An Efficient and Secure RFID Authentication Scheme for C1G2 Standard

Chen-Yang Cheng[1], Cheng-Ta Huang[2], Iuon-Chang Lin[3,4], Hung-Huei Hsu[3]

[1] Department of Industrial Engineering and Management, National Taipei University of Technology, Taiwan
[2] Department of Information Management, Oriental Institute of Technology, Taiwan
[3] Department of Management Information Systems, National Chung Hsing University, Taiwan
[4] Department of Photonics and Communication Engineering, Asia University, Taiwan
cycheng@ntut.edu.tw, cthuang@mail.oit.edu.tw, iclin@nchu.edu.tw, vc2541@hotmail.com

Abstract

Radio frequency identification promotes many applications for automatic identification such as supply chain, thief-prevention. The messages of RFID system are transmitted by radio waves, attackers can carry on common wireless attacks. The technology may incur user privacy and cause security problem. The popular of RFID system depends on low cost. EPCglobal introduces a new standard for low cost tags, called C1G2 standard. Many researchers devote to design authentication protocols which comfort to C1G2 standard. Predo introduced a new lightweight authentication scheme which compliant to C1G2 standard, called "Azumi protocol". The scheme needs an exclusive search in database during authentication phase and suffers security problems such as revealing of secret, impersonate attack. We present our attacks and point out the problems on Azumi protocol. We propose an improved scheme and analysis our scheme for security and performance. Our scheme can achieve high security level and efficient performance. Our scheme is compliant to requirements of C1G2 standard.

Keywords: Radio frequency identification, C1G2 standard, Mutual authentication, Low-cost tag

1 Introduction

Radio frequency identification (RFID) is the critical technology in recent years. Comparing with line-sight of barcodes, RFID technology can identify lots of tags at the same time. The convenience properties of RFID technology promote the development of many applications. The technology is used to many applications of automatic identification such as supply-chain management, thief-prevention, E-passport and entrance guard system. The system can identify the tagged items in the range of readers but the advantages may be utilized by malicious users. The messages in RFID system are transmitted by radio waves. RFID system suffers from some attacks in wireless network. Attacker may eavesdrop, modify and resend the message to trace or impersonate a legal entity. If the tagged object can be traced by attacker, the privacy of the user or business will be incurred. Malicious user may impersonate as a legal entity to cheat other legal entities. To against common attacks, reader and tag must authenticate each others. The popular of RFID system depends on the low price of the tag [1]. We should prevent the privacy problems and against most of possible attacks within the limit resources.

EPCglobal is an organization leading the development of RFID standards for Electronic Product Code (EPC) and the goal of EPCglobal is increasing efficiency between supply chain partners which apply the RFID system [2-3]. EPCglobal introduced a new standard for RFID lightweight tags, called Class-1 Generation-2 standard (C1G2 standard in short). The C1G2 standard defined the specification of lightweight tags in storage and computation capacities. Many researchers devoted to design lightweight authentication protocols but the schemes still suffer from privacy problems or security attacks. The utralightweight scheme which only uses simple bitwise computation was presented by Chien [4]. The novel schemes use error correction code (ECC) was presented [5]. The properties of quadratic residues were using for designing authentication protocol [6-7]. But the requirements for computation capacities of the tag in above schemes are not compliant to C1G2 standard. Some authentication schemes compliant to C1G2 standard which only use simple computation like CRC and PRNG are presented [1, 8-16]. Because of the limited capacities the C1G2 standard, the designed protocols still have some weaknesses. Chen proposed a lightweight protocol fit in with C1G2 standard [9], but Predo et al. claim that Chen et al. scheme still suffers from some security problems such as traceability,

*Corresponding Author: Iuon-Chang Lin; E-mail: iclin@nchu.edu.tw
DOI: 10.3966/160792642019052003028

impersonation attack, and denial of service attack [8]. Pedro heals the weakness of Chen et al. scheme and proposed a new lightweight protocol called Azumi protocol [8]. But there were some problems in Azumi protocol such as revealing of secret and impersonate attack. Azumi protocol has been broken by Safkhani et al [17].

As mentioned previously, many researchers devote to design authentication protocols which comfort to C1G2 standard. Predo introduced a new lightweight authentication scheme which compliant to C1G2 standard, called "Azumi protocol". However, the scheme needs an exclusive search in database during authentication phase and suffers security problems such as revealing of secret, impersonate attack. Therefore, we present the attacks on Azumi protocol and propose an improved scheme. We also perform security and performance analysis for our scheme. Our scheme can reach an acceptable security level and the scheme improves the performance. Our work in proposing C1G2 protocol can promote the development of low-cost RFID system. The contributions of our work are as follows:

1. We study the related works of recently authentication protocols which comfort to C1G2 standard. In this paper we point out the security weakness of Azumi protocol and proposed an improve scheme.

2. In our scheme, pseudonym identity of the tag is transmitted to the reader during communication. Backend server first checks the pseudonym identity storing in database to identify the tag. Once the pseudonym of tag is valid, the server authenticates the tag by verifying the authentication message which is computed by corresponding secret values. It improved the traceability and performance.

3. To achieve forward secrecy, the secret values and pseudonym identity are updated in a random way after a successful authentication. Attacker cannot acquire the related information of secret updating by eavesdropping on the authentication messages.

The rest in this paper is organized as follows: We introduce C1G2 standard, security requirement and previous works in section 2. In section 3, we review Azumi protocol and present weaknesses of Azumi protocol. We introduce our scheme in section 4. In section 5, we analyses the security and performance for our scheme. Then, we make a clear conclusion in section 6.

2 Related Work

First, we introduce the C1G2 standard which proposed by EPCglobal. For clear, we only focus on the computation, storage and communication capacities. Then we introduce security requirement in RFID systems. Finally, we introduce the recent work of RFID authentication protocols.

2.1 C1G2 Standard

EPC Class 1 Generation 2 standard which introduced by EPCglobal is a new standard for low-cost RFID tags. The main content of the standard integrates four standard including Class 0, Class1, ISO18000-6A, ISO18000-6B. In 2006, the C1G2 standard incorporated with ISO18000-6C and International Organization for Standardization (ISO) validated the standard. The standard defines the operation of the lightweight RFID system as follows [2-3, 18-19]:

- The standard defines the air interface of passive tags which is used in Ultra High Frequency band (UHF,860MHz~960MHz) and the communication distance is 2- 10 meters.
- The tag with C1G2 standard supports 16-bit PRNG (Pseudo Random Number Generator, PRNG-16) and 16-bit CRC (Cyclic Redundancy Code Checksum, CRC-16).
- The tag is limited by cost and it cannot perform complex computation such as symmetric/Asymmetric encryption, hash function.
- The tag stores a 32-bit Kill password. When the tag receives the password, it cancels all the function of the tag. The reader cannot query the tag anymore.
- The tag stores a 32-bit Access password. If user enters the password, the tag is transformed to secure mode and it can write and read the preserved memory of the tag.
- The memory in the tag is defined as follows:

A. Reserved memory: It is used to store 32-bit kill password and access password.

B. EPC memory: It is used to store the information of physical layer and various versions of EPC codes.

C. TID memory: It stores 8-bit identifier and the access control information of readers.

D. User memory: It is used to store special information of the user.

The popular of RFID system depends on low cost. EPCglobal devotes to developments of RFID standard and the C1G2 standard defined the detail specification for lightweight tags. A congruous standard can promote the development of RFID applications. The standard defines storage and computation capacities of lightweight tag, operations of communication, and the transmitted commands between reader and tags. To understand all the detail of lightweight tags is contributive to develop the design of the authentication protocol.

2.2 Requirements

To protect privacy of user, the reader and the tag must against most of attacks in RFID system. We must understand the security requirement in RFID systems. A secure RFID system must have the following properties [20-21]:

- Confidentiality: The message may be eavesdropped by malicious user. In order to protect the privacy of user, the transmitted message must be encrypted. The encrypt key or secret value must be well protected. The malicious user cannot decrypt the message.
- Untraceability: Malicious user may use the reader which has the same specification to query the specific tag. If the response message of the tag is a constant value, the adversary can trace the specific tag. A secure RFID system should protect the identity of the tag not revealed by attackers.
- Mutual authentication: A malicious user may impersonate a legal tag and reader to pass the authentication. To prevent impersonation attack, reader and tag must authenticate each others. A secure authentication scheme should have capacities to against most of possible attacks.
- Forward secrecy: If a tag is compromised by the attacker, the secret keys stored in memory of tag will be revealed. If attacker can calculate more keys which uses in previous sessions, the secret information transmitted in previous session may be calculated by attacker. To protect secret information of the user, a secure RFID system should make sure that the compromised key is irrelative to other keys which use in previous sessions and the system can prevent attacker to retrieve more keys which uses in previous session.
- Backward secrecy: If a tag is compromised by the attacker, the secret keys stored in memory of tag will be revealed. A secure RFID system should prevent attacker use the compromised key to calculate more keys which use in future sessions. The secret keys which use in future should be irrelative to the keys which compromised by the attacker.

2.3 Previous Work

Many lightweight authentication protocols are presented in recent years. Chien et al. (2007) proposed an Ultra-lightweight authentication protocol which provides strong authentication and data integrity. The protocol uses exclusive-OR and simple bitwise computation to perform mutual authentication. Raphael et al. (2009) analyze the SASI protocol and point out the scheme incurs traceability problem [22]. Chien et al. (2009) present a novel authentication protocol with a linear Error Correction Codes (ECC) [5]. Although the scheme can prevent synchronization problem, the scheme needs more storage spaces with increasing number of tags. The system cannot achieve scalability. Chen et al. (2008) proposed a novel RFID authentication scheme based on quadratic residues to enhance location privacy protection [6]. Chen's scheme suffers from tag impersonate attack, traceability problem and replay attack [7]. Yeh et al. (2011) heal the problems of Chen's scheme and proposed an improved scheme. Many researches devoted to design authentication scheme which comfort C1G2 standard are proposed. The standard define specific the limitation in resource of low-cost tags which including computation capacity, storage, memory. The following section we discuss the schemes which comfort C1G2 standard. Chien et al. (2007) proposed a mutual authentication protocol and the scheme use CRC and PRNG which is friendly to C1G2 standard [12]. Wang et al. (2011) point out that Chien's mutual authentication protocol has some security weakness due to the mathematic properties of CRC function [13]. Wang heal the weakness and present an improved scheme. Moessner et al. (2011) propose a novel cryptographic authentication protocol comfort for C1G2 standard [11]. The scheme shares a key table between reader and tag. But the scheme needs high communication cost during authentication and the reader and tag needs high storage spaces to store key tables. Chen and Deng (2009) proposed a mutual authentication scheme and the scheme only use simply CRC and PRNG function [9]. Pedro et al. (2011) present the attacks on Chen and Deng scheme and claim that Chen and Deng scheme suffers from reader impersonation, tag impersonation, traceability [8]. Pedro healed the problem and proposed a new scheme which is called Azumi protocol and claimed that Azumi protocol can achieve the security level and performance.

Elliptic curve cryptography (ECC) has been proved to enhance the higher security level of RFID protocol. Liao and Hsiao proposed an elliptic curve cryptography-based RFID authentication scheme and applied the ID-verifier transfer protocol to fulfill security requirements in RFID system [23]. Furthermore, Li et al. improved Liao and Hsiao's authentication protocol against identified attacks [24]. He et al. propose a new ECC based RFID authentication integrated with an ID verifier transfer protocol that overcomes the weaknesses of the existing schemes [25]. Chou proposed a elliptic curve cryptography RFID authentication protocol to avoid desynchronization, impersonation, and tracking attacks [26].

3 The Comparison of Azumi Protocol

Pedro claimed that Chen and Deng scheme suffers from reader impersonation, tag impersonation, traceability. Pedro healed the problems and proposed a new scheme which called Azumi protocol. Pedro claimed that Azumi protocol can achieve the security level and performance. In order to analyzethe Azumi protocol, we present the weakness of Azumi protocol. Unfortunately, there are some weaknesses in Azumi protocol. We point out the weaknesses of Azumi protocol as follows: (1) Full searching during authentication (2) Leakage of secret (3) Tag

impersonation. Azumi protocol consists of two phase: (1) Initial phase. (2) Authentication phase. Table 1 shows the notations of Azumi protocol:

Table 1. Notations of Azumi protocol

Notations	Descriptions
N_{16Ti}	32-bit access password N_{Ti} is cutting into two 16-bit fragment and the two fragments are exclusive-OR to form N_{16Ti}
K_{16Ti}	32-bit kill password K_{Ti} is cutting into two 16-bit fragment and the two fragments are exclusive-OR to form K_{16Ti}
EPC_{16Ti}	96-bit access password N_{Ti} is cutting into six 16-bit fragment and the six fragments are exclusive-OR to form EPC_{16Ti}
ID_{16R}	A 16-bit identity of reader
M_{req}	Request message sent by reader
M_{resp}	Response message sent by reader
RND	16-bit random number
CRC ()	16-bit cyclic redundancy code function
PRNG ()	One-way pseudo random number generator
$\oplus$	Exclusive-OR

3.1 Initial Phase

There are three roles in the scheme, reader, tag and database. First the tag_i stores $\{EPC_{Ti}, N_{16Ti}, K_{16Ti}\}$ in its memory. The database stores EPC_{16Ti}, old and new values of secret (N_{16Ti}, K_{16Ti}) for each tags. The old and new values of the secret for the tag are set initially as follows:

$$N_{16T_i}^{old} = N_{16T_i}^{new}, K_{16T_i}^{old} = K_{16T_i}^{new}$$

3.2 Authentication Phase

In most of schemes, we assume that the channel between the reader and the database is a secure channel. So we can combine the reader and database as the same instance. The following is the authentication phase of Azumi protocol (Figure 1):

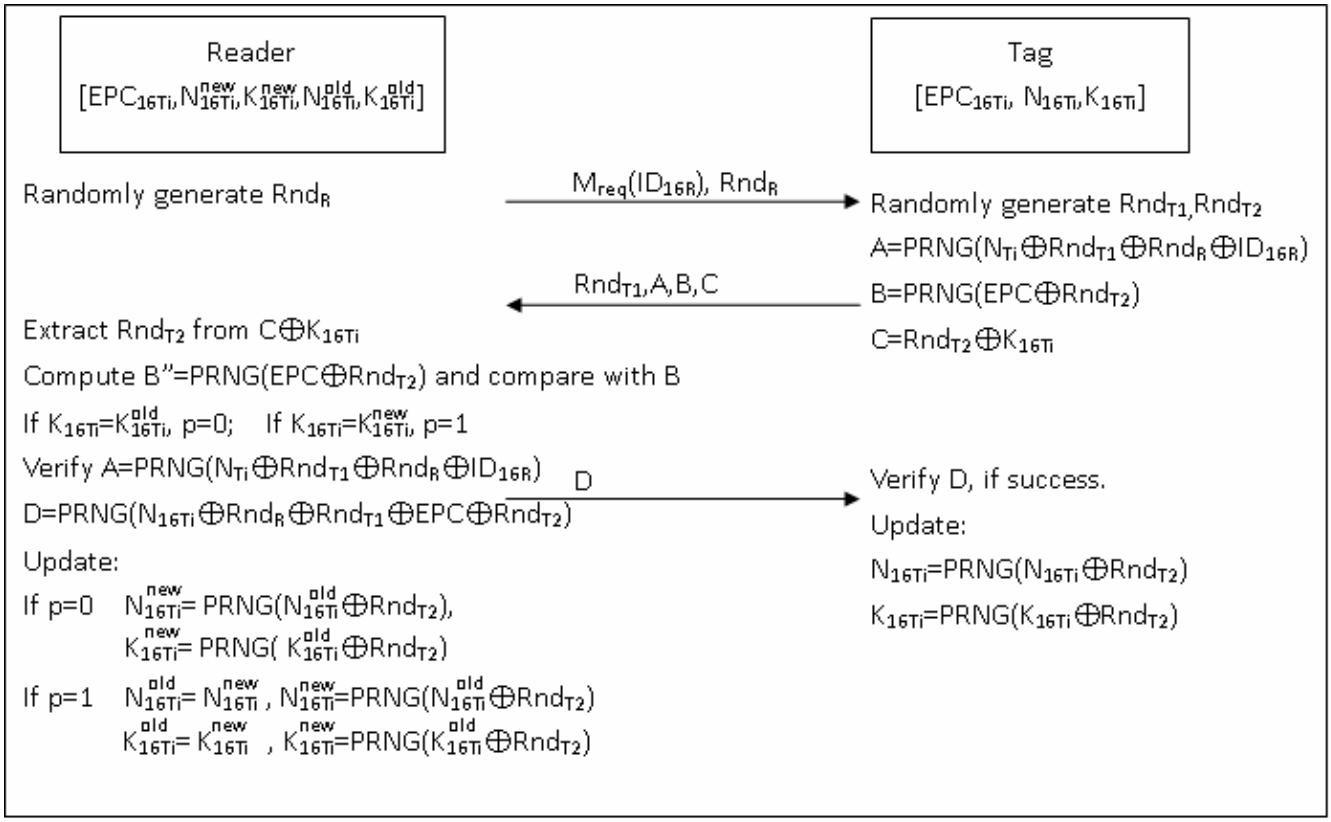

Figure 1. Azumi protocol

Step1: The reader randomly generates random number Rnd_R and sends request message contain reader identifier ID_{16R} and Rnd_R to the tag.

Step2: After receiving the message sends by the reader, the tag randomly generates *RndT1*, RndT2. Then, the tag computes A, B, C and sends (*RndT1*, *A*, *B*, *C*) to the reader.

A=PRNG (*NTi* $\oplus$*RndTi* $\oplus$*RndRi* $\oplus$*ID16Ri*)

B=PRNG (*EPC16Ti* $\oplus$*RndT2*)

C=(*RndT2* $\oplus$*K16Ti*)

Step3: After the reader receives the messages (*RNDT1*, *A*, *B*, *C*), the reader performs a searching process for identify the tag. First the reader uses the new/old values of K16Ti which store in database to extract *RndT2*.

Then the reader identifies the tag by computing

B"=PRNG (*EPC16Ti* ⊕ *RndT2*) with the extracted *RndT2*. If *B"* equals *B* then the tag is identified.

If the reader uses new value of *K16Ti*, the flag *p* is set to 1.

If the reader uses old value of *K16Ti*, the flag *p* is set to 0.

The reader continues to authenticate the tag. The reader uses the corresponding (*N16Ti*) to compute *A"* =PRNG (*NTi*⊕*RndTi*⊕*RndRi*⊕*ID16Ri*) and compare with *A*. If *A"* equals *A* then the tag is authenticated. In this moment, the new/old value of *N16Ti* is used determined by the new/old value of *KTi* which is used to identify the tag. The reader computes authentication message *D* and sends to the tag.

D=PRNG (*NTi* ⊕ *RndRi* ⊕ *RndTi* ⊕ *EPC16Ti* ⊕ *RndT2*)

Step4: Upon the tag receive the message D, the tag authenticates the reader by computing *D"* and comparing with *D*. If *D"=D*, the reader is authenticated and it continue to updating the secret values.

To prevent the desynchronize problem, the updating process depends on the flag *p* which indicates the synchronize state of the tag.

If *p*=0, there is desynchronize problem.

$$N_{16T_i}^{new} = PRNG(N_{16T_i}^{old} \oplus Rnd_{T2})$$

$$K_{16T_i}^{new} = PRNG(K_{16T_i}^{old} \oplus Rnd_{T2})$$

If *p*=1, there is not desynchronize problem.

$$N_{16T_i}^{old} = N_{16T_i}^{new}$$

$$K_{16T_i}^{new} = PRNG(K_{16T_i}^{old} \oplus Rnd_{T2})$$

$$K_{16T_i}^{old} = K_{16T_i}^{new}$$

$$K_{16T_i}^{new} = PRNG(K_{16T_i}^{old} \oplus Rnd_{T2})$$

The mechanism can against desynchronize attack and resynchronize the inconsistent state between reader and tag.

3.3 Authentication Phase

Azumi protocol uses PRNG and bitwise computation to perform mutual authentication and the scheme is conform to C1G2 standard. But there are some weaknesses in the scheme. We will discuss the problems of Azumi protocol in following section.

There are some problems in Azumi protocol:

1. Full searching: In order to identify and authenticate the tag, the reader must perform a full searching in database. In order to prevent the desynchronize state between reader and tag, the database stores new/old (K_{Ti}, N_{Ti}) values of each tags. All of new/old K_{16Ti} values in the database are used to identify the tag. In authentication phase the worse case of compute complexity is *O(2n)*.

2. Revealing of the secret *K*: After a success authentication, the reader and the tag will update the secret (N_{Ti}, K_{Ti}). The secret K is updated by computing $PRNG\ (K_{16Ti} \oplus Rnd_{T2})$, but the value $(Rnd_{T2} \oplus K_{16Ti})$ can be eavesdropped from authentication message *C* ($C = Rnd_{T2} \oplus K_{16Ti}$). After eavesdropping the ith session, the attacker can compute the K value of the tag in $(i+1^{th})$ session.

3. Tag impersonation attack: The attackers eavesdrop and record the message transmitted in previous session. The attacker modifies and resends the message to pass the authentication. The impersonal tag will be accepted as a legitimate tag.

In tag impersonation attack, there are two phase: (1) Eavesdropping Phase. (2) Cheating Phase. The following is the step of tag impersonation attack:

Eavesdropping phase. In ith session, the attacker eavesdrops and records the message in the normal session.

(1) Reader→Tag: M_{req}, Rnd_R

(2) Tag→Reader: Rnd_{T1}, *A*, *B*, *C*

(3) The attacker eavesdrops and records the message $(Rnd_R, Rnd_{T1}, A, B, C)$ in this normal session.

Cheating phase. In $i+1^{th}$ session, the attackers impersonates a legitimate tag and tries to pass the authentication.

(1) Reader→Tag: M_{req}, Rnd_R"

(2) Attacker: Compute $X1=Rnd_R" \oplus Rnd_R$

$Rnd_{T1}"=Rnd_{T1} \oplus X1$

(3) Tag→Reader: $Rnd_{T1}"$, *A"*, *B"*, *C"* (*A"=A*, *B"=B*, *C"=C*)

(4) Reader identifies and authenticates the tag successfully.

In $i+1^{th}$ session, a legitimate reader sends request including $Rnd_R"$. The attacker computes X1 by $Rnd_R \oplus Rnd_R"$. Attacker also computes $Rnd_{T1}"=Rnd_{T1} \oplus X1$ and sends ($Rnd_{T1}"$, *A*, *B*, *C*) to the reader. After receiving the message, the message can be verified by the legitimate reader.

Proof 1:

In tag identification phase, reader uses old/new value of K_{16Ti} in database to extract Rnd_{T2} ($Rnd_{T2}=K_{16Ti} \oplus C$). In our attack, the forgery message (B, C) can be resend to the reader. The reader identifies the tag as a legitimate tag with a desynchronize state.

In $i+1^{th}$ session, reader sends request including random number Rnd_R. The response B" and C" are used to identify the tag, but it does not change with Rnd_R. In $i+1^{th}$ session, the message (B", C") contains the K_{16Ti} in ith session and the tag will be defined as the tag with being failed in updating phase. The reader can successfully verify the message (B", C") and identify the tag.

Proof 2:

In tag authentication phase, reader verifies the tag

by using corresponding (N_{16Ti}, ID_{16R}) and message A". Although the message A" contains random number Rnd_R" and the message changes every session. We compute X1=Rnd_R ⊕Rnd_R". We modify the previous message (Rnd_{T1}"=X1 ⊕ Rnd_{T1}, A, B, C) and the message A" will be accepted because of the mathematic properties of exclusive-OR. The forgery messages (Rnd_{T1}", A", B', C") would be seen as a legal message.

We assume X1=Rnd_R" ⊕Rnd_R, Rnd_{T1}"=Rnd_{T1} ⊕X1, Rnd_R"=Rnd_R ⊕X1.

A"=PRNG (N_{16Ti} ⊕Rnd_{T1}" ⊕Rnd_{Ri+1} ⊕ID_{16R})
=PRNG (N_{16Ti} ⊕Rnd_{T1} ⊕X1 ⊕Rnd_{Ri+1} ⊕ID_{16R})
= PRNG (N_{16Ti} ⊕Rnd_{T1} ⊕X1 ⊕Rnd_{Ri} ⊕X1 ⊕ID_{16R})
=PRNG (N_{16Ti} ⊕Rnd_{T1} ⊕Rnd_{Ri} ⊕ID_{16R})
=A

In tag impersonate attack, the illegal message *(R1", A", B")* which sent by attacker can be identify as a legal tag and finally pass the authentication process. Attacker can forge a legal tag.

4 Proposed Scheme

In order to solve the problems mentioned above, this study proposes a new lightweight authentication protocol. Our scheme uses lightweight computation like PRNG and Exclusive-OR operation which comfort the C1G2 standard. To solve the full searching problem, we sends a pseudonym IDS to the reader. The reader can identify the tag by using IDS. After the reader identifies the tag, the reader continues to authenticate the tag. Once the authentication is success, the share secret values are updated to achieve forward secrecy. Table 2 shows the notation for our scheme:

Table 2. Notations of proposed scheme

Notations	Descriptions
Rnd_R	Random number generated by the reader
R1, R2	Random number generated by the tag
EPC	The unique EPC identity of the tag
IDS	Pseudonym identity of the tag
PRNG ()	One-way pseudo random number generator
⊕	Exclusive- OR
||	Concatenation

Our scheme include four phase: (1) Challenge and Response phase (2) Tag identification phase (3) Tag authentication phase (4) Reader authentication and Updating phase. Figure 2 shows the steps of authentication scheme.

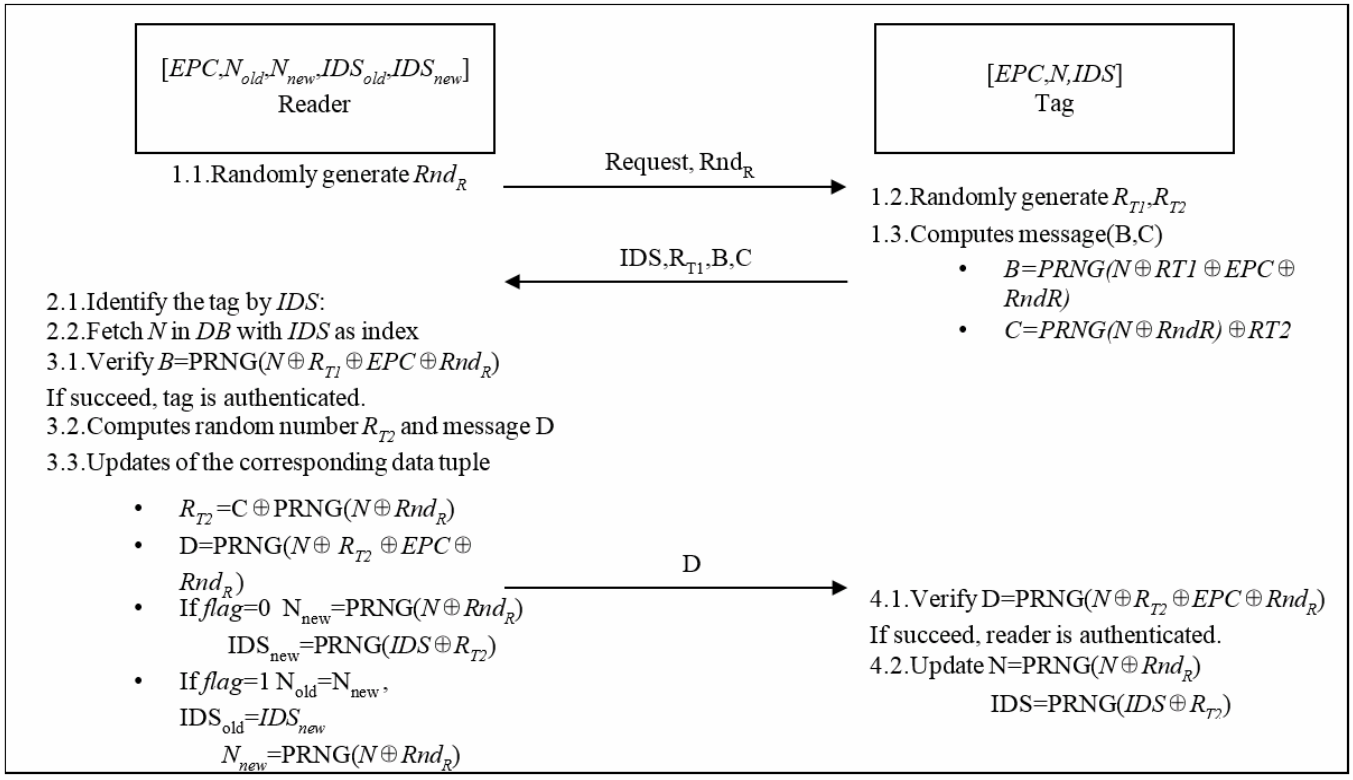

Figure 2. Proposed authentication scheme

(1) Challenge and Response phase: Reader randomly generates random number Rnd_R and sends request including Rnd_R. Upon receiving the request message, the tag generates two random numbers (R_{T1}, R_{T2}) and computes authentication message (*B*, *C*) as follows:

$$B=PRNG\ (N \oplus R_{T2} \oplus EPC \oplus Rnd_R)$$
$$C=PRNG\ (N \oplus Rnd_R) \oplus R_{T2}$$

The tag sends the message *(IDS*, R_{T1}, *B*, *C)* to the reader.

(2) Tag identification phase: After receiving the response message, reader uses the pseudonym *IDS* to identify the tag. The reader searches for the *IDS* in the database to find the corresponding tuple $\{EPC, IDS_{old}, IDS_{new}, N_{old}, N_{new}\}$.

If the old value of *IDS* is found in database ($IDS=IDS_{old}$), the tag may suffers from the desynchronize problem. If *IDS* equals IDS_{old} then $Flag=0$, $N=N_{old}$.

We need use old value to resynchronize the state. If the new value of *IDS* is found in database ($IDS=IDS_{new}$), the tag is in a normal state. *If* $IDS=IDS_{new}$ *then* $Flag=1$, $N=N_{new.}$. We use corresponding new value to continue the next steps.

(3) Tag authentication phase: To prevent the impersonal attack and replay attack, we need to verify the correctness of the message. The reader computes $PRNG\ (N \oplus R_{T1} \oplus EPC \oplus Rnd_R)$ to verify the message *B*. If verification success, the tag is successfully authenticated. Reader updates of the corresponding data tuple as follows:

If $flag=1$ *Update* $N_{old}=N$, $IDS_{old}=IDS$

If $flag=0$ *Update* $N_{old}=N$, $N_{new}=PRNG\ (N \oplus R_{T2})$

$$IDS_{old}=IDS,\ IDS_{new}=PRNG\ (IDS \oplus R_{T2})$$

It continues to reader authentication and updating phase. The reader extracts the random number R_{T2} by computing $C \oplus PRNG\ (N \oplus Rnd_R)$ and computes the authentication message *D* as following process.

$$D= PRNG\ (N \oplus R_{T2} \oplus EPC \oplus Rnd_R)$$

The reader sends the authentication message *D* to the tag.

(4) Reader authentication and Updating phase: After receiving the message *D*, the tag needs to verify the correctness of the message *D*. The tag computes $PRNG\ (N \oplus R_{T2} \oplus EPC \oplus Rnd_R)$ and compares with the message *D*. If the message is correct, the reader is authenticated. The tag updates the secret *N* and pseudonym *IDS* as follows:

$$Update\ N= PRNG\ (N \oplus R_{T2})$$
$$IDS= PRNG\ (IDS \oplus R_{T2})$$

Our scheme depends on challenge and response mechanism. During authentication the scheme uses pseudonym to against traceability. The reader uses pseudonym to identify the tag, and then authenticates the tag by verifying the message with corresponding secret value. After success authentication, the secret values and pseudonym are updated.

5 Analysis

In this section, we analyze our scheme with security and performance. Our scheme can reach a security level and have better performance than previous works.

5.1 Security Analysis

We examine the security of our scheme and show that our scheme is secure against most of attacks. Table 3 shows our scheme can reach higher security level than previous works [8-9].The following is the analysis of our scheme with some common attacks.

Table 3. Comparison of the resistance for common attacks

	Traceability	Replay attack	Man-in- middle attack	Forward secrecy	Desynchronization attack
Chen and Deng [9]	X	X	O	X	X
Azumi protocol [8]	X	X	O	X	O
Our scheme	O	O	O	O	O

(1) Traceability: Malicious user may use reader to query the specific tag and record the transmitted message. If the response message of the Tag is a constant value, the malicious user can trace the value to acquire secret information, it may cause user privacy problem. Therefore, we should make sure that the response is not a constant value and the tag identity cannot be revealed by attackers. In our scheme, the transmitted messages *IDS*, *B*, *C*, and *D* are calculated by the random numbers R_{T1} and R_{T2}. Thus, *IDS*, *B*, *C*, and *D* are not constant values, we proof that the malicious user cannot trace a specific tag.

Proof:

Suppose that an attacker sends Rnd_{Ri}, Rnd_{Ri+1}, Rnd_{Ri+2},..., Rnd_{Rn} *to a specific tag in sequence. Then the tag returns* (IDS_i, R_{T1i}, B_i, C_i), (IDS_{i+1}, R_{T1i+1}, B_{i+1}, C_{i+1}), ..., (IDS_n, R_{T1n}, B_n, C_n) *to attacker.*

$$Attacker\ (Reader) \rightarrow T:\ Rnd_{Ri},\ Rnd_{Ri+1},\ Rnd_{Ri+2},\ldots,\ Rnd_{Rn}$$

$$Tag \rightarrow Attacker\ (Reader):\ \left\{ \begin{array}{c} IDS_i, R_{Tli}, B_i, C_i \\ IDS_{i+1}, R_{Tli+1}, B_{i+1}, C_{i+1} \\ \cdots \\ IDS_n, R_{Tln}, B_n, C_n \end{array} \right\}$$

The attacker can collect several responses, but the response message seems random. Attacker cannot trace a specific tag from the response message.

Furthermore, the *IDS* is computed by $IDS_{new}= PRNG\ (IDS_{old} \oplus R_{T2})$, the attacker is difficult to recover the old *IDS* if the random number R_{T2} is keep secret. The real identity (*EPC*) also keeps secret in the scheme, and it is infeasible to compute EPC from $B=PRNG\ (N \oplus R_{T1} \oplus EPC \oplus Rnd_R)$ and $D=PRNG\ (N \oplus R_{T2} \oplus EPC \oplus$

Rnd_R).

(2) Replay attack: Attacker can eavesdrop the message in previous session and resend it to impersonate a legal entity. In our scheme, the authentication message (*IDS*, *B*, *C*, *D*) consists of random number (Rnd_R, R_{T1}, R_{T2}). The secret *N* and *IDS* update in a random way. Attacker cannot resend the message to perform impersonate attack.

Proof:

In ith session:

Attacker acquires IDS_i, R_{T1i}, B_i, C_i *by eavesdropping in ith session*

$B=PRNG\ (N_i \oplus R_{T1i} \oplus EPC \oplus Rnd_{Ri})$

$C=PRNG\ (N_i \oplus Rnd_{Ri}) \oplus R_{T2}$

In i+1th session

Reader→Attacker (Tag): Rnd_{Ri+1}

Attacker (Tag)→R: IDS_i, R_{T1i}, B_i, C_i

Reader check $B=PRNG\ (N_i \oplus R_{T1} \oplus EPC \oplus Rnd_{Ri+1})$ $C=PRNG\ (N_i \oplus Rnd_{Ri+1}) \oplus R_{T2}$

$Rnd_{Ri+1} \neq Rnd_{Ri}$ *tag authentication will fail.*

In the challenge and response phase of our scheme, reader generates a random number Rnd_R and tag generates two random numbers R_{T1} and R_{T2} for each session. If the random parameters are not correct in each session, the verification will be failed.

(3) Man-in-middle attack: Attacker eavesdrops, modifies and sends modifies message to pass the authentication. In our scheme, the message *(B*, *C*, *D)* is calculated by random number (Rnd_R, R_{T1}, R_{T2}). The attacker cannot compute a correct message which corresponds with the random number and secret values of tag.

Proof:

In ith session

Reader→Man-in-middle (Tag): $Request, Rnd_{Ri}$

Man-in-middle (Reader) →Tag: $Request, Rnd_{Ri}'$

Tag→Man-in-middle (Rweader): IDS_i, R_{T1i}, B_i', C_i'

Where $B_i' = PRNG\ (N_i \oplus R_{T1} \oplus EPC \oplus Rnd_{Ri}')$,

$C_i' = PRNG\ (N_i \oplus Rnd_{Ri}') \oplus R_{T2}$

Man-in-middle cannot compute B_i, C_i *from* B_i', C_i'*because the parameters EPC and* R_{T2} *are unknow. If man-in-middle direct sends* IDS_i, R_{T1i}, B_i', *and* C_i' *to Reader, the reader authentication will fail because* $B_i' \neq PRNG\ (N_i \oplus R_{T1} \oplus EPC \oplus Rnd_{Ri})$.

The same to the authentication between man-in-middle and Tag,

Man-in-middle (Reader) →Tag: D_i'

The Tag authentication will also fail because $D_i' \neq PRNG\ (N_i \oplus R_{T2} \oplus EPC \oplus Rnd_{Ri})$.

(4) Forward Secrecy: If the tag is compromised by an attacker, the secret data which stored in the tag will be revealed by the attacker. Suppose that the secret parameters *EPC* and *N* are revealed by the attacker. We can show that the attacker cannot find the relationship between *IDS* and *EPC* in previous sessions.

Proof:

Suppose that an attacker collect several transmitted messages $(Request, Rnd_{Ri})$, $(Request, Rnd_{Ri+1})$, …, $(Request, Rnd_{Rn})$ *from Reader to Tag and also can collect the transmitted messages* $(IDS_i, R_{T1i}, B_i, C_i)$, $(IDS_{i+1}, R_{T1i+1}, B_{i+1}, C_{i+1})$, …, $(IDS_n, R_{T1n}, B_n, C_n)$ *from Tag to Reader.*

Reader→

$$\text{Attacker (Tag):} \left\{ \begin{array}{c} Request, Rnd_{Ri} \\ Request, Rnd_{Ri+1} \\ Request, Rnd_{Rn} \end{array} \right\}$$

$$\text{Tag→Attacker (Reader):} \left\{ \begin{array}{c} IDS_i, R_{Tli}, B_i, C_i \\ IDS_{i+1}, R_{Tli+1}, B_{i+1}, C_{i+1} \\ \cdots \\ IDS_n, R_{Tln}, B_n, C_n \end{array} \right\}$$

In n+1 session, a Tag is compromised and the attacker obtains the parameters (EPC, N, IDS_{N+1}*). The attacker still cannot compute* IDS_i, IDS_{i+1},…, IDS_N *from the secret parameters (EPC,* N_{n+1}, IDS_{n+1}, R_{Tii}, R_{Tii+1}, …, R_{Tin}, R_{Tin+1}, Rnd_{Ri}, Rnd_{Ri+1}, …, Rnd_{Rn}, Rnd_{Rn+1}*), because IDS and N are updated in a random way after each successful authentication. In our scheme,* $N_{new}=PRNG\ (N \oplus Rnd_R)$*, where PRNG is an one-way function, attacker cannot computes previous N by using the formula.*

(5) Desynchronization attack: After the reader and the tag authenticate each other, it continues to update the secret and pseudonym *IDS*. In this moment, the authenticate message may be blocked or modified by attacker, it may cause a desynchronize state between the reader and the tag. In next session, the tag will not pass the authentication. In our scheme, database stores the old/new secret value of the tag (IDS_{old}, N_{old}, IDS_{new}, N_{new}). If a desynchronization attack is happened, we can resynchronize the unnormal state by using old value. The scheme can against the desynchronization attack.

5.2 Performance Analysis

Low cost RFID system limits the resource such as computation, memory, and communication overhead. We must make sure our scheme can be practiced in present system. In authentication phase of Azumi protocol, after reader receiving the response messages of the tag, the database always performs an exclusive searching to verify the message. To solve the above problem, our scheme uses pseudonym to identify the tag. The mechanism improves the performance. We analysis the performance as follows. Table 4 offers a view of performance comparsion for three schemes.

Table 4. Performance comparison

	Pass Rounds	Tag Computational Overhead	Reader Computational Overhead	Database Loading
Chen and Deng [9]	3	*2CRC+R*	*n CRC+R*	*O(n)*
Azumi protocol [8]	3	5PRNG+ *2R*	*n* PRNG+*R*	*O(n)*
Our scheme	3	5PRNG+ *2R*	PRNG+*R*	*O(1)*

n: number of tag in database. *CRC*: the operation of cyclic redundancy code checksum.
PRNG: the operation of pseudo random number generator. *R*: the operation of generating random number

- Storage overheads: Each tag stores three parameters, *EPC*, *N*, and *IDS*. The parameter *EPC* is stored in the *EPC* memory of the tag. The parameters *N* and *IDS* are stored in the preserved memory, and the user can read or write the data with correct password. The storage overhead is acceptable for tag.
- Computational overheads: In our scheme, we do not employ any public key or symmetric cryptography technique for authentication among reader and tag. On the other hand, we use 16 bit PRNG and two random numbers to generate the authentication messages. In the scheme, the tag totally performs five operations for PRNG and two operations for generating random numbers. These operations are not a big computation overhead used in resource-constrained RFID tags. Comparison with Chen and Deng [9] and Azumi's protocol [8] in Table 4, we can find that the tag computational overhead is similar to the three schemes, but our scheme is better than the other two schemes in terms of the reader computational overhead.
- Communication overheads: Our scheme only performs three rounds message pass in authentication phase. In the first pass rounds, reader transmit (*Request*, Rnd_R) to tag, where Rnd_R is a 16-bits random number. In the second pass round, tag transmits *IDS*, *B*, and *C* to reader, where each parameter is 16 bits, total 48 bits transmitted. In the third pass round, reader only transmits parameter *D* to tag, which is 16 bits.
- Database loading: In previous schemes, database performs an exclusive searching for identify the tag. If the number of Tags is *n*, the worst case is to search *n* times to find the tag. The order of database loading is *O(n)*, Our scheme identifies the tag by using pseudonym IDS, the loading of database can be decreasing. Our system is easier to achieve scalability than previous schemes.

6 Conclusions

The C1G2 standard is an important standard of lightweight RFID tags. Many researches devote to design the secure protocol. The previous schemes still has some weakness because of limited resources. Many researchers devote to design authentication protocols which comfort to C1G2 standard. Predo introduced a new lightweight authentication scheme which compliant to C1G2 standard, called "Azumi protocol". The scheme needs an exclusive search in database during authentication phase and suffers security problems such as revealing of secret, impersonate attack. In this paper, we point out the weakness of Azumi protocol and improve the scheme. Our scheme can reach a secure level and the performance is getting better. According the secruity and performance analysis, our scheme can achieve high security level and efficient performance. Our scheme is compliant to requirements of C1G2 standard. Futhermore, our scheme can be implemented in several applications which need to protect the user privicy, such as supply-chain management, logistics management, and health care management.

References

[1] H. Ning, H. Liu, J. Mao, Y. Zhang, Scalable and Distributed Key Array Authentication Protocol in Radio Frequency Identification-based Sensor System, *IET Communications*, Vol. 5, No. 12, pp. 1755-1768, August, 2011.

[2] EPCglobal, *EPC radio-frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz version 1.1.0*, EPCglobal, December, 2005.

[3] EPCglobal, *EPC Radio-frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz version 1.0.4*, EPCglobal, September, 2004.

[4] H. Y. Chien, SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity, *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 4, pp. 337-340, October-December, 2007.

[5] H. Y. Chien, C. S. Laih, ECC-based Lightweight Authentication Protocol with Untraceability for Low-cost RFID, *Journal of Parallel and Distributed Computing*, Vol. 69, No. 10, pp. 848-853, October, 2009.

[6] Y. Chen, J. S. Chou, H. M. Sun, A Novel Mutual-authentication Scheme Based on Quadratic Residues for RFID Systems, *Computer Networks*, Vol. 52, No. 12, pp. 2373-2380, August, 2008.

[7] T. C. Yeh, C. H. Wu, Y. M. Tseng, Improvement of the RFID Authentication Scheme Based on Quadratic Residues,

Computer Communications, Vol. 34, No. 3, pp. 337-341, March, 2011.

[8] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, J. C. A. V. D. Lubbe, Cryptanalysis of an EPC Class-1 Generation-2 Standard Compliant Authentication Protocol, *Engineering Applications of Artificial Intelligence*, Vol. 24, No. 6, pp. 1061-1069, September, 2011.

[9] C. L. Chen, Y. Y. Deng, Conformation of EPC Class 1 Generation 2 standards RFID System with Mutual Authentication and Privacy Protection, *Engineering Applications of Artificial Intelligence*, Vol. 22, No. 8, pp. 1284-1291, December, 2009.

[10] E. J. Yoon, Improvement of the Securing RFID Systems Conforming to EPC Class 1 Generation 2 Standard, *Expert Systems with Applications*, Vol. 39, No. 1, pp. 1589-1594, January, 2012.

[11] M. Moessner, G. N. Khan, Secure Authentication Scheme for Passive C1G2 RFID Tags, *Computer networks*, Vol. 56, No. 1, pp. 273-286, January, 2012.

[12] H. Y. Chien, C. H. Chen, Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation-2 Standard, *Computer Standards & Interfaces*, Vol. 29, No. 2, pp. 254-259, February, 2007.

[13] L. Wang, X. Yi, L. C. LV, Y. Guo, Security Improvement in Authentication Protocol for Gen-2 Based RFID System, *Journal of Convergence Information Technology*, Vo. 6, No. 1, pp. 157-169, January, 2011.

[14] Q. Cai, Y. Zhan, Y. Wang, A Minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis, *2008 ISECS International Colloquium on Computing, Communication, Control, and Management*, Guangzhou, China, 2008, pp. 449-453.

[15] R. Doss, W. Zhou, S. Yu, L. Gao, A Novel Mutual Authentication Scheme with Minimum Disclosure for RFID Systems, *2011 7th International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP)*, Adelaide, Australia, 2011, pp. 544-549.

[16] N. W. Lo and K. H. Yeh, A Secure Communication Protocol for EPCglobal Class 1 Generation 2 RFID Systems, *2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, Perth, Australia, 2010, pp. 562-566.

[17] M. Safkhani, N. Bagheri, M. Naderi, Cryptanalysis of AZUMI: an EPC Class-1 Generation-2 Standard Compliant RFID Authentication Protocol, *IACR Cryptology ePrint Archive*, Vo1. 1, No. 1, p. 424, 2011.

[18] EPCglobal, *Reader Protocol Standard version 1.1*, EPCglobal, June, 2006.

[19] EPCglobal, *EPC Information Services (EPCIS) 1.0 Specification Conformance Requirements Document*, EPCglobal, February, 2007.

[20] S. Qi, Y. Zheng, M. Li, L. Lu, Y. Liu, Secure and Private RFID-Enabled Third-Party Supply Chain Systems, *IEEE Transactions on Computers*, Vol. 65, No. 11, pp. 3413-3426, November, 2016.

[21] M. T. Sun, K. Sakai, W. S. Ku, T. H. Lai, A. V. Vasilakos, Private and Secure Tag Access for Large-Scale RFID Systems, *IEEE Transactions On Dependable and Secure Computing*, Vol. 13, No. 6, pp. 657-671, November/December, 2016.

[22] C. W. Phan, Raphael, Cryptanalysis of a New Ultralightweight RFID Authentication Protocol, *IEEE Transactions on Dependable and Secure Computing*, Vol. 6, No. 4, pp. 316-320, October-December, 2009.

[23] Y. P. Liao, C. M. Hsiao, A Secure ECC-based RFID Authentication Scheme Integrated with ID-verifier Transfer Protocol, *Ad Hoc Networks*, Vol. 18, No. 1, pp. 133-146, July, 2014.

[24] N. Li, Y. Mu, W. Susilo, F. Guo, V. Varadharajan, Vulnerabilities of an ECC-based RFID Authentication Scheme, *Security and Communication Networks*, Vo. 8, No. 17, pp. 3262-3270, November, 2015.

[25] D. He, N. Kumar, N. Chilamkurti, J. H. Lee, Lightweight ECC Based RFID Authentication Integrated with an ID Verifier Transfer Protocol, *Journal of Medical Systems*, Vol. 38, No. 115, https://doi.org/10.1007/s10916-014-0116-z, August, 2014.

[26] J. S. Chou, An Efficient Mutual Authentication RFID Scheme Based on Elliptic Curve Cryptography, *The Journal of Supercomputing*, Vol. 70, No. 1, pp. 75-94, October, 2014.

Biographies

Chen-Yang Cheng received his Ph.D. in Industrial and Manufacturing Engineering at Penn State University. He is currently an Assistant Professor in Department of Industrial Engineering and Enterprise Information at Tunghai University. Prof. Cheng's research interests include RFID in healthcare, Healthcare Systems, and Biomedical Informatics.

Cheng-Ta Huang is an assistant professor of Department of Information Management at Oriental Institute of Technology. He received his Ph.D. degree in Computer Science and Information Engineering at National Central University, Taiwan in 2013. His current research interests include data hiding, steganography, and medical image processing.

Iuon-Chang Lin received the Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. He is currently a professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan. His current research interests include electronic commerce, information security, Blockchain Security, and cloud computing.

Hung-Huei Hsu received the M.S. degree in Deptartment of Management Information Systems, from National Chung Hsing Universityg, Taichung in 2012. He current research interests include information security and IoT security.