentication. It is obvious to conclude that the desynchronization attack is successful.

	Input	Output
Tag	K_1=2033 K_2=1819 K_3 =2809	K_1=2633 K_2=1311 K_3 =3703
Tag	$TmetaID$=3807	$TmetaID$=2775
Server	K_1^{new}=2033 K_2^{new} =1819 K_3^{new} =2809	K_1^{new}=2033 K_2^{new} =1819 K_3^{new} =2809
Server	K_1^{old} =2646 K_2^{old} =2982 K_3^{old} =3750	K_1^{old} =2646 K_2^{old} =2982 K_3^{old} =3750
Server	$DmetaID^{New}$=3807	$DmetaID^{New}$=3807
Server	$DmetaID^{Old}$=149	$DmetaID^{Old}$ =149
Mes	n_1=3353 n_2'=2477	A =453 B =3647 C=1984 D'=1179 E'=2905

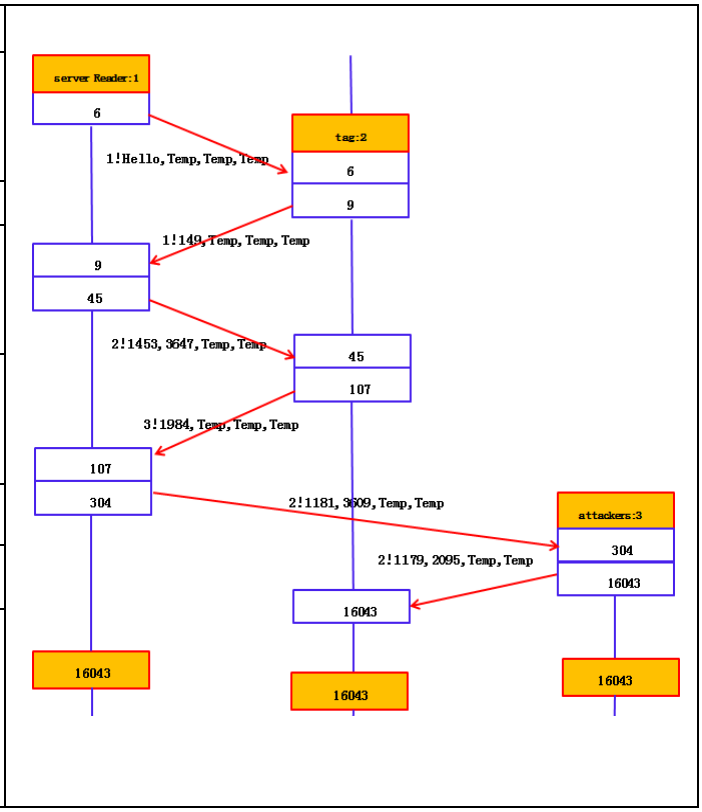


Figure 3 The SPIN Model of UAPP under the Attacks

3. The Proposed LPCP Scheme

3.1 Design of the LPCP Scheme

As an ultralightweight protocol, the major drawback of the UAPP scheme is that it has not considered the correlation of the message transmission. Any attackers could make good use of this flaw to attack the UAPP scheme. If we can reduce the relevance of the variables without increasing the cost of tag, it will become a better solution to overcome the shortcoming. Figure 4 illustrates the specification of the

protocol. The details of the messages exchanged are presented below. Table 2 shows the notations of the proposed LPCP scheme.

Table 2 Notation

Symbol	Meaning
$\oplus$	XOR operator
CRC-16(X)	CRC-16 is an efficient checksum algorithm. By the proposed protocol, the input X is divided into groups, each has 16 bits. Each 16-bit group will be encrypted one by one. The output of each is a 16-bit encrypted data. Each output will be combined together.
n	n is the secret key length
R_1	a random number
R_2	a random number
TID^{old}	the previous *TID* key in the back-end server
TID^{new}	the current *TID* key in the back-end server
Key^{old}	contains 3 secret key storage rooms $KeyH^{old}$, $KeyM^{old}$, $KeyL^{old}$ which are used to keep the previous secret key in the back-end server
Key^{new}	contains 3 secret key storage rooms $KeyH^{new}$, $KeyM^{new}$, $KeyL^{new}$ which are used to keep the current secret key in the back-end server
TID_T	The tag's unique serial number
key_T	contains 3 secret key storage rooms Key_TH, Key_TL, Key_TM which are used to keep the tag secret key
$\alpha, \beta, \gamma, \delta, \zeta$	$\alpha, \beta, \gamma, \delta,$ and ζ are the variables which are used to send message between the tag and reader, for example α is used to send the random number R_1 with a mask to the tag. And the tag will extract R_1 by XOR α with CRC(Per(*KeyM, KeyH*)).

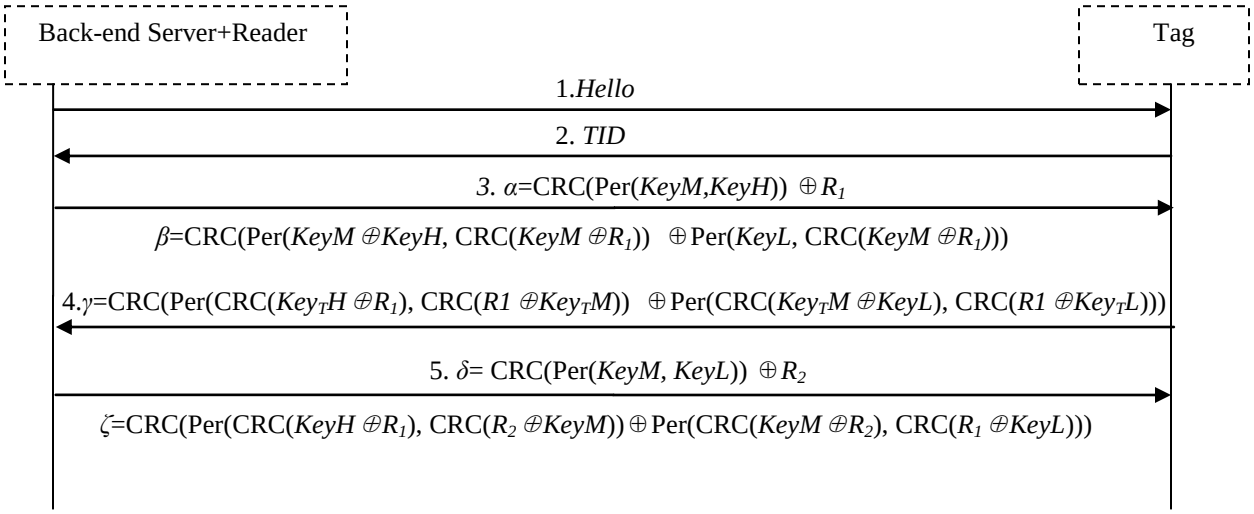
3.2 Operations of the LPCP Protocol

1. The reader sends a "Hello" message to the tag to initiate a protocol session.

2. Upon receiving the reader's query, the tag transmits TID_T to the reader.

3. After receiving TID_T, the reader uses it as an index to search a matched entry in the database. If it is an old *TID*, the reader will use { $KeyH^{old}$, $KeyM^{old}$, $KeyL^{old}$ } to computer the messages. If *TID* is new, { $KeyH^{new}$, $KeyM^{new}$, $KeyL^{new}$ } will be used. If *TID* is not in the database, the reader will terminate the session as this may be an invalid tag. Suppose the reader has found { *KeyH, KeyL, KeyM* } as the tag's entry. It will generate an n-bit random number R_1 and compute α and β. α is used to send the random

number R_1 with a mask to the tag. The purposes of β include the authentication of the reader and the integrity of the messages. Then α and β are sent to the tag.



Updating: 1)if TID^{old} is received TID^{New}= CRC(Per(TID^{old}, R_1 ⊕R_2) ⊕$KeyH^{old}$ ⊕$KeyM^{old}$ ⊕$KeyL^{old}$) $KeyH^{new}$= CRC(Per ($KeyH^{old}$, R_1) ⊕$KeyM^{old}$) $KeyM^{new}$= CRC(Per ($KeyM^{old}$, R_2) ⊕$KeyH^{old}$) $KeyL^{new}$= CRC(Per ($KeyL^{old}$, R_1 ⊕R_2) ⊕TID^{old}) 2)if IDS^{New} is received TID^{old}= IDS^{new}, $KeyH^{old}$= $KeyH^{new}$ $KeyM^{old}$=$KeyM^{new}$, $KeyL^{old}$=$KeyL^{new}$ TID^{New}= CRC(Per(TID^{old}, R_1 ⊕R_2) ⊕$KeyH^{old}$ ⊕$KeyM^{old}$ ⊕$KeyL^{old}$) $KeyH^{new}$= CRC(Per ($KeyH^{old}$, R_1) ⊕$KeyM^{old}$) $KeyM^{new}$= CRC(Per ($KeyM^{old}$, R_2) ⊕$KeyH^{old}$) $KeyL^{new}$= CRC(Per ($KeyL^{old}$, R_1 ⊕R_2) ⊕TID^{old})	Updating: Key_TH = CRC(Per (Key_TH, R_1) ⊕Key_TM) Key_TM= CRC(Per (Key_TM, R_2) ⊕Key_TH) Key_TL= CRC(Per (Key_TL, R_1 ⊕R_2) ⊕TID)

Figure 4. The Operation of the LPCP Protocol

4. The tag extracts R_1 by XOR α with CRC(Per(*KeyM, KeyH*)) and computes a local value of β. If the local value of β is equal to the received β, the tag will compute and transmit γ to the reader. Otherwise, the tag will do nothing because the received messages may be modified or sent by an unauthenticated reader.

5. When receiving γ, the reader will compare it with the local γ to authenticate the tag. If the tag is authenticated, the reader will generate another n-bit pseudo random number R_2. Both R_1 and R_2 will be used for the key update. The reader computes δ and ζ , then the reader sends δ and ζ to the tag. Then the reader will update the corresponding tag entry.

6. The tag extracts R_2 from δ and computes a local value of ζ. If the local value of ζ equates to the received ζ, the tag will authenticate the reader and update the pseudonym and the secret keys.

We analyze the security of the LPCP scheme in two main aspects: the security functionality and the ability to resist various malicious attacks. We show that the proposed LPCP scheme has the ability to prevent various attacks including the desynchronization attacks, tracing attacks, replay attacks, and disclosure attacks.

4.1 Data Confidentiality

In terms of data confidentiality, the messages $\alpha, \beta, \gamma, \delta$ and ζ are all related to the shared keys between the reader and the tag. Moreover, it is difficult to recover the random numbers and the tag *TID* without knowing these keys. As *KeyH* and *KeyM* are kept secret, it is impossibility to guess the *KeyH*, *KeyM* or R_1 from the possible combinations of Per(*KeyM, KeyH*) and R_1. So the data confidentiality can be assured. And the messages β and ζ cannot only provide the evidence for authentication of the reader, but also can assure the integrity of the messages. For example, if an adversary tries to modify R_1 by flipping certain bits in α, the tag cannot verify the messages since β is invalid. However, it is very difficult for the adversary to adjust β to a correct value since the CRC(Per(*KeyM* $\oplus$*KeyH*, CRC(*KeyM* $\oplus R_1$)) $\oplus$ Per(*KeyL*, CRC(*KeyM* $\oplus R_1$))) ensures that little change in R_1 will lead to a very different output.

4.2 Resistance to Desynchronization Attacks

The proposed LPCP scheme can resist the particular desynchronization attacks and overcome the defect of the UAPP scheme. By the LPCP scheme, a checksum code can be used to provide security. The checksum code is often used to check the integrity of data being sent or received, while the popular cryptographic checksum codes are cryptographic hash function in nature such as Message Authentication Codes (MAC) and Hash-based Message Authentication Codes (HMAC). In this paper, we make use of the well-known, efficient (yet less cryptographically strong) checksum arithmetic, namely CRC-16. According to the specification of the EPC global Class-2 Gen-2, a 16-bit CRC checksum is used to detect

errors in the transmission of data. Since the CRC-16 is not reversible like the MD5, which is equivalent to a one-way function. The CRC-16 function can reduce the correlation of the transmitting message without increasing any cost. In order to verify that the proposed LPCP scheme has the ability to resist the particular desynchronization attacks, the formal verification tool of SPIN is used to perform the formal verification. Figure 5 shows the SPIN model built with the values of the input and the output variables of the LPCP scheme in the authentication process. The reader and the tag will compute α=17605, β=39157, γ=61304, δ=12957 and ζ=41294 in terms of R_1 =64793 and R_2 =43373 which are two random number produced by the reader. Experiment shows that if there is no attack, the messages $\alpha, \beta, \gamma, \delta, \zeta$ are able to pass the authentication by the LPCP scheme.

	Input	Output
Tag	Key_TH=55894 Key_TM=48038 Key_TL=52902	Key_TH =25229 Key_TM=12155 Key_TL=44031
Tag	TID=149	TID=43359
Server	$KeyH^{new}$=55894 $KeyM^{new}$ =48038 $KeyL^{new}$ =52902	$KeyH^{new}$=25229 $KeyM^{new}$ =12155 $KeyL^{new}$ =44031
Server	$KeyH^{old}$ = $KeyM^{old}$ = $KeyL^{old}$ =	$KeyH^{old}$ =55894 $KeyM^{old}$ =48038 $KeyL^{old}$ =52902
Server	TID^{new}=149	TID^{new}=43359
Server	TID^{Old}=	TID^{Old} =149
Mes	R_1=64793 R_2=43373	α =17605 β=39157 γ=61304 **δ=12957** **ζ=41294**

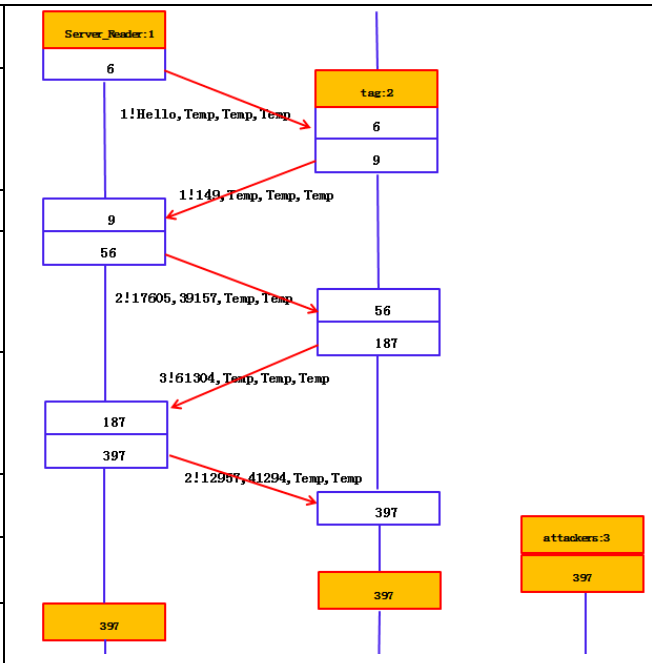


Figure 5 The SPIN Model of the LPCP

The Figure 6 shows the SPIN model of the operation of the proposed LPCP scheme under a desynchronization attack. In the process of the attack, the attacker changes two bits of α. The value of the δ and ζ will be changed to δ' and ζ' due to the changes of α. Originally, δ is *12957*, while it could be changed to δ'=*92499*. And correspondingly, ζ =*41294*, it could be changed to ζ'=*21199*. Then, ζ' will be sent to the tag for the authentication by the reader. It is shown by the experiment result, the attack is not

able to cheat the tag to get it authenticated by the proposed LPCP scheme due to its use of XOR operation, build-in CRC-16 function, permutation and the secret key backup technology. It is clear that the proposed solution has a strong ability to prevent the particular desynchronization attacks.

	Input	Output
Tag	Key_TH=55894 Key_TM=48038 Key_TL=52902	Key_TH =55894 Key_TM=48038 Key_TL =52902
Tag	TID=149	TID=43359
Server	$KeyH^{new}$=55894 $KeyM^{new}$ =48038 $KeyL^{new}$ =52902	$KeyH^{new}$= $KeyM^{new}$ = $KeyL^{new}$ =
Server	$KeyH^{old}$ = $KeyM^{old}$ = $KeyL^{old}$ =	$KeyH^{old}$ =55894 $KeyM^{old}$ =48038 $KeyL^{old}$ =52902
Server	DID^{New}=149	DID^{New}=
Server	DID^{Old}=	DID^{Old} =149
Mes	R_1=64793 R_2=43373	α =17605 β =39157 γ=61304 **δ=92499** **ζ=21199**

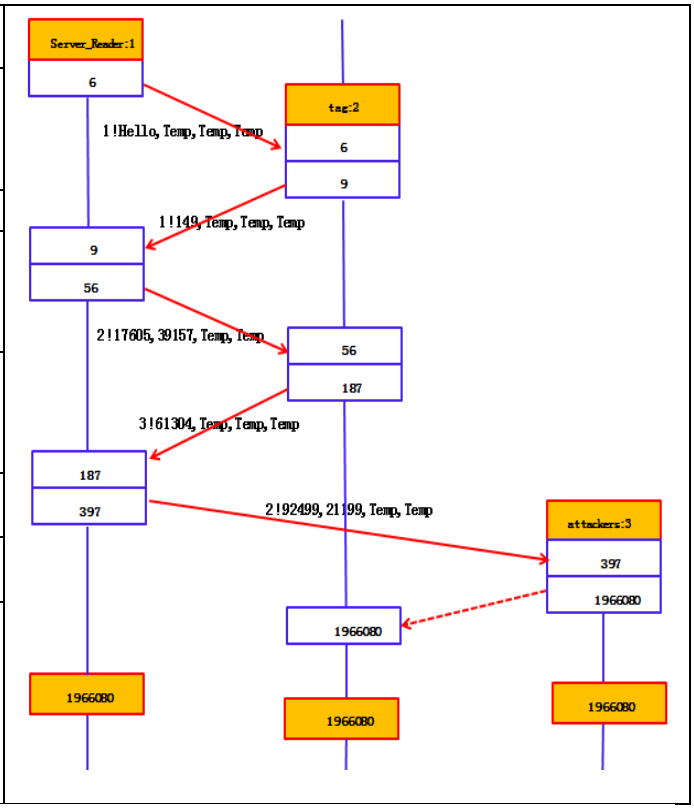


Figure 6 The SPIN Model of the LPCP under an Attack

4.3Resistance to Tracing Attacks

A tracing attack is the most powerful attack which could be issued by a "malicious active reader". The goal of the attack is to discover the presence of a specific tag. The attacker actively scans the tag from a far distance and logs all the RF signals by the small device near the tag. If the tag replies a message twice, such as the same *TID*, it can be traced. By the proposed LPCP scheme, changing the value of R_1, R_2 makes the resulted α, β , γ , δ and ζ changed in each communication process, while *TID* must be updated after each authentication process. In this way, the proposed protocol can resist various tracing attacks well.

4.4 Resistance to Replay Attack

If a malicious reader attempts to retransmit α=CRC(Per(*KeyM*,*KeyH*)) $\oplus R_1$ and β=CRC(Per(*KeyM*$\oplus$*KeyH*, CRC(*KeyM*$\oplus R_1$))$\oplus$Per(*KeyL*, CRC(*KeyM*$\oplus R_1$))), which have been intercepted by the reader at step 3, to pass the authentication with the tag, the tag will extract the retransmitted α to form the R_1 by XOR α with CRC(Per(*KeyM*, *KeyH*)). The tag can use the R_1 and the secret key to calculate the local β' and compare it with the retransmitted β to pass the authentication of the step 4. In the next step, the tag sends γ which is calculated from the forged R_1 by the reader. But the authentication will fail because the reader cannot identify the forged R_1 which produces by the reader and the value of R_1 will be changed in each round, so the malicious reader is not able to forge γ=CRC(Per(CRC($Key_T H \oplus R_1$), CRC($R_1 \oplus Key_T M$))$\oplus$Per(CRC($Key_T M \oplus$*KeyL*), CRC($R_1 \oplus Key_T L$))). Therefore, we can conclude that the LPCP can resist the replay attacks.

4.5 Resistance to Disclosure Attack

The XOR operation on two or more messages sent in the session cannot disclose any secrets. If an adversary obtains α=CRC(Per(*KeyH*,*KeyM*))$\oplus R_1$, he cannot determine *KeyH* or *KeyM* or R_1 because there are many possible pairs that will result in the same value as CRC(Per(*KeyH*,*KeyM*)) and R_1. The adversary may use modify-and-test method to guess the secrets. For example, the adversary can modify α and β and send the modified messages to the tag to test the correctness of the modification. However, due to the introduction of the CRC function, which has the one-way function features, so it is impossibility to guess the *KeyH*, *KeyM* or R_1 from many possible combinations of Per (*KeyH*, *KeyM*) and R_1. In this way the proposed protocol can resist the disclosure attack.

5. Performance Evaluation

Figure 7 shows the logic diagram of the proposed LPCP scheme. Due to the fact that a message consists of three or more pieces, it requires one *n*-bit register to temporarily store intermediate results. The core component of the LPCP logic is the Arithmetic Logic Unit (ALU). The ALU has two inputs and one control signal. One of the inputs is the data path for data to be fetched from the register, while another is the bit stream from outside. The control to the ALU is the control signal (C_1) to select the input to the ALU from either the bit stream or the data stored in the register. The control signal C_2 will determine the operation that will be performed in the ALU.

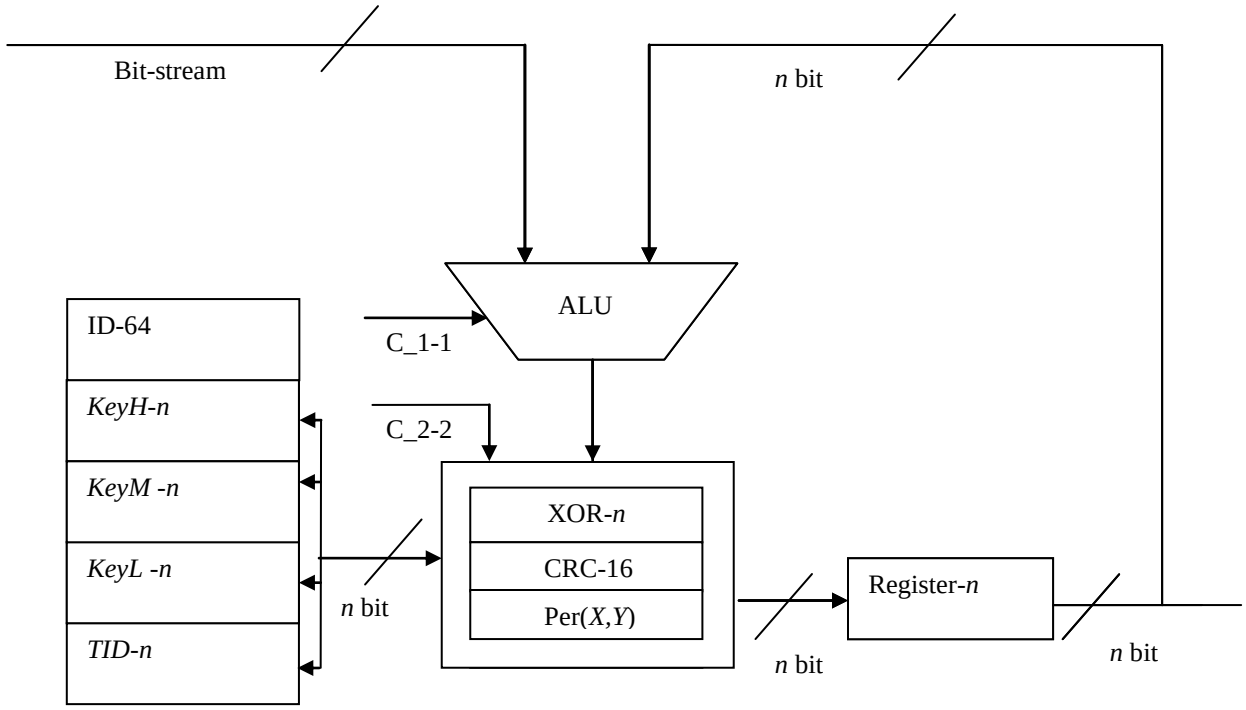


Figure 7 Logic Scheme of LPCP

Table 3 Comparison of Logical Gates and Length of the Secret Key

Key length（*n*）	8-bit	16-bit	32-bit	64-bit	96-bit	128-bit	256-bit
Gates number	99	131	195	323	451	579	1091

Table 3 shows the comparison of logical gates and length of the secret key. Hash function like MD5 generally needs 16000 logical gates. SHA-1 needs 20000 logical gates. The number of the logical gates required by the proposed protocol is much less than that of the protocols equipped with the hash functions obviously. Therefore, the proposed LPCP scheme is suitable for the low cost RFID systems.

We analyze the performance of the proposed LPCP scheme in terms of the computation operations, the storage requirements and the communication costs for each tag. The computation operations are indicated by the types of operations required for each tag. The storage requirements are measured by the memory size required to store a static tag ID and the shared elements in a tag. The communication costs are calculated by the amount of the messages sent by the tag in one protocol execution. The comparison results among the solution in [23] and some other protocols are listed in Table 4. In Table 4, "+" denotes the addition mod 2^L.

Table 4 Performance Comparison of Some Ultralightweight Authentication Protocols

	M^2AP [18]	SASI [6]	Gossamer [21]	UAPP[23]	LPCP
Types of computation operations	+, ⊕, AND, OR	+, ⊕, OR, Ror	+, ⊕, Ror, MixBits	⊕, Ror, Per	⊕, Per, CRC-16
Storage requirement	6L	7L	7L	5L	5L
Communication messages	3L	2L	2L	2L	2L
Resistance to desynchronization attacks	No	No	No	No	Yes
Resistance to disclosure attacks	No	No	Yes	Yes	Yes
Resistance to tag tracking	No	No	Yes	Yes	Yes

6. Conclusion

In this paper, we have reviewed the UAPP scheme with the vulnerability exploration. It is discovered that the UAPP scheme cannot resist one particular type of desynchronization attacks. In order to overcome the vulnerability, we have proposed a close to ultralightweight RFID authentication protocol which integrates the operation of the XOR operator, build-in CRC-16 function, permutation and the secret key backup technology to enhance the security functionality without increasing any security cost. We have formally verified the security functionality of the proposed scheme by using SPIN. Analysis shows that our proposal has a strong ability to prevent most possible malicious attacks.

ACKNOWLEDGMENTS

This work was partially supported by the National Natural Science Foundation of China (NSFC) under grant No. 61072063, 61202379.

Reference

[1] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, Vol. 24, No 2, Feb. 2006, pp. 381-394.

[2] H. M. Sun and W. C. Ting," A Gen2-based RFID Authentication Protocol for Security and Privacy," IEEE Transactions on Mobile Computing, Vol. 8 , No 8, Aug. 2009, pp. 1052-1062.

[3] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-frequency Identification: Secure Risks and Challenges," RSA Laboratories Cryptobytes, Vol. 6, No.1, Jan. 2003, pp.2-9.

[4] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices," Massachusetts Institute of Technology, 2003.

[5] A. Juels, R. L. Rivest, and M. Szydlo, "The Bblocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proceedings of the l0th ACM Conference of Computer and Communications Security, 2003, pp.l03-111.

[6] H. Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," IEEE Transaction of Dependable and Secure Computing, Vol. 3, No. 4, Oct 2007, pp. 337-340.

[7] S. E. Sarma, S. A. Weis and D. W. Engels, "RFID Systems and Security and Privacy Implications," Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, Nov 2003, pp.454-469.

[8] D. Henrici, and P. Muller, "Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers," Proceedings of 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops, Mar 2004, pp.149-153.

[9] L. Gao, M. Ma, Y. Shu, and Y. Wei, "A Security Protocol Resistant to Intermittent Position Trace Attacks and Synchronization Attacks in RFID Systems," Wireless Personal Communications, Vol. 68, No. 4, Feb 2013, pp. 1943-1959.

[10] S. Zhou, Z. Zhang, and Z. Luo, "A Lightweight Anti-desynchronization RFID Authentication Protocol," Information Systems Frontiers, Vol. 12, No. 5, Nov 2010, pp. 521–528.

[11] A. Blurn, M. Furst, and M. Keams, "Cryptographie Primitives Based on Hard Leaming Problems," Advances in Cryptology-CRYPTO, 1993, 1-10.

[12]A. Juels and S. A. Weis, "Authenticating Pervasive Devices with Human Protocols," Advances in Cryptology–CRYPTO, Aug 2005, pp. 293-308.

[13] J. Bringer, H. Chabanne, and E. Dottax, "HB++: a Lightweight Authentication Protocol Secure against Some Attacks," Proceedings of IEEE International Conference on Pervasive Services Workshop on Security, Jun 2006, pp.28-33.

[14] S. Piramuthu, "HB and Related Lightweight Authentication Protocols for Secure RFID Tag/reader Authentication," Proceedings of the CollECTeR Conference, June 2007, pp. 1-8.

[15] D. N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," White Paper, 2006, 1-11.

[16] R. Doss, S. Saravanan, and W. L. Zhou," A Practical Quadratic Residues Based Scheme for Authentication and Privacy in Mobile RFID Systems," Ad Hoc Networks, Vol. 11, No. 1, June 212, pp. 383-396.

[17] R. Doss, W. L. Zhou, S. Saravanan, S. Yu, and L. X. Gao, "A Minimum Disclosure Approach to Authentication and Privacy in RFID Systems, " Computer Networks, Vol. 56, No. 15, Oct. 2012, pp. 3401-3416.

[18] P. P. Lopez and J. H. Castro, "M^2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags," Proceedings of the International Conference on Ubiquitous Intelligence and Computing, Sep 2006, pp. 912-923.

[19] M. Bárász, B. Boros, and P. L. K. Lója, “Passive Attack Against the M^2AP Mutual Authentication Protocol for RFID Tags,” Proceedings of the First International Workshop on RFID Technology, 2007, pp. 1-4.

[20] H. M. Sun, W. C. Ting, and K. H. Wang, “On the Security of Chien's Ultralightweight RFID Authentication Protocol,” IEEE Transaction Dependable and Secure Computing, Vol. 8, No. 2, Mar. 2011, pp. 315-317.

[21] P. Peris-Lopez, J. C. Hernandez-Castro, and J. M. E. Tapiador, “Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol,” Proceedings of the 9th International Workshop on Information Security Applications, Aug. 2009, pp. 56-68.

[22] E. G. Ahmed, E. Shaaban, and M. Hashem,” Lightweight Mutual Authentication Protocol for Low Cost RFID Tags,” Journal of Network and Computer Applications, Vol. 2,No. 2, Apr. 2010, PP. 27-37.

[23] Y. Tian, G. L. Chen, and J. H. Li, "A New Ultralightweight RFID Authentication Protocol with Permutation," IEEE Communications Letters, Vol. 16, No. 5, May 2012, pp. 702-705.

[24] D. Paolo, and A. D. Santis, "On Ultralightweight RFID Authentication Protocols," IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 4, Aug 2011, pp. 548-563.

[25]G. Avoine, X. Carpent, and B. Martin, “Privacy-friendly Synchronized Ultralightweight Authentication Protocols in the storm, “Journal of Network and Computer Applications, Vol. 35, No. 2, March 2012, pp. 826–843.

Author Biographies

Lijun Gao received his B.Sc. and M.Sc. degrees in Department of Computer Science and Technology, Shenyang Aerospace University in 2000 and 2007 respectively. He has been a lecturer at Shenyang Aerospace University since 2005. He has extensive research interests including wireless networking and wireless network security, etc. He is currently pursuing his Ph.D. at the Department of Computer Engineering, Tianjin University, doing research on the RFID security.

Dr. Maode Ma received his Ph.D. degree in computer science from Hong Kong University of Science and Technology in 1999. Now, Dr. Ma is an Associate Professor in the School of Electrical and Electronic Engineering at Nanyang Technological University in Singapore. He has extensive research interests including wireless networking and network security. Dr. Ma has more than 250 international academic publications including over 100 academic journal papers and more than 130 international conference papers. He currently serves as the Editor-in-Chief of *International Journal of Electronic Transport.* He also serves as an Associate Editor for other 5 international academic journals. Dr. Ma is a Fellow of *IET* and a senior member of *IEEE Communication Society and IEEE Education Society.* He is the vice Chair of the *IEEE Education Society*, Singapore Chapter. He is also as an *IEEE Communication Society Distinguished Lecturer*.

Yantai Shu was a visiting scholar at UCLA in 1981-1984. Yantai Shu is a professor of computer science at Tianjin University, China. He is a member of the IEEE and the ACM. He has published more than 120 papers and contributed to one book. His current interests are focused on computer communication networks, wireless networks, real-time systems, modeling and simulation.

Yuhua Wei received her B.Sc. degrees in Department of Computer Science and Technology, Shenyang Aerospace University in 2005. She has extensive research interests including wireless networking and wireless network security, etc. She is currently pursuing her M.Sc. degrees at the Department of Computer Science and Technology, Shenyang Aerospace University, doing research on the network security.