Appl. Math. Inf. Sci. 6 No. 2S pp. 425S-431S (2012)

Applied Mathematics & Information Sciences
An International Journal

Two Ultralightweight Authentication Protocols for Low-Cost RFID Tags

Yung-Cheng Lee
Department of Security Technology and Management, WuFeng University, Chiayi 62153, Taiwan
Corresponding author: Email: yclee@wfu.edu.tw

Received June 1, 2011; Revised September 2, 2011; Accepted December 1, 2011
Published online: May 1, 2012

Abstract: The Radio Frequency Identification (RFID) system plays an important role in authentication, security control, supply chain management, and inventory control. Due to market consideration, low-cost RFID systems have become very popular in recent years. In many applications, such as e-passport, RFID systems need security mechanisms to resist all possible attacks and security risks. However, because of extensive computation requirements and high memory space demand for most security mechanisms, they are not suitable for low-cost RFID tags. In this paper, we propose two ultralightweight authentication protocols for low-cost RFID tags. The first protocol is based on dynamic identity and the second one on static identity. Both protocols have the merits of obtaining mutual authentication, protecting the user's privacy, and low computation cost. Furthermore, the proposed protocols can resist replay, impersonation, and de-synchronization attacks.

Keywords: Low-Cost RFID, RFID Authentication, RFID Tags, Network Security

1 Introduction

Radio Frequency Identification (RFID) systems have become very popular in recent years due to the well-developed technology and variety of potential applications. The RFID system is an important technology for authentication, security control, supply chain management, and inventory control. RFID systems are used for automatic object identification in microchip fabrication and automobile manufacturing among various other industries, and even in animals.

A typical RFID system consists of tags, readers, and a server with a database. Initially, the readers inquire tags by broadcasting radio frequency signals. The responding data from the tags can be read automatically with wireless at a rate of several hundred tags per second, from a range of several meters.

In many applications, such as authentication, the RFID systems need security mechanisms to resist all possible attacks and threats. However, most of the security mechanisms have extensive computation requirements or need large memory space, so they are not suitable for low-cost RFID tags.

Although authentication is an important requirement for many RFID applications, many RFID systems used today lack secure authentication mechanism. Some of the previous lightweight authentication schemes are vulnerable to various attacks [9,10]. Adversaries may inquire unprotected RFID tags to obtain information illegally, spoof tags to get secret information, or release denial of service attack. In some situations, privacy is also an important requirement to protect tag holders. However, most RFID systems also lack a privacy protection mechanism; so many RFID systems are vulnerable to security and privacy risks.

An RFID system usually consists of one server, many readers, and hundreds or thousands of tags. With regard to market share consideration, the cost of RFID tags plays an important role in system development. Based on the computational cost and the operations supported on the tags, the RFID

authentication protocols can be divided into four classes as follows [3]:

(1) The full-fledged class: The protocols such as an application on e-passport [10,11] that need the support of conventional cryptographic functions, one-way hash functions, or even public key cryptographic algorithms.
(2) The simple class: The protocols like the schemes [4,7,20,21] that install a pseudo random number generator or one-way hash function on tags.
(3) The lightweight class: The protocols [2,14] that require a pseudo random number generator and simple functions like Cyclic Redundancy Code (CRC) checksum.
(4) The ultralightweight class: The protocols [5,13,16,17] that only require simple bitwise operations, such as bitwise XOR, AND, and OR, in tags.

The first two classes above belong to high-cost RFIDs, and the other two classes are considered low-cost RFIDs. Due to market share consideration, the low-cost RFID tags are the best option. However, the low-cost RFID tags, with no more than 10K logic gates in which at most 3K can be used for security functions [3], usually cannot adopt a complex security algorithm in it. Thus it is essential to develop a simple algorithm with minimum memory for ultralightweight RFID tags.

In 2006, Peris-Lopez et al. [15-17] proposed a family of ultralightweight mutual authentication protocols. In their protocols, only simple bitwise operations like XOR, AND, OR, and modular addition were adopted in the tags. The computations of their schemes were very simple so they were suitable for low-cost tags. Unfortunately, their protocols suffered de-synchronization attacks, active attacks, and passive attacks [1,13]. Nevertheless, they were an interesting advance in the field of lightweight cryptography for low-cost RFID tags. In 2007, Chien [3] proposed a new ultralightweight protocol (SASI protocol). The protocol provided mutual authentication, tag anonymity, and forward security. It was designed to resist de-synchronization attacks, replay attacks, and man-in-the-middle attacks. However, Sun et al. [19] showed that Chien's protocol could not resist de-synchronization attacks.

In 2009, David et al. [6] proposed an ultralightweight mutual authentication protocol for low-cost RFID tags, but Hernandez-Castro et al. [8] showed that David et al.'s protocol was vulnerable to traceability attacks and full disclosure attacks. Lee et al. [12] also proposed an ultralightweight RFID authentication protocol in 2009; however, Peris-Lopez et al. [18] showed that the protocol was insecure.

In this paper, we propose two ultralighweight authentication protocols for low-cost RFID tags. The first protocol is based on dynamic identity and the second protocol is based on static identity. Both of the protocols have the merits of providing mutual authentication, and resisting various attacks such as traceability, replay attacks, de-synchronization attack, and impersonation attack. Most importantly, the computation cost of the protocols is quite low. The rest of this paper is organized as follows. In Section 2, we describe the preliminaries and notations. The two new proposed ultralighweight authentication protocols for low-cost RFID tags are described in Sections 3 and 4, respectively. Security analysis and performance evaluation are described in Section 5. Finally, we make conclusions in Section 6.

2 Preliminaries and Notations

Generally, the communications between the reader and the backend server are through secure channels, but the communications between the reader and the tag are susceptible to all possible attacks due to the open nature. Hereafter, for simplicity, both the server and the reader will be named as reader.

In the proposed protocols, the pseudo random number generator (PRNG) is only installed in the server, and the tags only perform simple bit-wise operations such as XOR ($\oplus$), OR ($\vee$), AND ($\wedge$), and left rotation $Rot(A,B)$. The notations used throughout this paper are as follows:

IDT : tag's static identity.
$DIDT_i$: tag's dynamic identity.
IDR : reader's static identity.
K_i : the secret key of the tag.
R_i : a random integer.
$\oplus$: bitwise XOR operation.
$\wedge$: bitwise AND operation.
$\vee$: bitwise OR operation.
$A \rightarrow B : M$: A sends M to B through a public channel.
$Rot(A, B)$: an $w(B)$-bit left rotation on A, where $w(B)$ denotes the Hamming weight of B.

3 An Ultralightweight RFID Protocol with Dynamic Identity

Let the tag and reader share the tag's dynamic identity and secret key. The dynamic identity and secret key are updated after each authentication session to resist traceability. To resist a possible de-synchronization attack, after the *i*-th authentication session, both the tag and the server share two pairs of information, $(DIDT_i, K_i)$ and $(DIDT_{i+1}, K_{i+1})$, in the memory. Where $(DIDT_i, K_i)$ is the dynamic identity and secret key used at the *i*-th authentication session, and $(DIDT_{i+1}, K_{i+1})$ is used for the potential next session. The server has a pseudo random number generator(PRNG).

The protocol consists of two main phases: (1) authentication phase and (2) key updating phase. In the authentication phase, the reader first inquires the tag, and then the reader and the tag authenticate each other. In the key updating phase, the reader and the tag update their dynamic identifications and secret keys, respectively.

For simplicity, the proposed ultralightweight RFID protocol with dynamic identity is named the DIDRFID protocol. The authentication and key updating procedures for the *i*-th session are described in the following sub-sections.

3.1 Authentication Phase

Step L-1. Tag → Reader: $DIDT_i$.

The tag transmits its dynamic identity $DIDT_i$ to the reader after receiving an inquire message from the reader.

Step L-2. Reader → Tag: (A_i, B_i).

After receiving $DIDT_i$, the reader finds the tag's corresponding secret key K_i from the database. Then the reader generates a random number R_i and computes (A_i, B_i) as follows:

$$A_i = K_i \oplus R_i,$$
$$B_i = Rot(K_i, K_i) \oplus Rot(R_i, R_i).$$

Then the reader sends (A_i, B_i) to the tag.

Step L-3. Tag → Reader: C_i.

Upon receiving (A_i, B_i), the tag obtains R_i' by

$$R_i' = A_i \oplus K_i.$$

Then the tag computes B_i' with K_i and R_i' by

$$B_i' = Rot(K_i, K_i) \oplus Rot(R_i', R_i').$$

The reader will be authenticated if $B_i' = B_i$. Next, the tag computes C_i as follows if the reader is authenticated:

$$C_i = Rot(K_i, R_i) \oplus Rot(R_i, K_i).$$

Finally, the tag forwards C_i to the reader.

Step L-4. Reader authenticates tag.

Upon receiving C_i from the tag, the reader computes C_i' by

$$C_i' = Rot(K_i, R_i) \oplus Rot(R_i, K_i).$$

The tag will be authenticated if $C_i' = C_i$. If $C_i' = C_i$, the reader and the tag obtain mutual authentication.

3.2 Key updating phase

After mutual authentication is obtained, the reader and the tag compute a new dynamic identity $DIDT_{i+1}$ and secret key K_{i+1} for the next session by

$$DIDT_{i+1} = Rot(R_i, R_i \vee K_i) \oplus Rot(K_i, R_i \wedge K_i).$$
$$K_{i+1} = Rot(R_i, R_i \wedge K_i) \oplus Rot(K_i, R_i \vee K_i).$$

Then both the reader and the tag store $(DIDT_i, K_i)$ and $(DIDT_{i+1}, K_{i+1})$ in the memory. For an illustration, the DIDRFID protocol is shown in Fig.1.

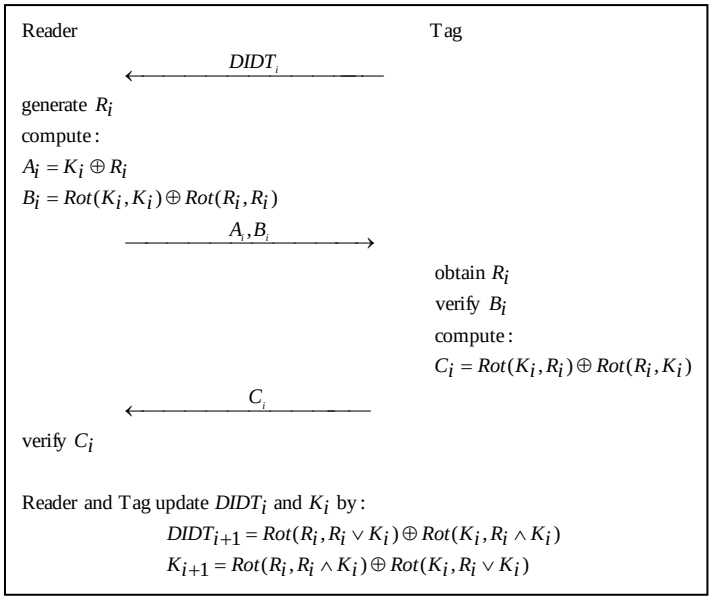

Figure 1: An ultralightweight RFID protocol with dynamic identity

4 An Ultralightweight RFID Protocol with Static Identity

In this section, we propose an ultralightweight RFID protocol with static identity (SIDRFID protocol for short). Suppose that the tag's and the reader's secret identities are *IDT* and *IDR*, respectively. *IDT* and *IDR* are installed in the tag's and the reader's memories. The server has a PRNG. At the *i*-th session, the authentication procedure of the SIDRFID protocol is described as follows:

Step S-1. Reader → Tag: S_i.

The reader first generates a random integer R_i and computes S_i by $S_i = R_i \oplus IDR$.

The reader sends S along with a request message to the tag.

Step S-2. Tag → Reader: (P_i, Q_i).

After receiving S_i, the tag obtains R_i by $R_i = S_i \oplus IDR$.

Then the tag sends P_i and Q_i to the reader, where

$P_i = IDT \oplus Rot(R_i, IDR)$,

$Q_i = Rot(IDT, IDT) \oplus Rot(R_i, R_i)$.

Step S-3. Reader → Tag: Z_i.

Upon receiving $\{P_i, Q_i\}$, the reader obtains IDT' by $IDT' = P_i \oplus Rot(R_i, IDR)$.

Then the reader computes Q_i' by

$Q_i' = Rot(IDT', IDT') \oplus Rot(R_i, R_i)$.

Next, the reader authenticates the tag by checking whether $Q_i = Q_i'$. After the tag is authenticated, the reader computes Z_i by

$Z_i = Rot(IDT, IDR \oplus R_i) \oplus Rot(IDR, IDT \oplus R_i)$.

Finally, the reader sends Z_i to the tag.

Step S-4. Reader authenticates tag.

Upon receiving Z_i, the tag computes Z_i' by

$Z_i' = Rot(IDT, IDR \oplus R_i) \oplus Rot(IDR, IDT \oplus R_i)$.

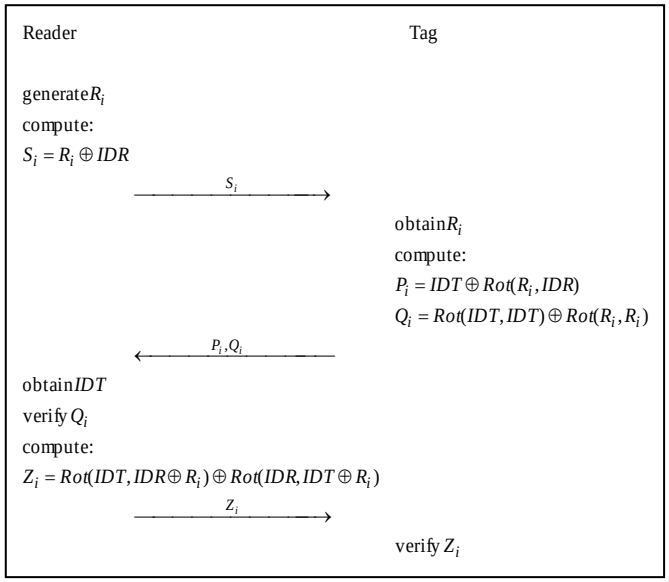

Figure 2: An ultralightweight RFID protocol with static identity

The tag will be authenticated if $Z_i' = Z_i$. Hereafter, the reader and the tag obtain mutual authentication. The proposed ultralightweight RFID protocol with static identity is illustrated in Fig. 2.

5 Security Analysis and Performance Evaluation

5.1 Security Analysis

In addition to the computation cost is quite low; the proposed protocols have the merits of protecting user's privacy, obtaining mutual authentication, and resisting several attacks. The advantages of the proposed two protocols are as follows:

(1) Protect user's privacy.

For some RFID system applications, the capability of resisting traceability is an important requirement. For example, in e-passport systems or for some VIPs, the users cannot withstand their whereabouts exposed. In general, the dynamic identity property will protect the authentication schemes from ID-theft attack. It is difficult for an adversary to trace the user if the forward message is really dynamic. Since the dynamic identity $DIDT_i$ is adopted in the DIDRFID protocol, the protocol can resist traceability. Moreover, the current $DIDT_i$ is irrelevant to any of the previous dynamic identities.

In the SIDRFID protocol, though the identity of the tag is static, but the static identity has not been transmitted and all forward messages contain a pseudonym which is changed for each session. The request and the response messages are different in each session even though the tag is the same. The forward messages are not fixed, so an adversary cannot identify or trace the tag. Thus the proposed protocols protect user's privacy and the anonymity merit of the tag is maintained.

(2) Obtain mutual authentication.

For many RFID systems, the mutual authentication feature is not required. However, in many applications, such as e-bank payments, mutual authentication is a basic requirement of RFID systems. In the DIDRFID protocol, the tag can authenticate the reader by verifying B_i and the tag is authenticated if C_i is verified. Similarly, in the SIDRFID protocol, the reader and the tag can authenticate each other by checking Q_i and Z_i, so our protocols obtain mutual authentication.

(3) Low computation cost.

The computation costs of cryptographic algorithms and hash functions are very high. Furthermore, it needs large memory space to install these algorithms and functions, so the cryptographic algorithms and hash functions are not suitable for the low-cost RFID tags. In the proposed protocols, the computations are based on simple bitwise XOR, AND, OR and rotation operations, and the computation cost is quite low.

(4) Forward secrecy.

The forward secrecy feature prevents adversaries from obtaining previous secrets even if the tag is compromised. In the DIDRFID protocol, even if the current dynamic identity $DIDT_i$ and secret information K_i are compromised, the adversary still cannot find the previous identity and secret information because the random number is unknown. Thus, the protocol obtains forward secrecy which can greatly reduce the damages that result from revealing secret information.

The proposed protocols can also resist several attacks. The security of the protocols is analyzed as follows:

(1) Resist impersonation attack.

In the DIDRFID protocol, if an adversary wants to masquerade as a legal reader to deceive the tag, the attack will fail because the adversary cannot find A_i and B_i consistently for authentication. Similarly, if an adversary wants to masquerade as a tag to deceive the reader, the attack will also fail because the adversary cannot forge C_i for verification successfully. In the SIDRFID protocol, an adversary cannot successfully masquerade as a legal entity since he/she cannot forge consistent P_i, Q_i and Z_i to pass the authentication. Because of this, the protocols can resist impersonation attacks.

(2) Resist de-synchronization attack.

In the DIDRFID protocol, both the reader and the tag keep two sets of information, $(DIDT_i, K_i)$ and $(DIDT_{i+1}, K_{i+1})$, in the memories after the *i*-th session of authentication. Note that the former pair is used for authentication on the *i*-th session and the latter pair is used for the next session. If the reader and the tag cannot obtain mutual authentication with the candidate information $(DIDT_{i+1}, K_{i+1})$ at the *i*+1-th session, they can still use $(DIDT_i, K_i)$ for a successful authentication, so, the proposed protocol can withstand de-synchronization attacks.

(3) Resist replay attack.

In the DIDRFID protocol, before the *i*-th authentication session, the information stored in both the tag and the reader are $(DIDT_{i-1}, K_{i-1})$ and $(DIDT_i, K_i)$. On the *i*-th session, the information transmitted between the tag and the reader is A_i, B_i, and C_i. After mutual authentication is obtained, the information stored in both the tag and the reader is $(DIDT_i, K_i)$ and $(DIDT_{i+1}, K_{i+1})$. We explain why the DIDRFID protocol can resist the replay attack by using the following two cases: (a) On the (*i*+1)-th session of authentication, suppose that an adversary replays the previous intercepted message A_i and B_i to the tag; though the tag cannot authenticate the reader by using candidate secrets $(DIDT_{i+1}, K_{i+1})$, the tag still can authenticate the reader by using $(DIDT_i, K_i)$. That is, the replay message will pass the verification eventually. However, because the reader's pseudonym is R_{i+1}, while the recovered pseudonym is R_i in the tag, the tag cannot compute a consistent C_{i+1} for a successful authentication. The adversary also cannot obtain a consistent C_{i+1} for verification since he/she does not know the secret information and pseudonym. Thus the reader will detect the attack. (b) If the adversary replays the previous message C_i at the *i*+1-th session of authentication, the attack will fail since the pseudonyms in the reader's and the tag's memories are different. In the SIDRFID protocol, if an adversary resends an old S_i for a new authentication, this attack will not work since the verification of Q_i will fail. Similarly, if the adversary sends an old Z_i to the tag, the replay attack still will not work since it cannot pass the verification. Thus, our protocols can withstand replay attacks.

5.2 Performance Evaluation

In our DIDRFID and SIDRFID protocols, the systems only require simple bitwise XOR, AND, OR, and rotation operations. The computation costs of the proposed protocols are quite low, and thus they can be effectively implemented on ultralightweight RFID tags. Some lightweight RFID systems [3,16] need modular addition operations besides XOR, AND, OR, and rotation operations. However, the modular addition operation is not sufficiently quick to address its carry propagation problem.

The pseudo random number generator is not a simple or computation effective algorithm for RFID tags. Furthermore, hackers can easily attack a system if its pseudo random number generator is not properly designed. Due to its limitation on memory and computation, it is not easy for ultralightweight RFID tags to install a PRNG. In our protocols, instead of tags, only the server needs to implement a PRNG. Therefore, the proposed protocols are practical in implementation.

In the DIDRFID protocol, each tag needs one static and two pairs of dynamic identity and secret information. Thus, if each identity or secret information is 16 bytes in length, only 80 bytes of memory is required, which is fewer than other schemes [3,16,17]. In the SIDRFID protocol, each tag only stores the tag's and the reader's static identities. A simple comparison of ultralightweight authentication protocols is listed in Table 1.

Table1. Comparison of Ultralightweight Authentication Protocols

Protocols	LMAP[16]	EMAP[17]	SASI[3]	DIDRFID	SIDRFID
Protect user privacy	×	×	✓	✓	✓
Mutual authentication	×	×	✓	✓	✓
Forward secrecy	×	×	✓	✓	✓
Resist desynchronization attack	×	×	✓	✓	✓
Secret information stored in each tag*	6L	6L	7L	5L†	2L#
Operations in the tag	∧,∨,⊕,+	∧,∨,⊕	∧,∨,⊕,+, Rotation	∧,∨,⊕, Rotation	∧,∨,⊕, Rotation

Note: *: L denotes the bit length of identity or secret information.
†: Each tag stores IDT, $(DIDT_i, K_i)$ and $(DIDT_{i+1}, K_{i+1})$.
#: Each tag stores IDT and IDR.

6 Conclusions

The Radio Frequency Identification (RFID) system plays an important role in authentication, security control, supply chain management, and inventory control. Low-cost RFID systems have become very popular in recent years. In many applications, such as e-passport, the RFID systems need security mechanisms to resist all possible attacks and threats. However, because of extensive computation requirements and memory limitations for most security mechanisms, they are not suitable for low-cost RFID tags.

In this paper, we proposed two ultralightweight authentication protocols for low-cost RFID tags. Both protocols have the merits of obtaining mutual authentication, protecting the user's privacy, and low computation costs. Furthermore, the proposed protocols can resist replay, impersonation, and de-synchronization attacks. In addition, these protocols are very practical since they can be implemented in the low-cost tags easily.

Acknowledgements

This research is partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC 99-2622-E-274-001-CC3. The author also gratefully acknowledges the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] M. Bárász, B. Boros, P. Ligeti, K. Lója and D.A. Nagy, Breaking LMAP, International Conference on RFID Security 2007, Malaga, Spain (2007).

[2] J. Bringer, H. Chabanne and E. Dottax, HB++: A Lightweight Authentication Protocol Secure against Some Attacks. International workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing–SerPerU'06, (2006), 28−33.

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

[4] H.Y. Chien, Secure Access Control Schemes for RFID Systems with Anonymity. Proceedings of the 7th International Conference on Mobile Data Management, (2006), 96-96.

[5] H.Y. Chien and C.W. Huang, Security of Ultra-Lightweight RFID Authentication Protocols and Its

Improvements. ACM Operating System Review, Vol.41, No.2, (2007), 83-86.

[6] M. David and N.R. Prasad, Providing Strong Security and High Privacy in Low-Cost RFID Networks. Procedings of Security and Privacy in Mobile Information and Communication Systems, Springer Berlin Heidelberg, (2009), pp.172-179.

[7] T. Dimitriou, A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM, (2005), 59-66.

[8] J.C. Hernández Castro, P. Peris-Lopez, R.C.W. Phan, J.M. Estévez-Tapiador, Cryptanalysis of the David-Prasad RFID Ultralightweight Authentication Protocol. Procedings of the 6th International Workshop on Radio Frequency Identification: Security and Privacy Issues, (2010), 22-34.

[9] A. Juels, RFID Security and Privacy: A Research Survey. The IEEE Journal on the Selected Areas in Communications, Vol.24, Is.2, (2006), 381-394.

[10] A. Juels, D. Molner and D. Wagner, Security and Privacy Issues in EPassports. Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm'05, (2005), 74-88.

[11] S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri and A. Kanai, Privacy Enhanced Active RFID Tag. Proceedings of the First International Workshop on Exploiting Context Histories in Smart Environments, (2005).

[12] Y.C. Lee, Y.C. Hsieh, P.S. You and T.C. Chen, A New Ultralightweight RFID Protocol with Mutual Authentication. Proceedings of The 2009 WASE International Conference on Information Engineering, (2009), Vol.2, 58-61.

[13] T. Li and G. Wang, Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. Proceedings of the 22nd IFIP TC-11 International Information Security Conference, (2007).

[14] J. Munilla and A. Peinado, HB-MP: A Further Step in the HB-Family of Lightweight Authentication Protocols. Computer Networks, Vol.51, No.9, (2007), 2262-2267.

[15] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, M^2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags. Procedings of UIC'06, LNCS 4159, (2006), 912-923.

[16] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags. Proceedings of the Second Workshop RFID Security, (2006).

[17] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags. Proceedings of the OTM Federated Conference and Workshop: IS Workshop, (2006), 352-361.

[18] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estévez-Tapiador, E.S. Millán and J.C.A. van der Lubbe, Security Flaws in an Efficient Pseudo-Random Number Generator for Low-Power Environments. Proceedings of the First International ICST Workshop on Security in Emerging Wireless Communications and Networking Systems, SEWCN 2009, (2009), 25-35.

[19] H.M. Sun, W.C. Ting and K.H. Wang, On the Security of Chien's Ultralightweight RFID Authentication. IEEE Transactions on Dependable and Secure Computing, Vol.8, Is.2, (2011), 315-319.

[20] S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels, Proceedings of the First International Conference on Security in Pervasive Computing (SPC), LNCS 2802, (2003), 201-212.

[21] J. Yang, J. Park, H. Lee, K. Ren and K. Kim, Mutual Authentication Protocol for Low-Cost RFID, Ecrypt Workshop on RFID and Lightweight Crypto, (2005).

Yung-Cheng Lee received the Ph.D. degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 1999. He was the Chairman of the Department of Electrical Engineering and Department of Computer Science and Information Engineering, National Formosa University; the Dean of Security and Engineering School, WuFeng University. Currently, he is the Dean of Academic Affair, WuFeng University, Taiwan. His research interests include network security, artificial intelligence and cryptography.