# An Efficient Mutual Authentication Scheme for EPCglobal Class-1 Generation-2 RFID System

N.W. Lo and Kuo-Hui Yeh

Department of Information Management
National Taiwan University of Science and Technology
No. 43, Sect. 4, Keelung Rd., Taipei, 106 Taiwan, R.O.C.
Fax number: 886-2-2737-6777
nwlo@cs.ntust.edu.tw
D9409101@mail.ntust.edu.tw

**Abstract.** The nature of data security vulnerability and location privacy invasion of RFID systems have become a serious problem after hundreds of RFID application systems deployed all over the world. One of the promising solution directions is to provide an efficient authentication scheme with the compliance of international RFID standards such as EPCglobal, ISO18000-1 and ISO18000-6. In this study, we propose a novel authentication scheme for RFID systems with excellent data security properties, robust location privacy preservation and efficient data matching/retrieval mechanism. In addition, our scheme is compatible to EPCglobal Class-1 Generation-2 RFID standards because only simple cryptographic primitives such as pseudo-random number generator and cyclic redundancy check are required to be implemented in RFID tags.

**Keywords:** RFID; EPCglobal; Location Privacy; Data Security; Authentication; CRC.

## 1 Introduction

With extended information storage space, enhanced information retrieval capability removing the line of sight restriction, and new identification scheme which assigns every associated object with a unique code number, Radio Frequency Identification (RFID) systems have been pervasively deployed in our daily lives to replace optical bar code systems and make lots of innovating applications. Recent applications in manufacture industry, supply chain management, livestock tracking, and children/seniors location monitoring have demonstrated the potential benefits, impact, and success of RFID technology to human life in the near future.

A RFID system generally consists of radio frequency (RF) tags (i.e., transponders), RF readers (i.e., transceivers), and backend application server. Readers can broadcast an RF signal to inquiry tags of their contents without contacting them physically. Tags respond their resident data, typically including a unique serial number, to readers. RFID tags can be classified as two categories: active tag and passive tag. Active tags contain an on-board power source and can actively transmit data to the reader;

however, passive tags must be triggered by an RF signal through the forward channel from the reader and reply their contents via the backscatter channel. Because of active tags can push their reply signals further with their own power, active tags can be read by a reader from a longer distance than passive tags do.

In terms of logistics and retailer industry, the low-cost passive tags are far more charming than expensive active tags. The "Electronic Product Code"(EPC) standardized by the EPCglobal [3], a joint venture between EAN International (Europe) and UCC (USA), has become the dominant RFID technology standards on logistics. An EPC contains the manufacturer information, type of product, and a unique serial number to identify each individual item. Undoubtedly, the deployment of EPCs on all kinds of goods will invoke the greatest influence ever on the global world market. One of the most important standards proposed by the EPCglobal is the EPCglobal Class-1 Generation-2 RFID specification which defines the functionality and operation of a passive RFID tag. We abbreviate this type of RFID tag as GEN-2 RFID tag later in this paper. According to the EPC Class-1 GEN-2 standard [13], the major RFID features and restrictions are delineated as follows:

1. The operating energy of EPC passive tag is acquired from the RF signal generated by RFID interrogators (readers).
2. The wireless communication range of EPC passive tag is about 2 to 10 meters and EPC RFID systems operate within the frequency range of UHF band (800-960 MHz).
3. Because of the restriction on production cost, tag cannot provide sufficient computing resources to perform complex functions such as data/key encryption and hash function calculation.
4. A EPC Class-1 GEN-2 tag supports the following functions:
   (a) 16-bit pseudo-random number generation (PRNG): a tag shall be able to generate 16-bits random or pseudo-random number $Q$ using PRNG, have the ability to extract a subset of $Q$, and temporarily store at least two 16-bits random numbers.
   (b) 16-bit cyclic redundancy code checksum: a tag shall implement the CRC function to protect and calibrate the commands/messages transmitted between tags and readers.
5. A 32-bits access PIN is used to trigger a tag into the secure mode, and then the tag is able to be read or written.
6. For the reason of privacy protection, a tag is permanently unusable when it receives a kill command with corresponding access PIN.
7. Tag memory shall be logically separated into four distinct sections:
   (a) Reserved memory: 32-bit kill and access passwords are stored in this section.
   (b) EPC memory: this part of memory contains 16-bit CRC, 16-bit protocol control (PC) and EPC with various sizes (64/96/256 bits).
   (c) TID memory: this section stores ISO/IEC 15693 allocation class identifier (8-bits) and provides space for information of custom commands and optional features that a tag supports.
   (d) User memory: this area is reserved for user-specific data.

In order to meet the low-cost manufacture requirement, GEN-2 RFID tag can only equip with very primitive computation power and functions. Since GEN-2 RFID tag specification did not consider much regarding to user privacy and data security mat-

ters, many security attacks become the potential threats for the success of EPC-enabled RFID systems. For example, EPC-tagged objects in the supply chain make it easier for corporate espionage to remotely eavesdrop and gather unprotected information. A man can easily be traced where he went as long as an identified EPC tag (on an object item) is carried with him. Similarly, the monetary values of items a person worn or carried with him can be determined by an adversary effortlessly. Adversaries can also utilize the association rule on a set of EPC-tagged items to gain transaction information about items, and to track people without knowing their identities. Even more sophisticated security threats such as breadcrumb threat and RFID cloning [5] can potentially occur under current deployment. Hence, in order to survive from these potential security threats, a robust and secure RFID system should provide three important security and privacy functionalities: data content security during transmission, mutual authentication, and anonymity between communicating parties.

The vast literature devoted to RFID security field has been reviewed on several occasions [1, 2, 4-12]. However, some of them cannot be compatible with the EPC GEN-2 standards, and the others have weakness in terms of privacy protection or content security. Only few schemes [1, 2, and 6] can be implemented on EPC GEN-2 tags. Nevertheless, these schemes still suffer from threats such as replay attack, Denial-of-Service (DoS) attack, and identity tracking problem. In this paper, we first point out the security weaknesses of Chien and Chen's scheme [1] and derive a new mutual authentication scheme, which requires two authentication keys and two transaction data stored onto RFID tag memory associated with dedicated two-way message-passing authentication process. Based on security analysis, our scheme can resist security threats such as replay attack and DoS attack, and provide privacy protection such as anonymity and forward secrecy. Furthermore, the proposed scheme complies with the EPC GEN-2 standards and improves the efficiency of data retrieval at backend database.

The rest of this paper is organized as follows. Section 2 gives an introduction of EPC GEN-2 specifications and related RFID authentication research works. Next, we review Chien and Chen's scheme [1] and discuss their security weakness in Section 3. Section 4 presents a new authentication scheme to conquer these security pitfalls. The security analysis of our scheme is addressed in Section 5. Finally, we summarize our conclusion in Section 6.

## 2 Related Work

From information security point of view, the EPC GEN-2 standards do not thoroughly consider privacy invasion problems and data security issues. Only simple kill and access commands are specified in GEN-2 specifications to provide authentication function and data/privacy protection. In order to protect privacy-related information between communicating parties and to prevent counterfeit data attacks against RFID systems, many authentication schemes were introduced recently. Weis et al. [4] proposed two authentication mechanisms, hash-based access control and randomized access control, to achieve security and privacy aspects for RFID systems. In their schemes, a key in a RFID tag is either pre-defined or created by a pseudo-random

number generator. In hash-based access control scheme, with the pre-defined shared key as the argument, a tag's hash function generates its fixed tag identifier *metaID*. When a reader queries the tag, it replies with its *metaID*. In randomized access control scheme, the random-generated key *R* and hashed value of the pre-defined ID concatenated with key *R* are transmitted back to reader in response to reader's query. Since both schemes allow the reader to unlock the hash-locked tag by sending unencrypted pre-defined key or ID, an attacker can eavesdrop the communication channel and easily get all necessary information to either break these authentication schemes or trace specific tags. Based on the proposed brute-force ID search mechanism, the backend server can be overloaded easily by spending a lot of computation resources on ID matching for every query. More importantly, both authentication mechanisms cannot resist the replay attack and did not comply with EPC GEN-2 standards.

Ohkubo et al. [9] developed a mutual authentication scheme for RFID systems based on hashing chain mechanism. Their scheme aims to provide two security properties: indistinguishability and forward security. The indistinguishability of RFID tag indicates a tag's output must be indistinguishable from truly random values, while forward security denotes as even if the adversary acquires the secret data in a tag such as ID or access PIN, the attacker cannot trace the previous locations of the tag through revealed (eavesdropped) information in the past. However, this authentication mechanism cannot resist the replay attack either.

In [2] Henrici & Műller developed a novel scheme to prevent tag tracing problem by updating the identification of tag after each successful authentication. During the authentication process, the tag always responds a reader's query with the same hashed value before it updates its secret identification at the end of the query communications. This design allows an attacker to eavesdrop and trace a specific tag easily. In addition, the difference between the current transaction number and the last successful transaction number ($\Delta TID$), which is used for a receiver(reader) to calculate the current transaction number (*TID*) stored in the tag, is broadcasted by the tag in a plain text format. Adversaries can utilize this $\Delta TID$ to invoke a replay attack.

Molnar and Wagner in [8] investigated the authentication process for book management systems in a library. Nonetheless, the PRF-based private authentication scheme proposed by Molnar et al. does not provide forward security to the tags stamped on books. Similarly, in [10] Rhee et al. used pseudo-random number generator and hash function to develop a challenge-response based RFID authentication protocol which does not offer forward security either.

An and Oh [12] proposed a new scheme, which is based on hash function and random-number generator function, to complete the authentication between the tag and the backend server. However, location tracking problem and replay attack are not resolved in their scheme. Yang et al. [11] pointed out the Henrici & Műller's scheme cannot solve location tracking problem and proposed a new scheme to solve this problem. Their scheme assumes the tag has the ability of performing PRNG function and hash function to generate different responses according to the random number sent from the reader. Unfortunately, Avoine et al. in [14] had pointed out the scheme proposed by Yang et al. cannot provide privacy to the tag carrier.

More recently, several new mechanisms [1, 6, 7], all compatible with the EPC GEN-2 specifications, have been proposed to achieve secure authentication process for RFID systems. Karthikeyan et al. [7] proposed a RFID authentication protocol

based on XOR (exclusive OR) and matrix computation. Nevertheless, their scheme cannot resist DoS attack, replay attack, and privacy-revealing problem. In [6] Duc et al. developed a simple authentication scheme by replying a server query with a random number $R$, $M_1=CRC(EPC||R)\oplus Key_i$, and $CRC(M_1\oplus R)$. However, if attackers can intercept the "End Session" at the final communication step, the backend server will not update the old key in its database. Therefore, the opportunity for attackers to perform the DoS attack and counterfeit tag attack is open. Furthermore, this scheme is not able to provide forward secrecy either. Finally, Chien and Chen [1] improved the scheme invented by Karthikeyan et al. [7] and Duc et al. [6] to provide stronger privacy and security properties. However, their scheme still has space for improvement in terms of performance efficiency and data security. From the performance efficiency aspect, their scheme will generate heavy computation load on backend server because of the brute-force search mechanism applied for data match. In terms of data security, this scheme cannot resist the replay attack before both the tag and backend server complete their authentication process and key synchronization.

## 3 Security Analysis of Chien and Chen's Scheme

In this section, we briefly review Chien and Chen's authentication scheme, which was published in February 2007, in RFID systems and discuss the security weaknesses of their scheme.

Chien and Chen developed a mutual authentication, which is compatible with EPCglobal class 1 generation 2 standards. In their scheme, only lightweight operations, such as pseudo-random number generator (PRNG), XOR function, and CRC checksum function, are utilized for security enhancement and privacy preservation. Each tag, denotes as $Tag_x$, shares a unique identification $EPC_x$ and the secret key values $K_{x\_i}$ and $P_{x\_i}$ with backend server, denotes as *Server*, during each authentication session $i$. In addition, *Server* maintains two record of each shared secret key value ($K_{new}$, $K_{old}$, $P_{new}$, $P_{old}$) for each entry. This design is used to prevent their scheme against *DoS* attack. We illustrate the normal operation procedure of Chien and Chen's scheme as in Fig. 1.

**1. $Reader_y \rightarrow Tag_x$: $N_1$**

When $Reader_y$ sends a random number $N_1$ as a request to inquire $Tag_x$, $Tag_x$ first generates a random number $N_2$ and computes the response value $M_1=CRC(EPC_x||N_1||N_2)\oplus K_{x\_i}$

**2. $Tag_x \rightarrow Reader_y \rightarrow Server$: ($M_1$, $N_1$, $N_2$)**

$Tag_x$ transmits ($M_1$, $N_2$) to $Reader_y$, which forwards ($M_1$, $N_1$, $N_2$) as an authentication request to *Server*. Once receiving the incoming authentication request, *Server* iteratively retrieves key values ($K_{new}$, $K_{old}$, $P_{new}$, $P_{old}$) from each entry in backend database. Then, *Server* computes the $I_{new}=M_1\oplus K_{new}$ and $I_{old}=M_1\oplus K_{old}$, and find the matching entry in backend database depending on which of the following conditional relationships holds: $I_{new} = = CRC(EPC_x||N_1||N_2) \oplus K_{x\_i}$ or $I_{old} = = CRC(EPC_x||N_1||N_2) \oplus K_{x\_i}$.

If *Server* finds the matching entry, it computes $M_2=CRC(EPC_x||N_2)\oplus P_{new}$ or $M_2=CRC(EPC_x||N_2)\oplus P_{old}$ depending on which value ($K_{new}$ or $K_{old}$) satisfies the previous verification process. Finally, *Server* updates the shared symmetric key value$P_{old}=P_{new}$, $K_{old}=K_{new}$, $K_{new}=PRNG(K_{new})$ and $P_{new}=PRNG(P_{new})$ through the PRNG function and sends ($M_2$, *ObjectData*) to $Reader_y$.

**3. *Server* → $Reader_y$ → $Tag_x$:** ($M_2$, *ObjectData*)

$Reader_y$ retrieves *ObjectData* and forwards $M_2$ to $Tag_x$. Upon receiving $M_2$, for the correctness of the incoming message, $Tag_x$ verifies whether the $M_2\oplus P_{x\_i}$ and computed value $CRC(EPC_x||N_2)$ are identical or not. If both values are the same, $Tag_x$ updates its shared symmetric key $K_{x\_i+1}=PRNG(K_{x\_i})$ and $P_{x\_i+1}=PRNG(P_{x\_i})$.

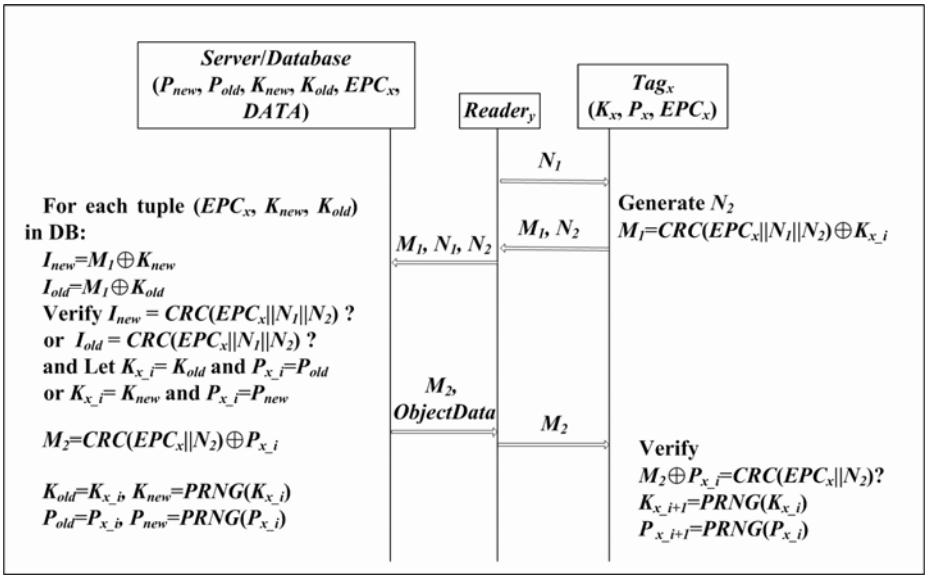


**Figure 1. Chien and Chen's authentication scheme.**

After studying Chien and Chen's authentication scheme, we have identified several weaknesses of their scheme. For the performance efficiency viewpoint, their scheme will generate heavy computation load on finding the matching data entry at backend server side due to *Server* have to XOR incoming message $M_1$ and the shared symmetric key ($K_{new}$, $K_{old}$) of each entry in backend database. For security aspect, before *Server* updates the shared symmetric key, attacker can easily perform replay attack to *Server* with iteratively issuing the eavesdropped legitimate authentication request ($M_1$, $N_1$, $N_2$). In addition, the anonymity property also cannot be guaranteed in their scheme. We illustrate the attack scenario in Fig. 2. Before $Tag_x$ updates the shared secret key, if the attacker sequentially sends two queries to $Tag_x$ in a reasonable time, $Tag_x$ will response two values $M_1$ and $M_2$ back to attacker. After XORing $M_1$ and $M_2$, the shared secret key $K_{x\_i}$ will be eliminated. According to the known $N_1$, $N_2$, $N_3$ and $N_4$, the attacker can easily trace the $Tag_x$ without being noticed. For example, for the simplicity, we assume $EPC_x$, $N_1$, $N_2$, $N_3$ and $N_4$ are all 4-bits length. Attacker sequentially sends $N_1$=0101 and $N_3$=0110 as a request to $Tag_x$, and then $Tag_x$ responds $M_1$, $M_2$,

$N_2$=1011 and $N_4$=1001 to attacker. After computing the $M_1 \oplus M_2$ value, if the left 12-bits of computation result are (0000, 0011, 0010), attacker can identify $Tag_x$ even if the $EPC_x$ is unknown. Ex: $M_1 \oplus M_2 = CRC(EPC_x||N_1||N_2) \oplus CRC(EPC_x||N_3||N_4) = (EPC_x \oplus EPC_x, N_1 \oplus N_3, N_2 \oplus N_4, CRC_{M1} \oplus CRC_{M2}) = (0000, 0101 \oplus 0110, 1011 \oplus 1001, CRC_{M1} \oplus CRC_{M2}) = (0000, 0011, 0010, CRC_{M1} \oplus CRC_{M2})$.

Finally, their scheme cannot provide forward security either. We illustrate this weakness in Fig. 3. For each session, attacker first issues a query to $Tag_x$ to get $M_1$ and sends $M_1$ to *Server* for obtaining $M_2$. Then, attacker stores these two values $M_1$ and $M_2$ without transmitting $M_2$ to $Tag_x$. Next, attacker eavesdrops the transmitted message $M_3$ and $M_4$ between $Tag_x$ and other legitimate $Reader_y$. With these four transmitted $M_1$, $M_2$, $M_3$ and $M_4$ of each session, once $Tag_x$ is compromised (the attacker would get the current secret information such as the $EPC_x$), the transmitted message $M_3$ and $M_4$ can be derived with known $EPC_x$, $N_1$, $N_2$, $N_3$ and $N_4$. Hence, the forward security also cannot be guaranteed.

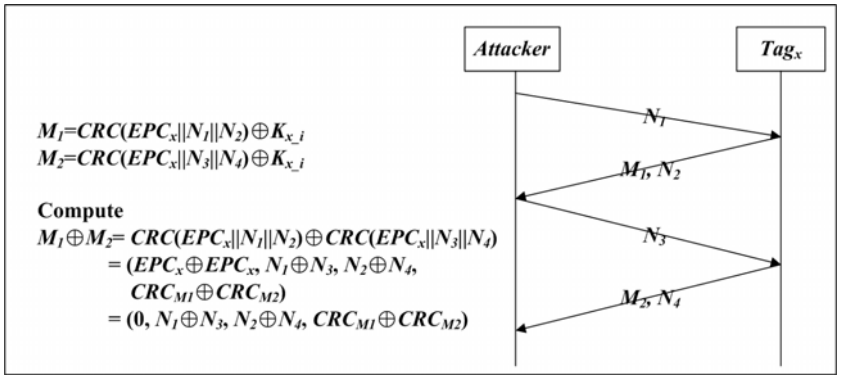


**Figure 2. Security weakness (anonymity) in Chien and Chen's scheme.**

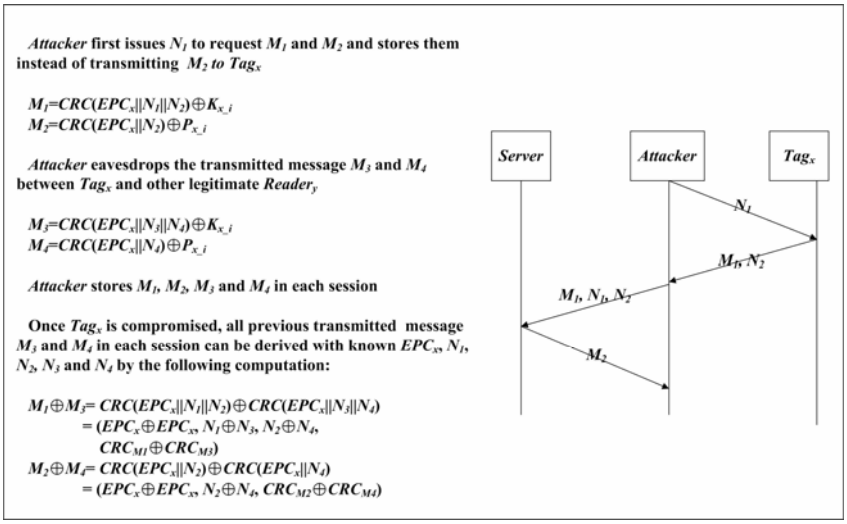


**Figure 3. Security weakness (forward security) in Chien and Chen's scheme.**

## 4 New Authentication Scheme

In this section we introduce a new derived mutual authentication scheme to achieve RFID system requirements for data security, privacy protection, and the efficiency of server utilization. Our scheme is designed to accommodate the EPC GEN-2 standard. The vulnerability of RFID tag is assumed. Once a tag was compromised, its contents can be retrieved and modified by the attacker. As previous proposed schemes, we assume that the attacker can monitor the communication channels and broadcast counterfeit messages between the RFID readers and tags, while the communication channels between the readers and the backend server are secure.

### 4.1 System Initialization

For each tag denoted as $Tag_x$, an initial setup is performed to store five various values in the tag's memory. The authentication key $K_{x\_0}$ and the database access key $K_{DB}$ are generated from a PRNG function initially at the server side before inserting into $Tag_x$. These two keys ($K_{x\_0}$ and $K_{DB}$) are used to secure data. Note that the database access key $K_{DB}$ will be shared by all tags within this database. A pre-defined value for the Electronic Product Code ($EPC_x$) and two default values for the transaction number (*TID*) and the last successful transaction number (*LST*) are assigned to both the server database and a corresponding tag during system initialization. For the sake of simplicity, the initial values of *TID* and *LST* are usually set to the same. In our scheme we have modified the Henrici & Műller's mechanism to prevent the replay attack. In addition, from the view point of forward security, the authentication key will be updated at both the querying server end and the responding tag end after each successful authentication. The authentication key after the *i*-th successful session update is denoted as $K_{x\_i}$. For each EPC value, the backend server also maintains a record of twelve fields in the database including $EPC_{x\_new}$ and $EPC_{x\_old}$, the old and new authentication keys associated with this $EPC_x$ ($K_{old}$ and $K_{new}$), the shared database access key ($K_{DB}$), the old and new transaction numbers ($TID_{old}$ and $TID_{new}$), the old and new values of last successful transaction numbers ($LST_{old}$ and $LST_{new}$), the optional information (*DATA*), and the fast search key ($PRNG^m(EPC_{x\_new})$ and $PRNG^m(EPC_{x\_old})$). The fast search key is designed to find the corresponding data tuple in database efficiently during the reader query process, where *m* is a pre-defined positive integer and the dual-record design (*old* and *new*) is adopted to defense DoS attack. The initial values of the old and new authentication keys associated with $EPC_x$ are both set to $K_{x\_0}$. After system initialization, when the readers query RFID tags, the normal authentication process between reader and tag is activated as shown in Fig. 4.We describe the detail operation procedures in the next section.

### 4.2 Normal Authentication Operation

**1. $Reader_y$ → $Tag_x$: *Query***

$Reader_y$ sends a *Query* signal as a challenge to the $Tag_x$.

**2. $Tag_x$ → $Reader_y$ →Server: $M_1$, $M_2$**

$Tag_x$ first generates two random numbers $n$ and $N_1$ where $n \leqq m$, computes $TID=TID+1$, $\Delta TID=TID\text{-}LST$, $M_1=(CRC(EPC_x||N_1||TID||\Delta TID))\oplus PRNG(K_{x\_i}\oplus N_1)$ and $M_2=CRC((PRNG^n(EPC_x)||n||N_1)\oplus K_{DB})$ sequentially, and sends the values ($M_1$, $M_2$) to the server. Note that when operating the XOR operation in our scheme, the size of each variant will be set to the same length by iteratively append the variant itself. For example, if the length of the ($CRC(EPC_x||N_1||TID||\Delta TID)$) and $PRNG(K_{x\_i}\oplus N_1)$ are 144-bits and 16-bits individually, we first concatenate eight 16-bits $PRNG(K_{x\_i}\oplus N_1)$ into one temporary 144-bits variant $T$ and then XOR $T$ with the ($CRC(EPC_x||N_1||TID||\Delta TID)$) as the output $M_1$.

When the backend server receives the authentication request from $Reader_y$, it first use database access key $K_{DB}$ to retrieve $PRNG^n(EPC_x)$, $n$ and $N_1$. Server then computes the $PRNG^m(EPCx) = PRNG^{m-n}(PRNG^n(EPC_x))$, and finds the corresponding record entry from the database. After retrieving the values of related fields in the corresponding tuple, the server computes the values $H_1=M_1\oplus PRNG(K_{new}\oplus N_1)$ and $H_2=M_1\oplus PRNG(K_{old}\oplus N_1)$. Next, the binary string length function $LEN()$ and the binary string truncation function $TRUNC()$ are applied to calculate the following values:

$$I_{new}=TRUNC(H_1, LEN(CRC(EPC_x||N_1))),\ I_{old}=TRUNC(H_2, LEN(CRC(EPC_x||N_1))),$$
$$TID_1=TRUNC(H_1, LEN(CRC(EPC_x||N_1)), LEN(TID_{new})),$$
$$\Delta TID_1= TRUNC(H_1, LEN(CRC(EPC_x||N_1))+LEN(TID_{new}), LEN(TID_{new}))$$
$$TID_2=TRUNC(H_2, LEN(CRC(EPC_x||N_1)), LEN(TID_{old})),$$
$$\Delta TID_2= TRUNC(H_2, LEN(CRC(EPC_x||N_1))+LEN(TID_{old}), LEN(TID_{old}))$$

Note that the function $LEN(x)$ returns the length of binary string $x$, and the truncation function with two varieties $TRUNC(x, y)$ and $TRUNC(x, y, z)$ returns a partial binary string that contains either only the first $y$ bits of the original string $x$ or the substring with $z$ bits of length started from the $y$-th bit position of the original string $x$, respectively.

Once the server has the intermediate values $I_{new}$, $I_{old}$, $TID$ and $\Delta TID$, the verification process is invoked to determine the authentication key hidden in the incoming tag response is the up-to-date one or the previous one. If $I_{new}=CRC(EPC_x||N_1)$, then the authentication key from tag reply is up-to-date; the server computes $K_{x\_i}=K_{new}$, $EPC_{x\_i}=EPC_{new}$ and $TID^*=LST_{new}+\Delta TID_1$. Otherwise, the equation $I_{old}=CRC(EPC_x||N_1)$ should be true, the equations $K_{x\_i}=K_{old}$, $EPC_{x\_i}=EPC_{old}$ and $TID^*=LST_{old}+\Delta TID_2$ are calculated by the server. Before generating the reply message to the reader, the server still needs to check abnormal conditions in order to prevent malicious attacks. Therefore, two logical relations, $TID^* \neq TID_1$ (or $TID^* \neq TID_2$) and $TID^* \leqq TID_{old}$, are examined. If one of them was true, the server will discard the tag reply and deny further communication. The first logical relation, $TID^* \neq TID_1$ (or $TID^* \neq TID_2$), is adopted to detect counterfeit tag attack, while the second logical relation is to determine whether a replay attack is encountered.

Once the server successfully authenticates the tag in the previous step, it generates a random numbers $N_2$ and computes $M_3=CRC(EPC_x||N_2)\oplus PRNG(K_{x\_i}\oplus N_2)$. At the same time the server will update the related fields of the corresponding $EPC_x$ entry in its database including the authentication keys, transaction numbers and the last suc-

cessful transaction numbers. The update equations are listed in the sequence of execution order:

$$K_{old}=K_{x\_i},\ K_{new}=PRNG(K_{x\_i}),\ EPC_{x\_new}=PRNG\ (EPC_{x\_i}\oplus N_2),\ EPC_{x\_old}=EPC_{x\_i},$$
$$TID_{new}=LST_{new}=TID^{*},\ TID_{old}=TID^{*},\ LST_{old}=TID^{*}-\Delta TID,$$
$$PRNG^{m}(EPC_{x\_old})=PRNG^{m}(EPC_x) \text{ and } PRNG^{m}(EPC_{x\_new})$$

Afterwards, the server sends ($M_3$, $N_2$) with optional object data as a reply message to $Reader_y$.

**3. *Server → Reader$_y$: $M_3$, $N_2$, Object Data***

$Reader_y$ retrieves the product information (object data), if any, and forwards $M_3$ and $N_2$ to $Tag_x$.

**4. *Reader$_y$ → Tag$_x$: $M_3$, $N_2$***

Upon receiving $M_3$ and $N_2$, the tag verifies whether the equation $M_3\oplus PRNG(K_{x\_i}\oplus N_2)=CRC(EPC_x||N_2)$ holds or not. If the verification is passed, the tag will update its EPC code, authentication key and the last successful transaction number by applying the following equations: $K_{x\_i+1}=PRNG(K_{x\_i})$, $LST=TID$, $EPC_x=PRNG(EPC_x\oplus N_2)$.

## 5 Security Analysis

In this section, we analyze the proposed mutual authentication scheme and compare it with previous researches based on the following security and efficiency criterions.

Data security in RFID systems tends to focus on the data secrecy of messages transmitting between tags and readers. In our scheme data security is achieved by only transmitting bit-scrambled (XOR-ed) or transformed (PRNG-generated) data message such as $M_1$, $M_2$, and $M_3$. While $N_2$ is transmitted in plain text format, however, it is a random-generated one-time-valid number and must be associated with corresponding $M_3$ to perform meaningful computation. Even though these plain numbers can be modified or eavesdropped, the security robustness of meaningful data in t ransmitted messages will not be compromised. In addition, anonymity to both tags and readers can be provided in our scheme because only enciphered messages and one-time-valid random numbers are broadcasted during the reader-tag mutual communication periods of time. In other words, malicious attackers cannot easily trace a specific tag since there are no consistent clues revealed in each tag response. In the worst case, if a tag was compromised and all data stored in it was known by the adversary, the attacker still cannot trace back the trajectory of the compromised tag according to our authentication mechanism. Since the authentication key, EPC code and transaction numbers in a tag will be automatically updated after each successful authentication process, the forward security feature is naturally embedded in the proposed scheme.

Regarding to the tag privacy-revealing threat, the data matching mechanism of our scheme has a weakness; once a tag is compromised by an attacker, he can trace any targeted tag by utilizing the shared database access key $K_{DB}$ until the targeted tag updates its EPC value. Consider the case that the attacker already knew the key $K_{DB}$.

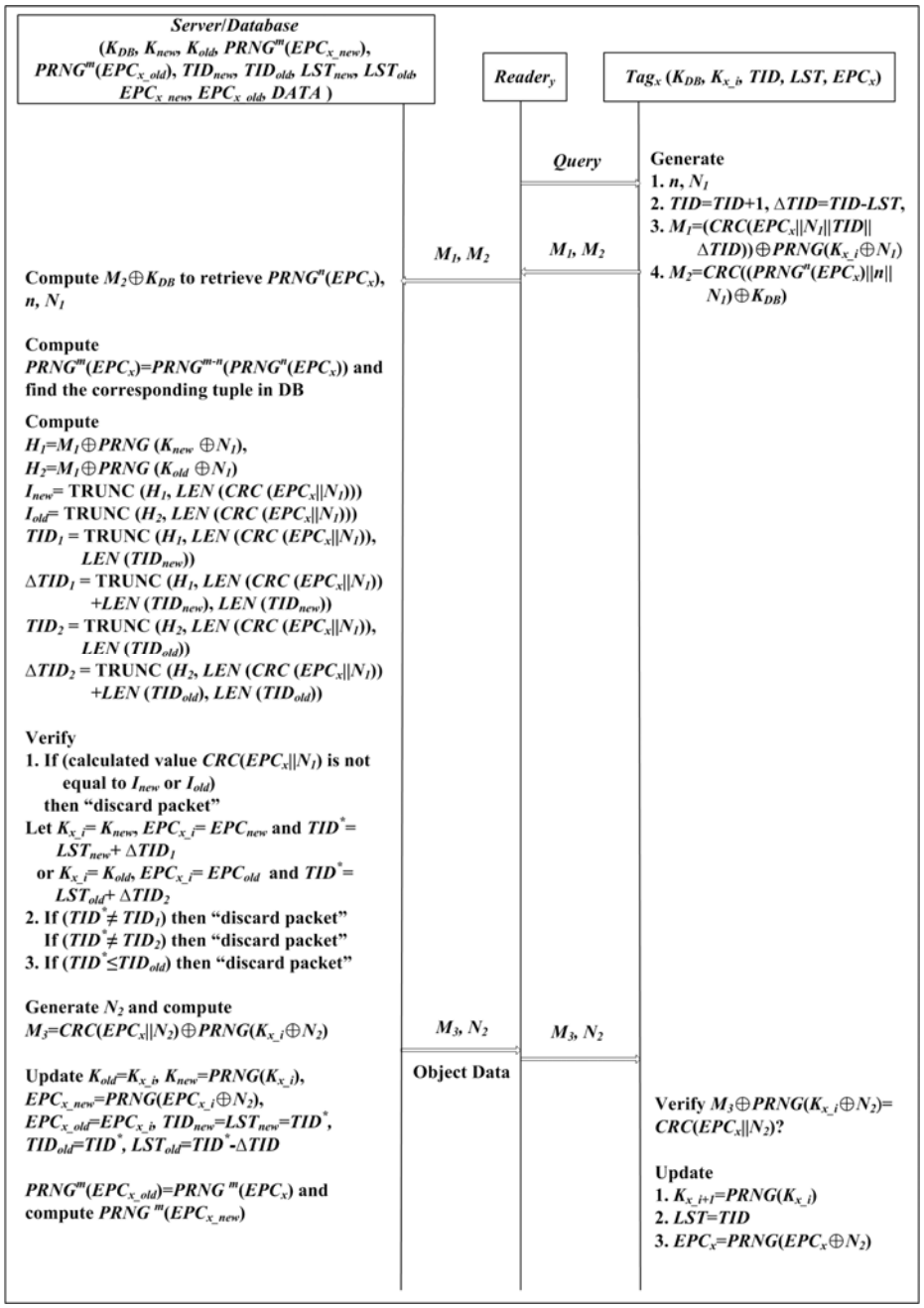


**Figure 4. Proposed mutual authentication scheme.**

He can simply use a reader to query his target tags twice before those tags have chances to update their EPC values. Hence, for each tag the attacker gets two replied

$M_2$ values i.e., $M_2 = CRC((PRNG^{n1}(EPC_x)||n_1||N_a) \oplus K_{DB})$ and $M_{2'} = CRC((PRNG^{n2}(EPC_x)||n_2||N_b) \oplus K_{DB})$, respectively. With the key $K_{DB}$ the attacker can easily derive values of $n_1$, $n_2$, $PRNG^{n1}(EPC_x)$ and $PRNG^{n2}(EPC_x)$. By evaluating the equality relationship between $PRNG^{u}(EPC_x)$ and $PRNG^{u-v}$ $(PRNG^{v}(EPC_x))$ where $u = Max(n_1, n_2)$ and $v = Min(n_1, n_2)$, the attacker can identify and trace a specific tag if it is included in the group of targeted tags. Even though there is a security weakness to our data matching scheme, we argue that once tags update their EPC values ($EPC_x$), the tags become anonymous again and it is not easy for an attacker to keep tracking the specific EPC-updated tag in a group of observed tags. In addition, the proposed matching mechanism can alleviate the computation burden in previous authentication schemes [1, 4, 6, 8-12].

In RFID systems, two of the easiest applicable attacks by malicious adversaries are replay attack and DoS attack. It is very hard, if not impossible, to prevent these kinds of security attacks in advance based on currently available security solutions. Therefore, after these attacks occurred, the resistance ability of a system becomes a very important measurement to its corresponding authentication scheme. In our scheme replay attack is defeated by acquiring the idea from Henrici and Műller in which the validity of a RFID tag message is associated with the transmitting transaction number (*TID*) and the difference ($\Delta TID$) between the current *TID* and the last-stored *TID* in this tag. However, in our scheme we encipher the $\Delta TID$ as part of the tag message $M_1$ instead of sending $\Delta TID$ in a plain text format as Henrici et al. described in [2]. Consequently, it is more difficult for an adversary to figure out the value of $\Delta TID$ and perform replay attack accordingly. Regarding to DoS attack, our scheme maintains the current and the last updated pairs of authentication key, transaction number, and last successful transaction number, in terms of a EPC table entry. This design allows a tag with non-synchronized keys and transaction numbers due to DoS attack, can still be authenticated by the backend server and re-synchronize its data with the server database.

In terms of the efficiency of authentication process, how to reduce computation workload of the backend server during identity match process between a tag-replied identification and database entries is one of the important measurements to evaluate the practical implementation possibility of a RFID authentication mechanism. We adopt the concept of *Efficient Identity Scheme* in [15] and propose a special data retrieval mechanism. We utilize the *m* iterative computation result of PRNG function with EPC value as the starting seed (argument), to be the primary key of EPC entry table in the backend database. This design enables our scheme to spend less computation time and resources, and find a match record more quickly when a record match process is invoked by backend server, since the server only needs to calculate *m-n* times of PRNG function iteratively with the received $PRNG^{n}(EPC_x)$ value as the starting seed before matching the computed result with the primary key of each EPC records. On the contrary, most of previous published schemes [1, 4, 6, 8-12] have to get each EPC entry, calculate its hashed value or perform other functional computation, then use the computed result to match with the received encrypted value from a RFID tag, and keep performing the same operation iteratively through all EPC records in the database until a match is found. In addition, our scheme is compatible with EPC Class-1 GEN-2 standards because only pseudo-random number generator and basic XOR function are adopted and both functions are specified in EPC standards. The

compliance of RFID standards of our authentication scheme greatly increases the possibility of its adoption by RFID systems vendors and corresponding industrial customers in practice.

Table 1 shows the comparison results among our scheme and the others in accordance with the security and efficiency requirements. Obviously, the proposed mutual authentication scheme is superior to the others by supporting all criterions.

**Table 1. Comparison among proposed RFID authentication schemes**

| | EPCglobal Class-1 Gen-2 standards compliance | Data security | Anonymity (resistance to tracking attack) | Resistance to replay attack | Resistance to DoS attack | Forward security | Backend server load |
|---|---|---|---|---|---|---|---|
| Weis et al. [4] (Hash-based access control) | X | X | X | X | O | X | O(1) |
| Weis et al. [4] (Randomized hash-locking access control) | X | X | O | X | O | X | O(k) |
| Ohkubo et al. [9] | X | O | O | X | O | O | O(k) |
| Henrici & Müller. [2] | X | O | X | O | O | X | O(1) |
| Rhee et al. [10] | X | O | O | X | O | X | O(k) |
| Molnar-Wanger [8] | X | O | O | X | O | X | O(k) |
| Yang et al. [11] | X | O | X | X | O | X | O(k) |
| An & Oh [12] | X | O | O | X | O | X | O(k) |
| Karthikeyan-Nesterenko [7] | O | O | X | X | X | X | O(1) |
| Duc et al. [6] | O | O | X | X | X | X | O(k) |
| Chien & Chen [1] | O | O | X | X | O | X | O(k) |
| Our scheme | O | O | O | O | O | O | O($m$-$n$) |

k: the number of tuples in database
m: server pre-defined value
n: random number generated at each session where $m>n$

## 6 Conclusion

In this paper we present a new mutual authentication scheme for RFID systems. Our scheme makes the RFID authentication process more robust and secure by introducing dynamical mechanism to change the authentication key and the access key with different random numbers at each authentication phase. Furthermore, the scheme also reduces the workload of the backend server from iteratively retrieving and computing each tuple linearly in database. Finally, our scheme improves data security and privacy protection for RFID systems from the previous authentication schemes and is compatible with the EPC Class-1 GEN-2 standards. In brief, our scheme can defend against the serious replay attack and DoS attack. At the same time the scheme provides excellent privacy protection such as anonymity and forward secrecy.

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

## References


1. Hung-Yu Chien and Che-Hao Chen, Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards, Computer Standards & Interfaces, Volume 29, Issue 2, Pages 254-259, February 2007.
2. Dirk Henrici and Paul Műller, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, in Workshop on Pervasive Computing and Communications Security (PerSec'04) at IEEE PerCom 2004, March 14-17, 2004, Orlando, Florida, USA PERCOMW, 2004.
3. EPCglobal, available at http://www.EPCglobalinc.org/
4. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, in Security in Pervasive Computing, Page(s):201-212, 2003.
5. Simon L. Garfinkel, Ari Juels and Ravi Pappu, RFID Privacy: An overview of Problems and Proposed Solutions, in IEEE Security & Privacy Magazine, 3 (3):34-43, May-June 2005.
6. Dang Nguyen Duc, Jaemin Park, Hyunrok Lee and Kwangjo Kim, Enhancing Security of EPCglobal GEN-2 RFID Tag against Traceability and Cloning, The 2006 Symposium on Cryptography and Information Security, Hiroshima, Japan, Jan. 17-20, 2006.
7. Sindhu Karthikeyan and Mikhail Nesterenko, RFID Security without Extensive Cryptography, in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Page(s):63-67, 2005.
8. David Molnar and David Wagner, Privacy and Security in Library RFID: Issues, Practices, and Architectures, in Conference on Computer and Communications Security - CCS'04, pp. 210-219, October 2004.
9. Miyako Ohkubo, Koutarou Suzki and Shingo Kinoshita, Cryptographic Approach to 'Privacyfriendly' Tags, in RFID Privacy Workshop, MIT, MA, USA, Nov. 2003.
10. Keunwoo Rhee, Jin Kwak, Seungjoo Kim and Dongho Won, "Challenge-response Based RFID Authentication Protocol for Distributed Database Environment," in International Conference on Security in Pervasive Computing - SPC 2005, pp.70-84, 2005.
11. Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren and Kwangjo Kim, "Mutual Authentication Protocol for Low-cost RFID," in the Encrypt Workshop on RFID and Lightweight Crypto, 2005.
12. Younghwa An and Soohyun Oh, RFID System for User's Privacy Protection, in Asia-Pacific Conference on Communications, Page(s):516-519, Oct. 2005
13. Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9, Available at http://epcis.mit.edu/CS/files/folders/epcglobal/entry21.aspx
14. G. Avoine, E. Dysli and P. Oechslin, Reducing Time Complexity in RFID Systems, in the 12th Annual Workshop on Selected Areas in Cryptography (SAC'05), Kingston, Canada, August 11-12, LNCS, Springer, 2005.
15. N.W. Lo and Kuo-Hui Yeh, Novel RFID Authentication Schemes for Security Enhancement and System Efficiency, to be appeared in the 4th VLDB workshop on Secure Data Management, SDM'07, September, LNCS, Springer, 2007.