Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 29 (2007) 254–259
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

Mutual authentication protocol for **RFID** conforming to **EPC** Class 1 Generation 2 standards

Hung-Yu Chien [a,*], Che-Hao Chen [b]

[a] *Department of Information Management, National Chi Nan University, University Rd. Puli, Nantou County, Taiwan 545-61, ROC*
[b] *Department of Information Management, Chaoyang University of Technology, Wufong, Taichung 41349, Taiwan, ROC*

Received 13 April 2006; accepted 19 April 2006
Available online 15 June 2006

Abstract

As low-cost Radio Frequency Identification (**RFID**) will become pervasive in our daily lives, **RFID** systems may create new threats to the security and privacy of individuals and organizations. However, the previous works on designing security protocols for **RFID** either do not conform to the **EPC** Class 1 Generation 2 standards or suffer from security flaws. This paper will point out the weaknesses of two **EPC** Class 1 **GEN-2**-conformed security protocols, and then proposes our new protocol, which raises the security level and conforms to the **EPC** Class 1 **GEN-2** standards.

Keywords: **RFID**; **EPCglobal**; Security; **CRC**; Hash

1. Introduction

Radio Frequency Identification (**RFID**) systems, thanks to their low cost and their convenience in identifying an object without physical contact, have found many applications in manufacturing, supply chain management, parking garage management, and inventory control. Technology advancements of Silicon manufacturing makes **RFID** systems more and more low-cost and makes them an economical replacement for optical barcode in consumer object identification. Beyond simple identification, other functions like integrated sensors, to read/write storage, encryption and access control might be incorporated into **RFID** systems. These convenient features and the low cost will make **RFID** systems the most pervasive microchips in history [1].

RFID systems consist of radio frequency (**RF**) tags, or transponders, and **RF** tag readers, or transceivers. Tag readers can *inquire* tags of their contents by broadcasting an **RF** signal, without physical contact, through non-conducting materials such as paper or cardboard, at a rate of several hundred tags per second, and from a range of several meters. **RFID** devices can be broadly classified as two categories: those with a power supply and those without. **RFID** devices with power supply that actively transmitted to a reader are known as "active tags" and un-powered tags that are triggered by a reader are called "passive tags". **EPCglobal** and **ISO** are two important organizations standardizing and promoting **RFID** technology. Particularly, **EPCglobal** is a joint venture between **EAN** International (Europe) and **UCC** (USA) aiming at developing industry **RFID** standards. It is believed that **EPCglobal** has great potential to influence the standard for **RFID** technology at the global scale [3,5,6]. One of the most important standards proposed by **EPCglobal** is the **EPCglobal** Class-1 **GEN-2 RFID** specification (which is called **GEN-2 RFID** for short in this paper) that defines the functionality and operation of a **RFID** tag. However, as pointed by the previous works [3,5,6], **GEN-2 RFID** specification with its limited resource pays little attention to the following security threats, which would harm its global proliferation.

The widespread deployment of **RFID** systems into consumer products identification may expose potential security threat and risks either to corporations or individuals. Corporate espionage may *inquire* unprotected **RFID**s to gather information illegally, spoof tags to provide wrong information, or even launch Denial of Service (**DOS**) attacks to their competitors. Most consumers would prefer to keep the **RFID** tagged contents private from outsiders. However, a tag reader at a fixed location could track

* Corresponding author.
E-mail addresses: redfish6@ms45.hinet.net (H.-Y. Chien), s9214630@mail.cyut.edu.tw (C.-H. Chen).

0920-5489/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2006.04.004

RFID-tagged products carried by people passing by or even identify the people if the tags contain information like special product brand or unique taste. Correlating data from multiple tag reader locations could even track the movement, and social interactions. Besides these passive eavesdropping and tracking, an **RFID** system might be susceptible to denial of service attacks or tag spoofing. A thief might use counterfeit tags to fool automated checkout or security systems into thinking that a product was still on the shelf or replace a tag that specifies an expensive item with a tag for cheap items. So, the security requirements for **RFID** systems might include content privacy, access control, authentication, and anonymity. Authentication is required for a tag reader to authenticate genuine tags for inquiring information, and for tags to provide information to authenticated readers only. After authentication, only authenticated readers can access the contents of tags. Some **RFID** implementations would expose tags identifications when readers inquire them. With anonymity, tags will not expose their identifications to eavesdroppers without authentications.

To cope with the security threats, several security protocols [2–15] had been proposed to enhance the security of **RFID** systems. However, all these protocols either cannot conform to **GEN-2 RFID** specifications (even though encryption function and hash function are commonly supported on smart cards, they are still infeasible on **GEN-2 RFID** tags, but these schemes required the support of either hash function or encryption function on the tag) or suffer from security flaws. Only few proposed schemes [3,5,6] can be implemented on **GEN-2 RFID** tags. For those schemes that use only **GEN-2** supported functions and can be effectively implemented on **GEN-2** tags, we call them **GEN-2** conformed schemes. Unfortunately, these schemes still suffer from security weaknesses. This paper will show the security weaknesses of two **GEN-2 RFID** conformed protocols, and then will propose a new scheme that conforms to the **GEN-2 RFID** specifications and conquer all the weaknesses of the previous schemes. The rest of this paper is organized as follows. Section 2 introduces **GEN-2 RFID** specifications, focusing on security-related features, and then discusses related works. Section 3 reviews two **GEN-2 RFID** conformed schemes and points out their security weaknesses. Section 4 proposes our new scheme for **GEN-2 RFID**, which conquers all the security problems that bother the previous schemes. Section 5 evaluates its performance and analyzes its security, which is followed by our conclusions in Section 6.

2. GEN-2 RFID specification and related works

2.1. GEN-2 RFID *specifications*

We briefly summarize some important properties of **GEN-2 RFID** specification [1] as follows.

GEN-2 RFID tag is passive, and its power is triggered by the readers. Cost limitation and limited resources dictate that **GEN-2** tags cannot afford the cost expensive public key encryptions, symmetric encryption, or even hash functions. **GEN-2 RFID** tag supports on-chip 16-bit Pseudo-Random Number Generator (**PRNG**), and a 16-bit Cyclic Redundancy Code (**CRC**) checksum is used to detect error in transmitted data. Tag memory is insecure and susceptible to physical attacks. That is, tags cannot be trusted to store global, long-term secrets, when left in isolation. A *kill* command with a 32-bit **PIN** is used to protect the privacy of a **GEN-2 RFID** tag by permanently make it usable. A 32-bit *access* **PIN** is required to trigger a tag into the secure mode. After that, the tag is allowed to READ/WRITE. Tags may be equipped with a physical contact channel for critical functions or for "imprinting secret keys". Tags readers are assumed to have a secure connection to a back-end database.

Duc et al. [3] had pointed out several weaknesses of **GEN-2 RFID** specification as follows. (1) **GEN-2 RFID** uses the *kill* command to permanently make a tag unusable to protect the privacy of the tag. This approach is not appropriate for some occasions. For example, the customer service would need the information of a product for warranty purpose, but the tag on the product had being *killed* after its purchase. (2) It is feasible for an attacker to eavesdrop the communications (which contain random numbers and **XOR**ed **PIN**s) and then to derive the **PIN** by **XOR**ing (exclusive **OR**) the 16-bit random number with the **XOR**ed **PIN**. After deriving the **PIN**, it is easy for the attacker to access the tags and trace the tags.

To overcome the above security weaknesses of **GEN-2 RFID** tags, Juels [5], Duc et al. [3], and Karthikeyan and Nesterenko [6] had respectively proposed their new security schemes for **GEN-2 RFID**-conformed tags. Their schemes, instead of using hash functions, public key cryptography, and convention encryptions, only use those operations (**PRNG** and **CRC**) supported on a **GEN-2 RFID** tag, and their schemes can be implemented on the resource-limited **GEN-2 RFID** tags.

2.2. Related works

Weis et al. [10,11] had proposed several security mechanisms for **RFID**. These mechanisms use **PRNG** function and hash functions, where hash functions are not supported on **GEN-2 RFID** tags. Therefore, their schemes are not **GEN-2 RFID** conformed. Additionally, we had reported several weaknesses of the schemes of Weis et al. [11]: (1) the schemes of Weis et al. require the backend server to store all the keys of the tags, which could be a big burden on the server; (2) the shared key between a tag and the server is highly likely to be exposed to an eavesdropper; (3) the reader or the server needs to perform exhaustive search to identify the tag, which not only limits the scalability but also increases the likelihood of chance of attackers to find a matched **ID** (the identity of a tag). Once a matched **ID** is found, the anonymity of the tag is violated. Even though Chien's scheme is secure, but it does not conform to the **GEN-2** standards.

Ohkubo et al. [8], also based on hashing chain, proposed a mutual authentication scheme for **RFID** system. The scheme aimed to provide the forward secrecy: that means even if we assume that an attacker can compromise a tag at some time, he cannot trace the past communications from the same tag. Unfortunately, the scheme cannot resist the replay attack [2].

The Henrici–MÄuller scheme [4] updates a tag's identification after each successful authentication, and uses this varying identification to protect location privacy and anonymity. However,

a tag always responses the same hashed value of the identification before the next successful authentication. This property allows an attacker to trace tags. Yang et al. [12,13] improved the Henrici–MÄuller scheme to achieve anonymity. However, it was pointed out that the scheme cannot protect privacy [2].

Rhee et al. [9], also based on **PRNG** function and hash function, proposed a mutual authentication scheme for **RFID** systems. However, the scheme cannot provide forward secrecy. Once a tag is compromised, the attacker can trace the past communications from this tag. Like Rhee et al.'s scheme, Molnar and Wagner's scheme [7] still cannot provide forward secrecy: once a tag is compromised, the past communications from this tag can be traced.

In addition to their security weaknesses, all the above mentioned schemes do not conform to **GEN-2 RFID** specifications, because the adopted hash functions cannot be supported on the current resource-limited **GEN-2 RFID** specifications. Aiming to enhance the security of **GEN-2 RFID** systems, the following schemes only use the functions support on **GEN-2 RFID** tags, and the schemes can be effectively implemented on **GEN-2** tags.

Juels [5] suggested a scheme to prevent the cloned tags from impersonating legitimate **GEN-2** tags. However, his protocol did not take eavesdropping and privacy issues into consideration, therefore provides no protection against privacy invasion and secret information leakage [3]. Another two recently published schemes for **GEN-2 RFID** tags are Karikeyan–Nesterenko's scheme [6] and Duc et al.'s scheme [3], where Karikeyan–Nesterenko's scheme only uses **XOR** operation and matrix operation and Duc et al.'s scheme uses only **PRNG** operation and **CRC** operations. However, we will show the weaknesses of these two schemes in this paper.

3. Two GEN-2 conformed security schemes and their weaknesses

This section briefly reviews two security schemes especially designed for **GEN-2 RFID**, and then shows their security weaknesses.

3.1. Karthikeyan–Nesterenko's scheme and its weaknesses

3.1.1. Review of Karthikeyan–Nesterenko's scheme

Karthikeyanand and Nesterenko [6], based on simple **XOR** operation and matrix operation, designed an efficient tag identification and reader authentication scheme for **GEN-2 RFID**. Initially, two matrices M_1 and M_2^{-1} are stored on each tag, and two matrices M_2 and M_1^{-1} are stored on the reader, where all the matrices are of size $p \times p$, and M_1^{-1} and M_2^{-1} are the inverses of M_1 and M_2 respectively. The tag and the reader also store a key K which is a vector of size q, where $q=rp$. That is, K can be represented as $K=[K_1, K_2, \ldots, K_r]$, where K_i, $i=1, 2\ldots, r$ are vectors of size p. As a slight abuse of notation, the notation $X=KM$, where K is a vector of size q and M is a $p \times p$ matrix, denotes a component-wise multiplication of K and M. That is, $X=[X_1, \ldots, X_r]=[K_1M, \ldots, K_rM]$.

When the reader inquires a tag, the tag computes $X=KM_1$, and sends back X to the reader. The reader then forwards the message to the backend server, where the server will search its database to find a match. If it can find a match, then the tag is identified, and the server performs the following operations to authenticate itself to the tag and renew the key. The server first computes $Y=(K_1 \oplus K_2 \oplus \ldots \oplus K_r)\, M_2$, randomly selects a vector X_{new} of size q, computes $K_{\text{new}}=X_{\text{new}}M_1^{-1}$ and $Z=K_{\text{new}}M_2$, and finally sends (Y, Z) to the reader, which forwards (Y, Z) to the tag. Upon receiving the response from the reader, the tag verifies whether the equation $YM_2^{-1} \stackrel{?}{=} (K_1 \oplus K_2 \oplus \ldots \oplus K_r)$ holds; if so, the tag updates the key as $K_{\text{new}}=ZM_2^{-1}$. The scheme is depicted in Fig. 1.

3.1.2. Weaknesses of Karthikeyan–Nesterenko's scheme

The scheme cannot resist the following attacks—Denial of Services attack (**DOS**), replay attack and individual tracing.

In Karthikeyan–Nesterenko's scheme, the tag does not authenticate the received value Z when updating the key. Therefore, an attacker can replace the transmitted Z with an old one $\overline{Z}$ or any random value Z^* without being noticed; Upon receiving a valid Y and the fake Z^*, the tag will authenticate the Y successfully and then will update the key as $K^*=M_1{}^1Z^*$. So, the legitimate reader and the tag cannot authenticate each other any more since the key is wrongly updated. The **DOS** attack succeeds. If the attacker replaces the Z with an old one $\overline{Z}$ (assuming $\overline{Y}$ and $\overline{Z}$ are previously sent in the ith legal session) in the above mentioned attack, then the attacker can replay the $\overline{Y}$ in the next session to cheat the tag in wrongly accepting the request and access the tag accordingly. He can even record the transmitted data from several sessions, and then launches the above attack several times. This will allow the attacker to trace the tag. Therefore, the anonymity property is violated.

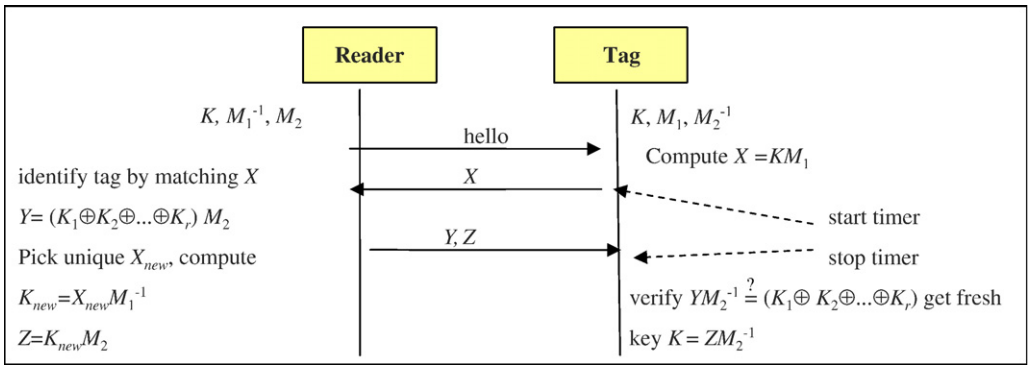


Fig. 1. Karthikeyan–Nesterenko's scheme.

3.2. Duc et al.'s scheme and its weaknesses

3.2.1. Review of Duc et al.'s scheme

Initially, each tag and the backend server share the tag's EPC code, the tag's *access* **PIN**, and an initial key K_0 (this key will be updated after each successful authentication, and K_i denotes the key after ith authentication). The steps of $(i+1)$th authentication are described as follows, where **CRC** denotes the Cyclic Redundancy Code, $f()$ denotes the **PRNG** function and "Reader → tag: M" denotes the reader sends the tag a message M.

1. Reader → tag: *Query request*.
2. Tag → reader → server: M_1, r, C.

The tag selects a random number r, computes $M_1 = \mathbf{CRC}(\mathbf{EPC}||r) \oplus K_i$ and $C = \mathbf{CRC}(M_1 \oplus r)$, and sends back ($M_1$, r, C) to the reader, where the reader will forward (M_1, r, C) to the backend server.

3. Server → reader: the tag's info or "*failure*".

For each tuple (**EPC**, K_i) in its database, the server verifies whether the equations $M_1 \oplus K_i \stackrel{?}{=} \mathbf{CRC}(\mathbf{EPC}||r)$ and $C \stackrel{?}{=} \mathbf{CRC}(M_1 \oplus r)$ hold. If it can find a match, then the tag is successfully identified and authenticated, and the server will forward the tag's information to the reader and proceed to the next step; otherwise, it stops the process with failure.

4. Server → Reader → tag: M_2

To authenticate itself to the tag and update the information on the tag, the server computes $M_2 = \mathbf{CRC}(\mathbf{EPC}||\mathrm{PIN}||r) \oplus K_i$ and sends M_2 to the tag through the reader. Upon receiving M_2, the tag locally computes its M_2, using its local values (**PIN**, r, **EPC**, K_i), and verifies whether the received M_2 equals the local one. If so, the tag will accept the "end session" command in the next step.

5. Reader → tag: "end session"
   Reader → server: "end session".

■ Upon receiving the "end session" command, both the server and the tag update their shared key as $K_{i+1} = f(K_i)$ (Fig. 2).

3.2.2. The weaknesses

Duc et al.'s scheme cannot resist the **DOS** attack against tags and readers, cannot detect the disguise of tags, and cannot provide forward secrecy. A **RFID** system with forward secrecy means that, even assume that a tag is compromised at some time later, the past communications from the same tag cannot be traced.

(1) In the last step of Duc et al.'s scheme, the reader sends the "end session" commands to both the tag and the backend server to update the key. If one of the "end session" commands is intercepted, then the shared key between the tag and the server will be out of synchronization. Thus, the tag and the reader cannot authenticate each other any more. The **DOS** attack succeeds. (2) If it is the "end session" command to the server is intercepted, then the server will hold the old key; therefore, a counterfeit tag can replay the old data (M_1, r, C) to disguise as a legitimate tag. So, the scheme fails to detect a disguised tag. (3) The scheme cannot provide forward secrecy. Suppose a tag is compromised, then the attacker would get the values (**EPC**, **PIN**, K_i) of the tag; so, from the eavesdropped data (M_1, M_2, r) of the past communications, the attacker can verify whether a communication comes from the same tag by performing the following checking. For each eavesdropped communication (M_1, M_2, r), he computes $M_1 \oplus M_2$ to derive the value $\mathbf{CRC}(\mathbf{EPC} \oplus r) \oplus \mathbf{CRC}(\mathbf{EPC}||\mathbf{PIN}||r)$, and then, using the compromised values (**EPC**, **PIN**, K_i) and the eavesdropped r, he can do the same computation to verify whether it came from the same tag. So, the past communications of a compromised tag can be traced.

4. New scheme

This section, based on the **EPC** Class 1 **GEN-2** standards, will propose a mutual authentication protocol for **RFID** systems to improve the security performance.

4.1. Assumptions

Our scheme is based on the **GEN-2** standards, where **PRNG** and **CRC** are supported on the passive tags. Like the previous schemes, we assume an attacker can monitor and modify the communications between the reader and the tags, but the communication between the reader and the backend server is secure. The passive tags are vulnerable to compromise, and the contents of a tag can be derived by the attacker once it is compromised.

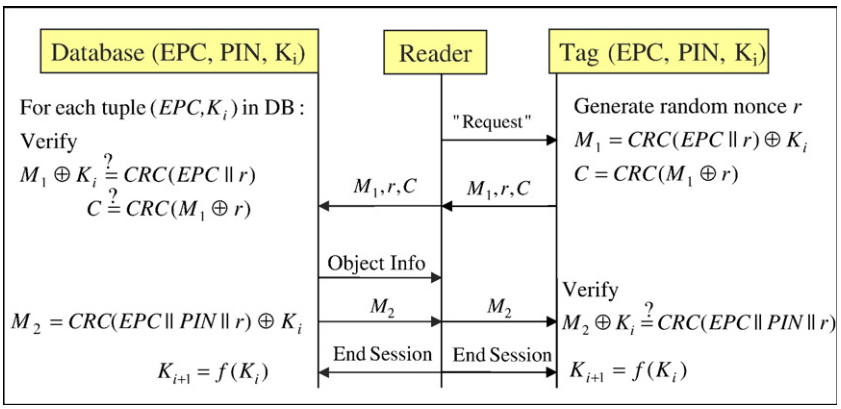


Fig. 2. Duc et al.'s scheme.

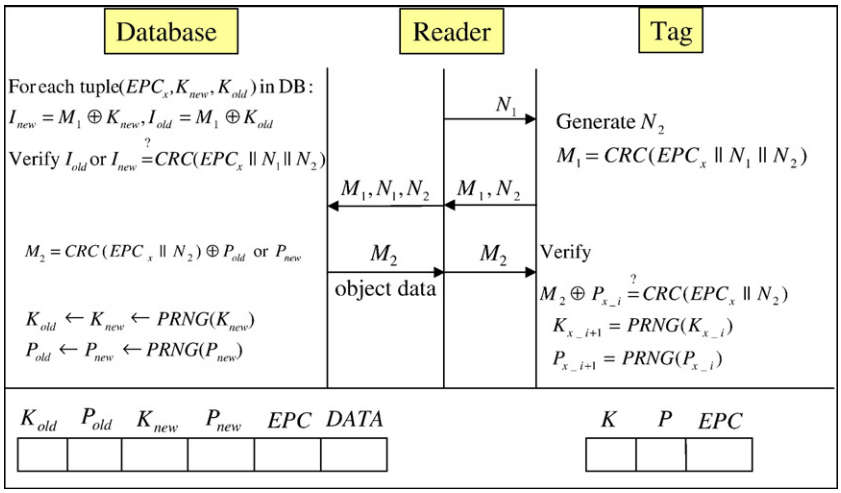


Fig. 3. Our proposed scheme.

4.2. Mutual authentication scheme for GEN-2 RFID

The scheme consists of two phases — the initialization phase and the authentication phase.

4.2.1. Initialization phase

For each tag, which is denoted as Tag_x, the server randomly selects an initial authentication key K_{x_0} and an initial access key P_{x_0}. The server initially stores three values in the tag — (1) $\mathbf{EPC}_x$ denotes the Electronic Product Code (**EPC** code) of the tag, (2) the initial authentication key K_{x_0}, and (3) the initial access key P_{x_0}. The authentication key and the access key will be updated after each successful authentication, and the authentication key after the ith successful session is denoted as K_{x_i} and the access key after the ith session is denoted as P_{x_0}. For each tag, the server also maintains a record of six values in its database — (1) $\mathbf{EPC}_x$; (2) K_{old} denotes the old authentication key for this tag, and it is initially set to K_{x_0}; (3) P_{old} denotes the old access key for this tag, and it is initially set to P_{x_0}; (4) K_{new} denotes the new authentication key, and it is initially set to K_{x_0}, too; (5) P_{new} denotes the new access key, and it is initially set to P_{x_0}, too; (6) DATA denotes all the other information about the tagged object. The design of two sets of authentication key and access key is to defend the **DOS** attack that causes out of synchronization between the tag and the server. After initialization, the reader and the tag can perform authentications, and the $(i+1)$th authentication between the tag (Tag_x) and the server (S) via the reader (R) is described as follow.

4.3. The (i + 1)th authentication phase

1. $R \rightarrow \text{Tag}_x$: N_1

The reader sends a random nonce N_1 as a challenge to the tag.

2. $\text{Tag}_x \rightarrow R \rightarrow S$: M_1, N_1, N_2

The tag generates a random number N_2, computes $M_1 = \mathbf{CRC}(\mathbf{EPC}_x \| N_1 \| N_2) \oplus K_{x\_i}$, and sends the values ($M_1$, N_1, N_2) back to the reader, which will forward these values to the server.

When the server receives the authentication request from the reader, it iteratively picks up an entry ($\mathbf{EPC}_x$, K_{old}, K_{new}, P_{old}, P_{new}, DATA) from its database, computes the values $I_{\text{old}} = M_1 \oplus K_{\text{old}}$ and $I_{\text{new}} = M_1 \oplus K_{\text{new}}$, and checks whether any of the two equations $I_{\text{old}} \stackrel{?}{=} \mathbf{CRC}(\mathbf{EPC}_x \| N_1 \| N_2)$ and $I_{\text{new}} \stackrel{?}{=} \mathbf{CRC}(\mathbf{EPC}_x \| N_1 \| N_2)$ hold. The process is iteratively repeated for each entry until it finds a match. If it can find a match, then the authentication of the tag succeeds, and the server performs the next step; otherwise, it sends a "failure" message to the reader to stop the process.

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

If the server successfully authenticates the tag in the previous step, it computes $M_2 = \mathbf{CRC}(\mathbf{EPC}_x \| N_2) \oplus P_{\text{old}}$ or $M_2 = \mathbf{CRC}(\mathbf{EPC}_x \| N_2) \oplus P_{\text{new}}$, depending on which value (K_{old} or K_{new})

Table 1
Comparisons among related security schemes for **RFID**

	GEN-2 conformed	Privacy	Anonymity	Resist to replay attack	Resistance to **DOS** attack	Forward secrecy
Weis et al. [11]	X	X	X	X	o	X
Ohkubo et al. [8]	X	o	o	X	o	o
Henrici–MÄuller [4]	X	o	X	X	o	X
Rhee et al. [9]	X	o	o	o	o	X
Molnar–Wagner [7]	X	o	o	o	o	X
Yang et al. [12,13]	X	o	X	o	o	X
Karthikeyan–Nesterenko [6]	o	o	X	X	X	X
Duc et al. [3]	o	o	o	X	X	X
Chien [15]	X	o	o	o	o	o
Our scheme	o	o	o	o	o	o

satisfies the verification equation in the previous step. It also updates $K_{old}=K_{new}$, $P_{old}=P_{new}$, $K_{new}=\mathbf{PRNG}(K_{new})$ and $P_{new}=\mathbf{PRNG}(P_{new})$. The server then sends (M_2, DATA) to the reader.

4. $R \rightarrow \mathrm{Tag}_x$: M_2

The reader retrieves the product information (DATA) and forwards M_2 to the tag.

Upon receiving M_2, the tag verifies whether the equation $M_2 \oplus P_{xi} \stackrel{?}{=} \mathbf{CRC}(\mathbf{EPC}_x||N_2)$ holds. If so, it updates its keys as $K_{x\_i+1}=\mathbf{PRNG}(K_{x\_i})$ and $P_{x\_i+1}=\mathbf{PRNG}(P_{x\_i})$. This design of updating the keys can resist the replay attack, and the design of simultaneously maintaining old key and new key for each tag can resist the **DOS** attack (Fig. 3).

5. Performance evaluation and security analysis

Our scheme ensures mutual authentication of the reader (the server) and the tag, and can resist the replay attack, due to the challenge and response technology and the freshness of the random number N_1 and N_2 per session. Only the randomized data (M_1, N_1, N_2) are transmitted on the wireless channel between the reader and the tag, and the product information ($\mathbf{EPC}_x$ and DATA) are only transmitted from the server to the reader through the secure channel. Therefore, the privacy property and the anonymity property are ensured. To defend against the **DOS** attack, we maintain two sets of (authentication key, access key) on the server, and this arrangement allows the server to authenticate the tag and to re-synchronize with the tag, even assuming they are out of synchronization due to the **DOS** attack. Because the keys are updated after each successful authentication and the keys are generated by applying the pseudo random function, the compromise of a tag would not lead to the compromise (or tracing) of the previous communications from the same tag. The forward secrecy is achieved. In summary, our scheme, which conforms to the **GEN-2** standards, overcomes all the security weaknesses found in the previous schemes, and the comparisons are summarized in Table 1.

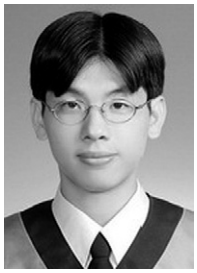
6. Conclusions

There have been several security schemes proposed for **RFID** systems, but only few of them conform to the **EPCglobal** Class 1**GEN-2** standards. However, we have pointed out the security weaknesses of two previous **GEN-2** conformed schemes — Karthikeyan–Nesterenko's scheme and Duc et al.'s scheme, and have proposed a new scheme that conforms to the **GEN-2** standards and improves the security performance.

References

[1] EPCglobal, http://www.EPCglobalinc.org/.
[2] G. Avoine, E. Dysli, P. Oechslin, Reducing time complexity in RFID systems, The 12th Annual Workshop on Selected Areas in Cryptography (SAC), 2005.
[3] D.N. Duc, J. Park, H. Lee, K. Kim, Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning, The 2006 Symposium on Cryptography and Information Security, 2006.
[4] A.D. Henrici, P. MÄuller, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, In the Proceedings of PerSec'04 at IEEE PerCom, 2004, pp. 149–153.
[5] A. Juels, Strengthening EPC tag against cloning, To Appear in the Proceedings of WiSe '05, 2005.
[6] S. Karthikeyan, M. Nesterenko, RFID security without extensive cryptography, Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005, pp. 63–67.
[7] D. Molnar, D. Wagner, Privacy and security in library RFID: issues, practices, and architectures, Conference on Computer and Communications Security — CCS'04, 2004, pp. 210–219.
[8] M. Ohkubo, K. Suzki, S. Kinoshita, Cryptographic approach to 'privacy-friendly' tags, RFID Privacy Workshop, 2003.
[9] K. Rhee, J. Kwak, S. Kim, D. Won, Challenge-response based RFID authentication protocol for distributed database environment, International Conference on Security in Pervasive Computing — SPC 2005, 2005, pp. 70–84.
[10] S.A. Weis, Security and privacy in radio-frequency identification devices, *Masters Thesis MIT*, 2003.
[11] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, The Proceedings of the First Security in Pervasive Computing, LNCS, vol. 2802, 2003, pp. 201–212.
[12] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, Mutual authentication protocol for low-cost RFID, Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, 2005.
[13] J. Yang, K. Ren, K. Kim, Security and privacy on authentication protocol for low-cost radio, The 2005 Symposium on Cryptography and Information Security, 2005.
[14] T. Phillips, T. Karygiannis, R. Kuhn, Security standards for the RFID market, IEEE Security and Privacy, vol. 3, No. 6, 2005, pp. 85–89.
[15] H.Y. Chien, Secure access control schemes for RFID systems with anonymity, *accepted and to be printed in proceedings of 2006 International Workshop on Future Mobile and Ubiquitous Information Technologies* (*FMUIT'06*), May, Japan.

Hung-Yu Chien received his B.S. degree in Computer Science from NCTU, Taiwan, 1988, his M.S. degree in Computer and Information Engineering from NTU, Taiwan, 1990, and his doctoral degree in applied mathematics at NCHU 2002. He was an assistant researcher at TL, MOTC, Taiwan, during 1992–1995. He was an associate professor of ChaoYang University of Technology during 2003–2006/08. Now he is an associate professor of National Chi Nan University, a member of the Chinese Association for Information Security, an IEEE member, IEICE member and an ACM member. His research interests include cryptography, networking and network security.



Che-Cho Chen received the M.S. degree in Information Management from ChaoYang University, Taiwan, 2006/06. His interests include RFID security and applications, and sensor network security.