RFID Ownership Transfer Authorization Systems Conforming EPCglobal Class-1 Generation-2 Standards

Chin-Ling Chen[1], Yeong-Lin Lai[2], Chih-Cheng Chen[2], Yong-Yuan Deng[1], and Yu-Cheng Hwang[1]
(Corresponding author: Chin-Ling Chen)

Department of Computer Science and Information Engineering, Chaoyang University of Technology[1]
168 Jifong E. Rd., Wufong Township, Taichung County, 41349, Taiwan, R.O.C. (Email: clc@mail.cyut.edu.tw)
Department of Mechatronics Engineering, National Changhua University of Education, Changhua, Taiwan[2]

(Received May 1, 2010; revised and accepted June 22 & June 30, 2010)

Abstract

Radio-frequency identification (RFID) has become the center of attention in automatic identification technology. However, many security problems still could be found in the system design. Recent researches have pointed out the applications of RFID to ownership transfer, but these applications cannot achieve the Electronic Product Code (EPC) Class-1 Generation-2 standards. In this paper, we propose an ideal RFID system, which conforms EPCglobal Class-1 Generation-2 standards ownership transfer. The system accomplished the functions including mutual authentication, guarantee of privacy, conformation to EPCglobal Class-1 Generation-2 industry standards, and prevention of any third party attack. The features in our method are to ensure the transaction security as well as protect the privacy.

Keywords: Authentication, electronic product code (EPC), ownership transfer, radio frequency identification (RFID), security

1 Introduction

Radio-frequency identification (RFID) is a new technology which combines many subjects and many technologies. In recent years, it has been enormously applied to our daily life. Nowadays, because many features of the RFID system consisting of tags, readers, hosts, and antennas are superior to the bar code system, a mass of bar code environments have been gradually replaced with the RFID system. The RFID system can identify objects far beyond the sight, while objects can only be censored in the extremely close and almost-touched distance within the bar code system. Besides, the RFID system is equipped with a large amount of storage space so as that every tag can have its unique code; the bar code system cannot have this function in this respect. Therefore, the RFID system does well in stock, sales management and its applications to the merchandize bring a lot of conveniences [3].

However, there is no denying that the RFID is exposed to the risk of privacy and danger. With the decreasing of RFID cost, the applications of the RFID system are getting wider and wider and mixing without daily life, such as exit and entrance control, pet identification, electronic toll collection, industrial control, asset management, and home automation. Owning to a lack of consistent standard, every manufacturer adopts different systems; therefore, the integration is not satisfactory [2].

RFID transmits data by wireless communication. In order to ensure the security in communication transmission, the readers and the tags have to be authorized to legalization of both sides. However, since the operational ability of the tag is limited, it does not have the abilities of the complex encryption or decryption. Therefore, some researchers have pointed out the authorization protocol of the hash function based on low cost to conform the legal of the communication targets [15].

The hash lock method refers to a process in which the reader makes a request signal to the tag, and the tag will transfer a metaID to the reader. The metaID is a value that the tag and the reader use the hash function to compute K and obtain $h(k)$. The result will be sent back to the tag, and tag can verify $metaID \overset{?}{=} h(k)$ to judge whether the reader is legal. However, when the attacker gets metaID and K from the communication between the tag and the reader, he may disguise himself as a legal tag and a legal reader to interfere the communication between the tag and the reader to keep the communication from privacy.

Later, the latest researchers [1, 12, 14, 16] improve the security by encryption with the key and by interruption of the random numbers. In order to encrypt or decrypt with the key, the tag must have stronger operational abilities. The power consumption, solidity, weight, and manufacture cost have to be taken into consideration. Besides, should the key be decrypted by the attacker or be known to the public, the previous transmitting record of the tag will be known by the attacker, and user's privacy will also be threatened.

In addition, plenty of literature reviews [5, 8, 10, 11, 13] have mentioned the RFID-related sources can be applied to ownership transfer. But these applications are not able to achieve the requirements of EPCglobal Class-1 Generation-2 standards ownership transfer. The new RFID standard by EPCglobal is named EPCglobal Class-1 Generation-2 RFID specification. We briefly summarize properties of Class-1 Generation-2 tag as follows [6, 7].

1) The Generation-2 RFID tag is passive, and the passive tag receives power supply from readers-2.

2) The Generation-2 RFID tag communicates at UHF band (800-960 MHz) and its communication range is from 2 m to 10 m.

3) The Generation-2 RFID tag only supports on-chip 16-bit Cyclic Redundancy Code (CRC) computation and 16-bit Pseudo-Random Number Generator (PRNG).

4) The Generation-2 RFID's privacy protection mechanism is to make the tag permanently unusable once it receives the kill command with a valid 32-bit kill PIN (e.g., tags can be killed at the point-of-sale).

5) Read/Write to Generation-2 RFID tag's memory is allowed only after it is in secure mode (i.e., after receiving access command with a valid 32-bit access PIN).

There are about 500-5000 logic gates in current RFID tags. Thus, the computing resource is limited. The similar encryption and hash function mechanisms [4, 8, 10] are infeasible for EPCglobal C1G2 RFID tags. None of these protocols can conform to EPCglobal C1G2 RFID standards.

The Cyclic Redundancy Check (CRC) is a checksum which is used to detect errors of data during transmission and storage. A CRC is a type of function in which a value of any length can be used as input, and a value of fixed length can be produced as output. The CRC checksum is then computed as a remainder of the division of the original data by the CRC polynomial. For example, the polynomial $x+1$ is a CRC polynomial resulting in 1-bit CRC checksum equivalent to parity bit. In EPCglobal Class-1 Gen-2 specification, a 16-bit CRC checksum is used to detect errors in transmitting data and the corresponding CRC polynomial of degree 16 is $x^{16}+x^{12}+x^5+1$.

In this paper, we design an ideal RFID system to conform the requirements of EPC Class-1 Generation-2 ownership transfer to ensure mutual authentication, privacy, meet the EPC Class-1 Generation-2 industry standards, and protect against the third party attack.

2 The Proposed Scheme

There our protocol focuses on the object to achieve the mutual authentication between the tags and the readers, and protect user's privacy to process the RFID ownership transfer system. We will explain the protocol in detail in the following section.

2.1 Notation

- N_i: a nonce word, if tags and readers are both registered to database, they will obtain N_i simultaneously.
- K_i: a key, if tags and readers are both registered to a database, they will obtain K_i simultaneously.
- $\oplus$: exclusive-or operation.
- RND: a random value which is generated by a reader.
- $Cert_i$: certificate of the object; when the user purchase the object i, he has the certificate.
- ID_x: the identification code of X.
- ID_{Ri}: the identification code of the i^{th} reader.
- A: old tag owner.
- B: new tag owner.
- Msg_{req}: request message.
- Sig_x: the signature value of x.
- $V_X(m)$: use X's private key to verify the message m.
- $E_X(m)$: use X's public key to encrypt the message m.
- $D_X(m)$: use X's public key to decrypt the message m.
- $S_X(m)$: use X's private key to make the signature of the message.
- $CRC(x)$: a Cyclic Redundancy Check (CRC) function.
- EPC_i: Electronic Product Code of i^{th} tag.
- $A \overset{?}{=} B$: compare whether A is equal to B or not.
- $PRNG$: pseudo random number.

2.2 Registration Phase

We divide the registration phase into two parts. Tags and readers must register to the database respectively. The database server gives the corresponding (N_i, K_i) to the tags and the readers. The corresponding (N_i, K_i) will be stored in the database server, as (N_i', K_i') in the tag, and as (N_i, K_i) in the reader. That is, only registered readers can read the specific tags of the object. In fact, after registration, the result is $N_i = N_i'$ and $K_i = K_i'$.

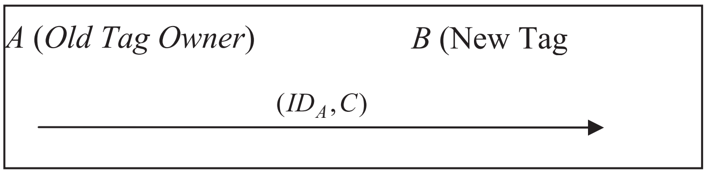

Figure 1: The flow chart of ownership transfer requiring phase

2.3 Ownership Transfer Requiring Phase

When user A wants to transfer the ownership of the tag to user B, A has to make up the message of ownership transfer and give it to B. Figure 1 is the first step of ownership transfer requiring phase. When user B wants to buy the product X from user A, user A has to transfer Tag_X of the product to user B, and simultaneously generates the message of ownership transfer. User A first makes the digital signature with its private key:

$$SG_A = S_A(Cert_i, ID_B).$$

1) After that, user A will encrypt (SG_A, $Cert_i$) with user B's public key to get $C = E_B(SG_A, Cert_i)$;

2) and transfers the message (ID_A, C) to User B.

2.4 Mutual Authentication Phase

Through the ownership transfer requiring phase, tags and readers can execute the mutual authentication procedures. The tags and the readers can judge whether they are legal devices or not. We utilize pseudo random number generators, exclusive-or operations and the lightweight CRC operation, which conforms to the EPC Class-1 Generation-2 standards to serve the function of mutual authentication. Figure 2 is the flow chart of the mutual authentication phase in this paper.

Step 1. When the reader wants to access a tag, it computes

$$A = CRC(N_i \oplus RND),$$

and sends a request message Msg_{reg}, A and RND to the tag.

Step 2. Upon receiving the A and RND, the tag will use the stored N_i' to compare as follows:

$$A \overset{?}{=} CRC(N_i' \oplus RND). \tag{1}$$

If the equation is true, the tag will generate a new random value RND_{new}, N_i'. Then, the tag calculates the parameters of Y, Z and update N_i'. Then, the tag computes:

$$\begin{aligned} N_i' &= N_{inew}{}' \\ X &= CRC(RND_{new} \oplus K_i') \\ Y &= (K_i' \oplus EPC_i \oplus X \oplus N_{i_{new}}') \\ Z &= CRC(X \oplus N_i' \oplus Y). \end{aligned}$$

Moreover, the tag updates (K_i') simultaneously, as follows:

$$K_{inew}' = PRNG(K_i').$$

The tag transfers (RND_{new}, Y, Z) to the reader.

Step 3. Upon receiving the responding message of the tag, the reader will use the K_i' and RND_{new} to calculate X' and CRC function to compare:

$$\begin{aligned} X' &= CRC(RND_{new} \oplus K_i) \\ Z &\overset{?}{=} CRC(X' \oplus N_i \oplus Y). \end{aligned} \tag{2}$$

If the equation is true, the reader will obtain $N_{i_{new}}$ and the tag also updates (K_i) as follows:

$$\begin{aligned} N_{i_{new}} &= (K_i \oplus EPC_i \oplus RND_{new} \oplus Y) \\ K_{i_{new}} &= PRNG(K_i). \end{aligned}$$

2.5 Ownership Transfer Phase for Renewal of Database Server

After the mutual authentication, the ownership transfer will be processed to update the database server. Figure 3 is the flow chart of the ownership transfer phase for the renewal of the database server.

Step 1. User B uses its own private key to decrypt C:

$$D_B(C) = (SG_A, Cert_i).$$

After obtaining SG_A, and $Cert_i$, user B uses user A's public key to verify the correction of SG_A as follows:

$$V_A(SG_A) \overset{?}{=} (Cert_i, ID_B).$$

User B uses its private key to make the signature of the message (ID_A, ID_B):

$$SG_B = S_B(ID_A, ID_B).$$

Then, user B uses the public key of the server to verify the correction of the certificate $Cert_i$ and to judge whether the $h(Cert_i')$ of Tag_X is correct. If the verification is correct, user B will transfer the message (ID_A, ID_B, SG_B, SG_A, $Cert_i$) to the reader of the server.

Step 2. When the reader received transfer message from tag, the reader will transfer (ID_A, ID_B, ID_{Ri}, SG_B, SG_A, $Cert_i$) to the server.

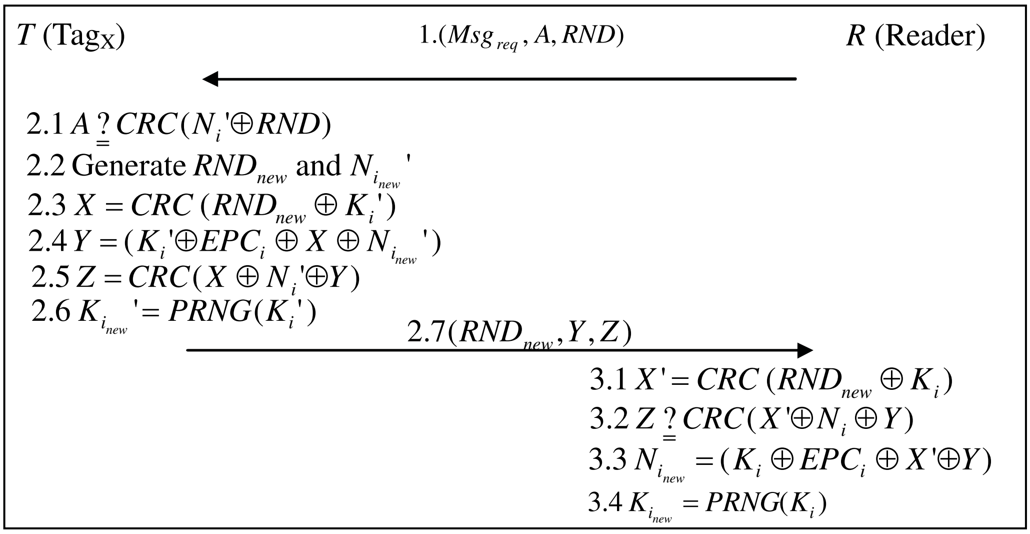
T (Tag$_X$)
1.(Msg_{req}, A, RND)
R (Reader)
2.1 $A \overset{?}{=} CRC(N_i' \oplus RND)$
2.2 Generate RND_{new} and $N_{i_{new}}'$
2.3 $X = CRC\ (RND_{new} \oplus K_i')$
2.4 $Y = (K_i' \oplus EPC_i \oplus X \oplus N_{i_{new}}')$
2.5 $Z = CRC(X \oplus N_i' \oplus Y)$
2.6 $K_{i_{new}}' = PRNG(K_i')$
2.7(RND_{new}, Y, Z)
3.1 $X' = CRC\ (RND_{new} \oplus K_i)$
3.2 $Z \overset{?}{=} CRC(X' \oplus N_i \oplus Y)$
3.3 $N_{i_{new}} = (K_i \oplus EPC_i \oplus X' \oplus Y)$
3.4 $K_{i_{new}} = PRNG(K_i)$

Figure 2: The flow chart of the mutual authentication phase

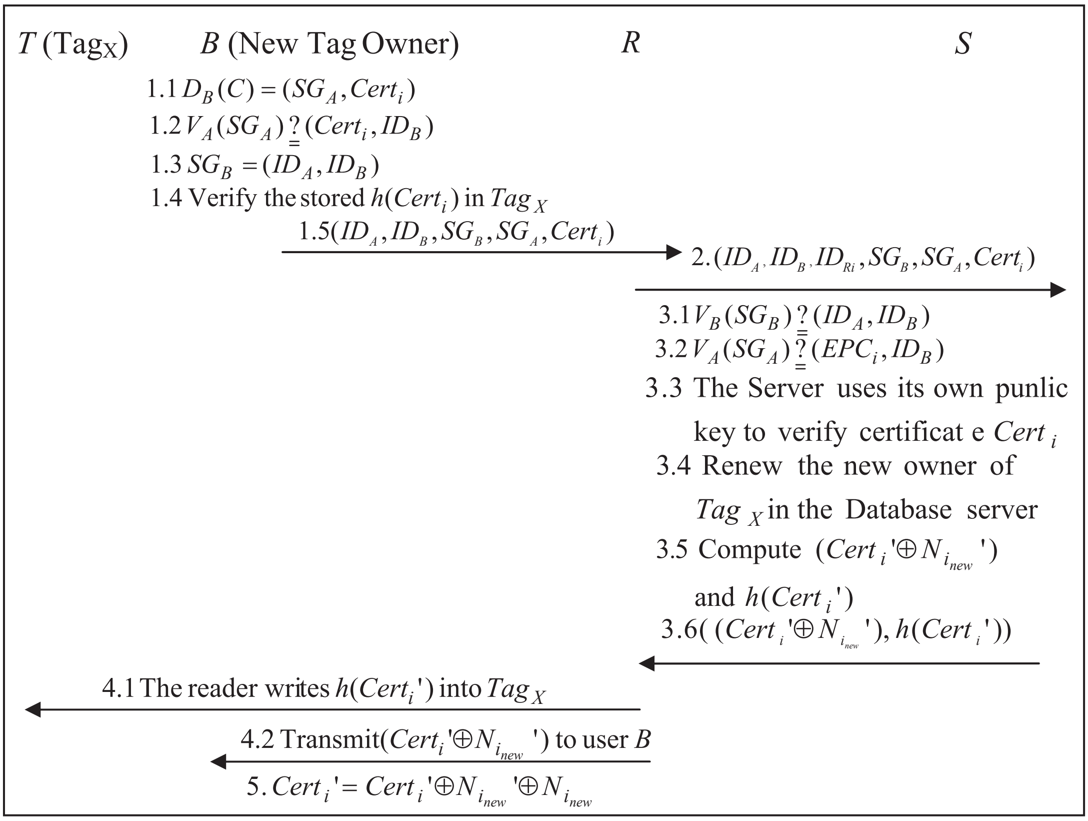
T (Tag$_X$)
B (New Tag Owner)
R
S
1.1 $D_B(C) = (SG_A, Cert_i)$
1.2 $V_A(SG_A) \overset{?}{=} (Cert_i, ID_B)$
1.3 $SG_B = (ID_A, ID_B)$
1.4 Verify the stored $h(Cert_i)$ in Tag_X
1.5$(ID_A, ID_B, SG_B, SG_A, Cert_i)$
2.$(ID_A, ID_B, ID_{Ri}, SG_B, SG_A, Cert_i)$
3.1 $V_B(SG_B) \overset{?}{=} (ID_A, ID_B)$
3.2 $V_A(SG_A) \overset{?}{=} (EPC_i, ID_B)$
3.3 The Server uses its own punlic key to verify certificat e $Cert_i$
3.4 Renew the new owner of Tag_X in the Database server
3.5 Compute $(Cert_i' \oplus N_{i_{new}}')$ and $h(Cert_i')$
3.6$((Cert_i' \oplus N_{i_{new}}'), h(Cert_i'))$
4.1 The reader writes $h(Cert_i')$ into Tag_X
4.2 Transmit$(Cert_i' \oplus N_{i_{new}}')$ to user B
5. $Cert_i' = Cert_i' \oplus N_{i_{new}}' \oplus N_{i_{new}}$

Figure 3: The flow chart of the ownership transfer phase for the renewal of the server's database

Step 3. After the database server receives the message, it will use user B's public key to verify B's signature:

$$V_B(SG_B) \overset{?}{=} (ID_A, ID_B).$$

If it is correct, the server will verify A's signature with A's public key:

$$V_A(SG_A) \overset{?}{=} (Cert_i, ID_B).$$

If the verification is correct, the server will use its public key to verify the correction of the certification $Cert_i'$.

The server will re-issue the new certificate $Cert'_i$, and then computes

$$Cert'_i \oplus N_{i'_{new}} \text{ and } h(Cert'_i).$$

The server also renews the new owner of Tag_X as B.

The server transmits $h(Cert'_i)$ and $(Cert'_i \oplus N_{i'_{new}})$ to the reader.

Step 4. After receiving the message, the reader will write $h(Cert'_i)$ into Tag_X and transmit $(Cert'_i \oplus N_{i'_{new}})$ to B.

Step 5. User B uses $N'_{i_{new}}$ stored in the memory to calculate $Cert'_i = Cert'_i \oplus N_{i'_{new}} \oplus N_{i'_{new}}$ and obtains the new certification $Cert'_i$.

3 Security Analysis and Discussion

In this section, we will examine and analyze the security requirements proposed in Section 1.

3.1 Security Analysis

3.1.1 Illegal Tag Access Analysis

The proposed scheme can avoid illegal tag access via the verification in Step 2 of the mutual authentication phase, in accordance with Equations (1). The tag will individually compare all values of N_i from the CRC function to the values of N_i from the reader. If there is the same value, the tag will do the further process. The message sent to the tag from the attacker will not contain the value of N_i which is allowed by the tag, so the tag will not make any response to it. Through this method, the illegal tag access from the attacker can be avoided.

3.1.2 Counterfeit Tag Attack Reader Analysis

The proposed scheme can also prevent attackers from using illegal tags to attack readers. The verification in Step 3 of the mutual authentication phase is according to Equations (2). The reader will use the random number RND_{new} in Step 1 to perform exclusive-or operation, and compare the value with Z from the tag to verify if they match for each other, and then the process will be performed further. The message sent to the reader from the attacker will not contain the correct N_i, so the reader will not do the follow-up operation. The attacker cannot use this method to paralyze the whole system.

3.1.3 Man-in-the-Middle Attack Analysis

This attack method refers to attackers attack the communication between tags and readers. However, this attack cannot succeed in our proposed scheme. Through RND and $CRC(N_i \oplus RND)$ in Step 1 of the mutual authentication phase and Z in Step 2 of the mutual authentication, we can verify the crucial transmission between the tag and the reader with the CRC function, the exclusive-or operation, or the protection of the key. The attackers cannot obtain the messages inside. Furthermore, we use the random values RND and RND_{new} during transmission process. When a reader finishes a query, the random value RND is always changed to increase the difficulty for attackers to decrypt.

3.1.4 User Privacy Analysis

Our scheme can protect the user's privacy for security. With layers and layers of protections, an attacker cannot obtain the ID value from the tag. Due to the verification formula in Step 2 of the mutual authentication is according to Equations (1).

The attacker cannot send out the value of N_i in the allowed list of the tag, so the tag will not make any response to the illegal reader. Moreover, through the protection in Step 2 of the mutual authentication phase, we can see that even if an attacker wants to intercept the messages between the tag and the reader, he only obtains the above protected message rather than know the real . Thus, the user's privacy can be ensured.

3.1.5 User's Location Privacy Analysis

Even though the attacker cannot obtain the message from a tag, yet he still cannot trace a user's location. However, he will fail in our proposed scheme. We use the CRC function and exclusive-or operation to protect the message $CRC(N_i \oplus RND)$ in Step 1 of the mutual authentication phase. Every time a tag and a reader finish a transmission, the reader will change the random value RND. Therefore, even if the attacker intercepts the message in which the tag responds to the legal reader, the reader will use a different random value for the next transmission. By doing so, the attacker will misjudge the identity of the tag; thus the attacker cannot lock the user's location.

3.1.6 Mutual Authentication between Tag and Reader Analysis

The proposed scheme can satisfy the mutual authentication mechanism between tags and readers. The verification in Step 2 of the mutual authentication phase is according to Equations (1).

Through the above verification, a tag can confirm whether it can be read by the legal reader. If a reader has not registered to the database and obtain the correct N_i, it cannot read the tag. After that, it will go into the verification in Step 3 of the mutual authentication phase in accordance with Equations (2).

The reader can confirm if the message is from the legal tag. Thus, the tag verifies the reader, and the reader also verifies the tag. The proposed scheme achieves mutual authentication between tags and readers.

Table 1: Security Comparison

Schemes	Hong and Tianjie Scheme [5]	Osaka et al.s Scheme [11]	Seo et al.s Scheme [13]	Our Scheme
Against Replay Attack	YES	YES	NO	YES
Against Denial of Service (DoS)	YES	YES	YES	YES
Against Man-in-the-Middle	NO	NO	NO	YES
Privacy	YES	YES	YES	YES
Against Counterfeit Tag	NO	NO	YES	YES
Mutual Authentication	NO	NO	NO	YES
Forward Security	YES	YES	YES	YES

3.1.7 Security Comparison

We make a security comparison with other related works in Table 1. Due to the previous schemes [5, 11, 13] only used one-way authentication, they suffer from the man-in-the-middle attack, counterfeit tag and replay attack. The tag cannot verify the transmission message of the reader, so if the attacker intercepts or falsifies the transmission messages from the reader, the tag can't confirm whether the message is legal or not. Therefore, they can't resist man-in-the-middle attack. Simultaneously, the previous works [5, 11, 13] cannot prevent counterfeit tag attack except for [13]. Our scheme ensures mutual authentication of the server and the tag, and can resist all of the possible attacks.

3.2 Discussions

3.2.1 EPCglobal Class-1 Generation-2 Standard Analysis

In the EPCglobal Class-1 Generation-2 standards, the computing resources of tags and readers are limited; they can only do CRC functions, exclusive-or operations, and generate random numbers. Other complex operations, like hash function, symmetric encryption, and asymmetric encryption cannot conform to the standard; thus our scheme can conform to the EPCglobal Class-1 Generation-2 standards.

3.2.2 Performance Evaluation

We compare the time complexity of the proposed method with those of the previous methods during the authentication phase in Table 2. Since our proposed scheme is using CRC and the random number generation operation which is a lightweight computation and it can achieve the mutual authentication. The previous methods [5, 11, 13] used hash function and RSA encryption operation, which is a high cost computation. Thus, the speed of the proposed scheme is even more efficient than the previous methods. Moreover, the proposed scheme can only be stored 96 bits in tag's memory that satisfies the standard of EPCglobal Class 1 Generation-2 RFID tag.

- N: the number of the tags.
- T_{COMP}: the time for comparing operation.
- T_{XOR}: the time for executing an exclusive-or operation.
- T_H: the time for executing a hash function (160 bits).
- T_{RNG}: the time for executing a random number generation operation (16 bits).
- T_{ASYE}: the time for executing an asymmetric encryption operation (1024 bits).
- T_{ASYD}: the time for executing an asymmetric decryption operation (1024 bits).
- T_{SY}: the time for executing a symmetric encryption/decryption operation (256 bits).
- T_{CRC}: the time for executing a Cyclic Redundancy Check (CRC) function (16 bits).

4 Conclusions

The RFID ownership transfer system achieved the following capabilities:

1) Mutual authentication;

2) Guarantee of privacy;

3) Conformation to EPC Class-1 Generation-2 industry standards;

4) Prevention of any third party attack.

The mutual authentication of the proposed system ensures the safety between the tag and the reader. The proposed scheme can reduce the load of the database and successfully transfer the ownership to the new owner to assure the secure transaction and protect personal privacy as well.

Table 2: The comparisons of the time complexity

Schemes	Hong and Tianjie Scheme [5]	Osaka et al.s Scheme [11]	Seo et al.'s Scheme [13]	Our Scheme
Tag	$1T_H + 1T_{RNG}$ $+2T_{XOR}$	$1T_H + 2T_{XOR}$	$1T_{XOR}$	$1T_{COMP} + 3T_{XOR}+$ $3T_{PRNG} + 3T_{CRC}$
Reader	T_{PRNG}	T_{PRNG}	$1T_{ASYD} + 1T_{ASYE} + 1T_{COMP}$	$1T_{SYD} + 1T_{CRC} + 1T_H$
Server	$NT_H + 1T_{SY}+$ $1T_{XOR} + 1T_{COMP}$	$NT_H + 1T_{SY}+$ $1T_{XOR} + 1T_{COMP}$	$1T_{ASYD} + 1T_{ASYE}+$ $1T_{COMP}$	$1T_{COMP} + 3T_{XC}+$ $1T_{PRNG} + 3T_{CR} + 1T_{SYE}$

Acknowledgements

This work is partially supported by the National Science Council, Taiwan, under contract No. NSC 99-2628-E-324-026. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols," *International Journal of Network Security*, vol. 9, no. 1, pp. 95-100, July 2009.

[2] S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed Solutions," *IEEE Security & Privacy Magazine*, vol. 3, no. 3, pp. 34-43, 2005.

[3] S. Han, H. Lim, and J. Lee, "An efficient localization scheme for a differential-driving mobile robot based on RFID system,"*IEEE Transations on Industrial Electronics*, vol. 54, no. 6, pp. 3362-3369, 2007.

[4] A. D. Henrici and P. MÄuller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," *Proceedings of PerSec' 04*, pp. 149-153, Mar., 2004.

[5] L. Hong and C. Tianjie, "RFID protocol enabling ownership transfer to protect against traceability and DoS attacks," *IEEE First International Symposium on Data, Privacy and E-Commerce*, pp. 508-510, 2007.

[6] (http://www.epcglobalinc.org/)

[7] (http://www.epcglobalinc.org/standards/uhfc1g2)

[8] A. Juels, "Strengthening EPC tags against cloning," *Proceedings of the 4th ACM workshop on Wireless security*, pp. 67-76, 2005.

[9] K. H. S. S. Koralalage, M. R. Selim, J. Miura, Y. Goto, and J. Cheng, "An approach to enhance the security and privacy of RFID systems used in product lifecycle with an anonymous ownership transferring mechanism," *Proceedings of ACM Symposium on Applied Computing*, pp. 270-275, 2007.

[10] D. Molnar, A. Soppera, and D. Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags," *Selected Areas in Cryptography*, pp. 276-290, 2005.

[11] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An efficient and secure RFID security method with ownership transfer," *Proceedings of IEEE International Conference on Computational Intelligence and Security*, vol. 2, pp. 3-6, 2006.

[12] J. Saito, J. C. Ryou, and K. Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags," *Proceedings of EUC'2004*, LNCS 3207, pp. 879-890, 2004.

[13] Y. Seo, T. Asano, H. Lee, and K. Kim, "A lightweight protocol enabling ownership transfer and granular data access of RFID tags," *Proceeding of Symposium on Cryptography and Information Security Sasebo*, pp. 23-26, 2007.

[14] B. Toiruul and K. Lee, "An advanced mutual-authentication algorithm using AES for RFID systems," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 6, no. 9, pp. 156-162, 2006.

[15] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," *Proceedings of 1st International Conference on Security in Pervasive Computing (SPC)*, pp. 12-14, 2003.

[16] X. Zhang, and B. King, "Security requirements for RFID computing systems," *International Journal of Network Security*, vol. 6, no. 2, pp. 214V226, Mar. 2008.

Chin-Ling Chen was born in Taiwan in 1961. He received his B.S. degree in Computer Science and Engineering from the Feng Cha University in 1991; his M.S. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005 respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at the Chunghwa Telecom Co., Ltd. He is currently an associate professor of the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include: cryptography, network security, communication networks and electronic commerce.

Yeong-Lin Lai received the Ph.D. degree from the Institute of Electronics, National Chiao Tung University, Taiwan, R.O.C., in 1997. From 1985 to 1989, he was with the Electronic Systems Research Division, Chung-Shan Institute of Science and Technology, Taiwan, where he worked in the field of electronic system design and testing. From 1992 to 1993, he was a Senior Engineer at Macronix, Inc., Hsinchu, Taiwan, where he was engaged in VLSI design. From 1993 to 1997, he joined the research programs at Hexawave, Inc., Taiwan, where he was engaged in the development of microwave semiconductor devices and circuits. From 1998 to 2001, he was an Assistant Professor of the Department of Electronic Engineering, Feng Chia University, Taiwan. Since 2001, he has been with National Changhua University of Education, Taiwan. Dr. Lai is currently with the Department of Mechatronics Engineering and the Graduate Institute of Display Technology, National Changhua University of Education, as an Associate Professor. His research interests include mobile communication, RFID, RFIC, NEMS, and display technologies.

Chih-Cheng Chen is a Lecturer in Department of Industrial Engineering and Management in National Chin-Yi Institute of Technology. He teaches IE & M courses in Automatic Data Capture System. From 1996 to 2004, he was a senior engineer of Syntegra Tech. Company, which is an integration application software provider for the enterprise. He earned a Master Degree in Department of Mechatronics Engineering from National Changhua University of Education in 2005. Now, he is a Ph.D. candidate in Department of Mechatronics Engineering from National Changhua University of Education in Taiwan. He has been practicing the RFID application system in many fields such as the patrol system and the long-term care of elders. His research interests include mobile technology and RFID applications.

Yong-Yuan Deng was born in Taiwan in 1983. He received the B.S. degree in Department of Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan in 2006; and received the Master degree at the Institute of Information Engineering and Computer Science, Chaoyang University of Technology in 2010. He is currently pursuing his Ph.D. degree in the Department of Information Management. His research interests include cryptography and radio frequency identification system.

Yu-Cheng Huang was born in Taiwan in 1984. He received the B.S. degree in Department of Electronic Engineering from Kao-Yuan University, Kaohsiung, Taiwan in 2007; and received the Master degree at the Institute of Information Engineering and Computer Science, Chaoyang University of Technology in 2010. He is currently pursuing his Ph.D. degree at the Department of Computer Science and information Engineering at National Central University. His research interests include cryptography and radio frequency identification system.