Short Papers

SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity

Hung-Yu Chien

Abstract—As low-cost RFIDs become more and more popular, it is imperative to design ultralightweight RFID authentication protocols to resist all possible attacks and threats. However, all of the previous ultralightweight authentication schemes are vulnerable to various attacks. In this paper, we propose a new ultralightweight RFID authentication protocol that provides strong authentication and strong integrity protection of its transmission and of updated data. The protocol requires only simple bit-wise operations on the tag and can resist all the possible attacks. These features make it very attractive to low-cost RFIDs and very low-cost RFIDs.

Index Terms—Security, privacy, authentication, RFID, synchronization.

1 Introduction

Due to the low cost and the convenience in identifying an object without physical contact, Radio Frequency Identification (RFID) systems have become more and more popular. But, their wide deployment also incurs many security concerns and practical attacks [2], [12], [13], [28]. Corporate espionage may *inquire* unprotected RFIDs 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 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. So, the security requirements for RFID systems include content privacy, access control, authentication, anonymity, and data recovery. Authentication is required for a tag and a reader to authenticate each other. After authentication, only authenticated readers can access the contents of tags. With anonymity, the attacker cannot identify tags or track specific tags from the communications. With data recovery, readers and tags can withstand the possible DOS attacks.

To have large market penetration, the cost of RFID tag plays an important factor. For a low-cost RFID tag, there are about 5K-10K logic gates, and only 250-3K can be used for security functions. Based on the computational cost and the operations supported on tags, we roughly classify the RFID authentication protocols into four classes. The first class called "*full-fledged* class" refers to those protocols (like the schemes [13], [16], [17]) that demand the support of conventional cryptographic functions like symmetric encryption, cryptographic one-way function, or even the public key algorithms. The second class called "*simple*" is for those protocols (like the schemes [4], [10], [20], [22], [27], [28], [29], [30], [31]) that should support random number generator and one-way hashing function on tags. The third class called "*lightweight*" protocols refers to those protocols [3], [5], [7], [9], [11], [12], [14], [15], [21], [26] that require a random number generator and simple functions like Cyclic Redundancy Code (CRC) checksum but not hash function. The fourth class called "*ultralightweight*" refers to the protocols [6], [18], [19], [23], [24], [25] that only involve simple bit-wise operations (like XOR, AND, OR, etc.) on tags. In this paper, we aim to design a new ultralightweight RFID authentication protocol for low-cost RFIDs and even very low-cost RFIDs, because the resources on these tags are very limited. And, the protocol should withstand all the possible attacks. We name the protocol *SASI* to highlight its *S*trong *A*uthentication and *S*trong *I*ntegrity protection on the transmission data and on the synchronization values. This property makes it much more robust than its counterparts [18], [19], [23], [24], [25].

The rest of this paper is organized as follows: Section 2 discusses related works. Section 3 introduces our new protocol, which is followed by the security and performance evaluation in Section 4. Finally, Section 5 states our conclusions.

2 Related Works

The protocols [13], [16], [17] belonging to the *full-fledged* class support cryptographic functions like hashing, encryption, and even public key algorithms on tags. One of the main applications of these full-fledged protocols is E-passport [13].

The tags in the protocols of the *simple* class should support random number function and hash functions but not encryption functions/public key algorithms. Examples are like [4], [10], [20], [22], [27], [28], [29], [30], [31], where Chien [4] had reported the secret key disclosure problem and the violation of anonymity in Weis [28] and Weis et al. [29], Avoine et al. [1] had reported the weakness of Ohkubo et al.'s scheme [22], and the weaknesses of the schemes [10], [20], [27], [30], [31] have been reported.

The *lightweight* RFID authentication protocols do not require hashing function on tags; for example, the EPCglobal Class-1 Gen-2 RFID tag [8] supports Pseudo-Random Number Generator (PRNG) and Cyclic Redundancy Code (CRC) checksum but not hashing function. The protocols [7], [12], [15] belong to this class, where the scheme [12] did not take the eavesdropping and privacy issues into consideration, and Chien and Chen [5] had reported the DOS attack, replay attack, tracking attack and spoofing tag problem on the schemes [7], [15], respectively. The HB-series [3], [9], [11], [14], [21], [26] can also be classified into this class, since they demand the support of random number function but not hash function on tags. Hopper and Blum [11], based on the LPN problem, first proposed the HB protocol to defect the passive attacker. Later, the HB protocol was successively attacked and improved by its sister works [3], [9], [14], [21], [26]. Actually, the HB-series cannot be regarded as *complete*, since these protocols only consider the authentication of tags. They neglected the issue of the authentication of the readers, the tracking problem, and the anonymity issue, and even the privacy of the tag identification.

Recently, Peris-Lopez et al. proposed a series of *ultralightweight* authentication protocols [23], [24], [25], where the tags involve only simple bit-wise operations like XOR, AND, OR, and addition mod 2^m. These schemes are very efficient, and they only require about 300 gates. Unfortunately, Li and Wang [19] and Li and Deng [18], respectively, reported the de-synchronization attack and the full-disclosure attack on these protocols, and Chien and Hwang [6] further pointed out the weakness of Li-Wang's improved scheme. We find that the previous schemes [18], [19], [23], [24], [25] only provided weak authentication and weak integrity protection, which make them vulnerable to various attacks. This paper aims to propose a new ultralightweight RFID authentication protocol for low-cost RFIDs and very low-cost RFIDs, and the scheme should withstand all the possible attacks.

- *The author is with the Department of Information Management, National Chi Nan University, University Road Puli, Nantou Hsien, Taiwan 545 Republic of China. E-mail: hychien@ncnu.edu.tw.*

Manuscript received 10 Mar. 2007; accepted 7 Aug. 2007; published online 31 Aug. 2007.
For information on obtaining reprints of this article, please send e-mail to: tdsc@computer.org, and reference IEEECS Log Number TDSC-2007-03-0032.
Digital Object Identifier no. 10.1109/TDSC.2007.70226.

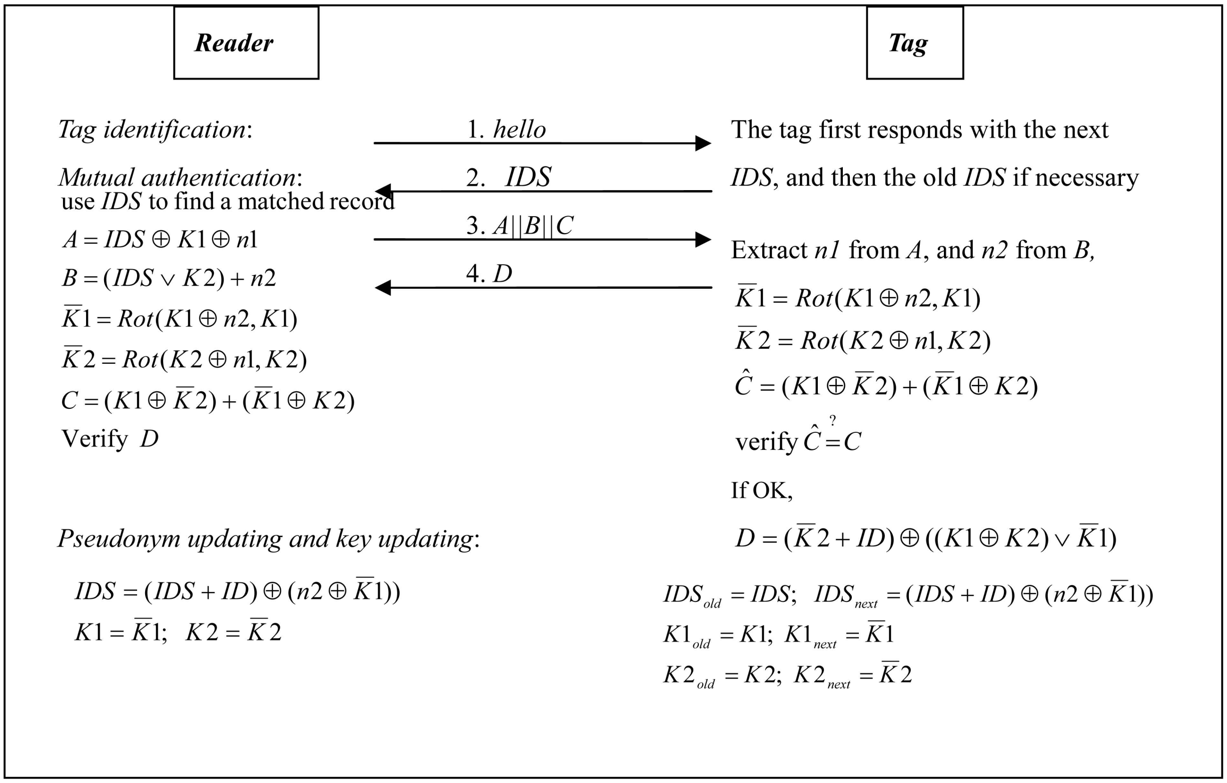
Reader
Tag
Tag identification:
1. hello
The tag first responds with the next IDS, and then the old IDS if necessary
Mutual authentication:
2. IDS
use IDS to find a matched record
$A = IDS \oplus K1 \oplus n1$
3. $A||B||C$
$B = (IDS \vee K2) + n2$
4. D
Extract n1 from A, and n2 from B,
$\overline{K}1 = Rot(K1 \oplus n2, K1)$
$\overline{K}2 = Rot(K2 \oplus n1, K2)$
$C = (K1 \oplus \overline{K}2) + (\overline{K}1 \oplus K2)$
$\hat{C} = (K1 \oplus \overline{K}2) + (\overline{K}1 \oplus K2)$
Verify D
verify $\hat{C} \overset{?}{=} C$
If OK,
Pseudonym updating and key updating:
$D = (\overline{K}2 + ID) \oplus ((K1 \oplus K2) \vee \overline{K}1)$
$IDS = (IDS + ID) \oplus (n2 \oplus \overline{K}1))$
$K1 = \overline{K}1;\ K2 = \overline{K}2$
$IDS_{old} = IDS;\ IDS_{next} = (IDS + ID) \oplus (n2 \oplus \overline{K}1))$
$K1_{old} = K1;\ K1_{next} = \overline{K}1$
$K2_{old} = K2;\ K2_{next} = \overline{K}2$

Fig. 1. SASI protocol.

3 SASI: New Ultralightweight Authentication Protocol

The protocol involves three entities: tag, reader, and backend server. The channel between the reader and the backend server is assumed to be secure, but that between the reader and the tag is susceptible to all the possible attacks. Each tag has a static identification (ID), and preshares a pseudonym (IDS) and two keys $K1/K2$ with the backend server. The length of each of $ID/IDS/K1/K2$ is 96 bits. To resist the possible de-synchronization attack, each tag actually keeps two entries of $(IDS, K1, K2)$: one is for the *old* values and the other is for the *potential next* values. This arrangement will become obvious when we introduce the protocol and analyze the possible attacks. The protocol consist of three stages: tag identification phase, mutual authentication phase, and pseudonym updating and key updating phase. In each protocol instance, the reader may probe the tag twice or once in the tag identification phase, depending on the tag's IDS is found or not. The reader first sends "*hello*" message to the tag, and the tag will respond with its *potential* next IDS. The reader uses the tag's response IDS to find a matched entry in the database, and goes to the mutual authentication phase if a matched entry is found; otherwise, it probes again and the tag responds with its old IDS. In the mutual authentication phase, the reader and the tag authenticate each other, and they, respectively, update their local pseudonym and the keys after successful authentication. After successful authentication, the tag stores the matched values to the entry $(IDS_{old} \parallel K1_{old} \parallel K2_{old})$ and stores the updated values to the entry $(IDS_{next} \parallel K1_{next} \parallel K2_{next})$. The random number generator is required on the reader only, and the tags only involve simple bitwise operations like bitwise XOR ($\oplus$), bitwise OR ($\vee$), bitwise AND ($\wedge$), addition mod 2^m (+), and left rotate ($Rot(x, y)$). $Rot(x, y)$ is defined to left rotate the value of x with y bits. The protocol procedures are described as follows:

Tag identification. Initially, the reader sends "*hello*" to the tag, which first responds with its potential next. If the reader could find a matched entry in the database, it steps into the mutual authentication phase; otherwise, it probes again and the tag responds with its old IDS.

Mutual authentication phase. The reader uses IDS to find a matched record in the database. It could be the potential next IDS or the old IDS of the tag. It then uses the matched values and two generated random integers $n1$ and $n2$ to compute the values A, B, and C (the calculation equations are specified in Fig. 1). From $A \parallel B \parallel C$, the tag first extracts $n1$ from A, extracts $n2$ from B, computes $\overline{K}1$ and $\overline{K}2$ and then verifies the value of C. If the verification succeeds, then it computes the response value D. Upon receiving D, the reader uses its local values to verify D.

Pseudonym updating and key updating. After the reader and the tag authenticated each other, they update their local pseudonym and keys as specified in Fig. 1.

Please notice that our scheme also provides confirmation of the synchronization values $(\overline{K}1, \overline{K}2)$ when the reader and the tag successfully authenticate each other. This property makes it robust to the possible de-synchronization attacks.

4 Security and Performance Evaluation

4.1 Security Analysis

It is obvious, from the protocol specification, that the tag and the reader can successfully authenticate each other, if only passive attacker is considered. We now analyze the security of the proposed protocol by examining the required properties and the possible attacks as follows:

1. **Mutual authentication and data integrity**. The tag and the reader can authenticate each other, because only the genuine reader who has the keys $K1$ and $K2$ can generate the consistent values $A \parallel B \parallel C$, and only the genuine tag who has the secret keys can derive the random numbers $n1$ and $n2$, and then to generate the response D. What makes our protocol quite different from its counterparts [18], [19], [23], [24], [25] is that our protocol can ensure both the authenticity and the integrity of the messages while its counterparts cannot ensure the authenticity and integrity. In our protocol, the calculations of the data C/D involve the current secret keys, the two random numbers and the

TABLE 1
A Simple Comparison of Ultralightweight Authentication Protocols

	LMAP	M^{2}AP	EMAP	SASI
Resistance to de-synchronization attacks	No	No	No	Yes
Resistance to disclosure attacks	No	No	No	Yes
Privacy & anonymity	No	No	No	Yes
Mutual authentication & forward secrecy	No	No	No	Yes
Total messages for mutual authentications	$4L$*	$5L$	$5L$	$4L$
Memory size on tag	$6L$	$6L$	$6L$	$7L$
Memory size for each tag on server	$6L$	$6L$	$6L$	$4L$
Operation types on tag	$\oplus,\wedge,\vee,+$	$\oplus,\wedge,\vee,+$	$\oplus,\wedge,\vee$	$\oplus,\wedge,\vee,+,Rot$

** L denotes the bit length of one pseudonym or one key.*

potential next keys. So, only the genuine reader and the genuine tag have the ability to generate the values.

2. **Tag anonymity and resistance to tracking**. The pseudonym of each tag is updated per successful authentication, and the update operation involves random numbers. So, the successive pseudonyms from the same tag look random, and the attacker cannot identify the identity of the tag and cannot track the tag. Of course, if the attacker successively probes the same tag many times between two successful authentications, then the tag will respond the same pseudonyms (the old pseudonym and the potential next pseudonym from the same tag). This situation lets the attacker track the same tag; however, this scenario does not have any practical value.
3. **Data confidentiality**. The calculation of each value of A, B, C, and D involves at least two secret values (including the keys and the random numbers); so, the static identification and the secret values are well protected from the eavesdroppers.
4. **Forward security**. The forward security property means to protect the past communications from a tag even assuming the tag be compromised some day. In our scheme, if we assume an attacker compromises a tag and acquires the two entries of (ID, IDS, $K1$, and $K2$) some day, the attacker still cannot infer the previous secret data and keys of the same tag, because each of the updating equations and the calculations of $A \parallel B \parallel\parallel D$ involve at least two random values. So, the attacker cannot compromise the past communications from the same tag.
5. **Explicit key confirmation and resistance to de-synchronization attack**. The previous RFID authentication schemes that require synchronization of shared data are vulnerable to the denial-of-service attack, because the attacker can easily modify the data to make the reader and the tag out of synchronization without being noticed. But, in our scheme, the authenticity and the integrity of random values ($n1/n2$) are ensured and the potential next keys ($\overline{K}1/\overline{K}2$) are explicitly confirmed, because the calculations of C and D explicitly involve these values. So, the attacker cannot change the data without being noticed. Of course, the attacker can intercept the data D sent by the tag to make the tag updates its local data while the reader does not. Fortunately, this cannot cause trouble to our scheme, because the tag keeps two entries of secret data (one is for the potential next values and the other is the old values), and can still authenticate with the reader using the old value for this situation.

   There are two possible approaches to de-synchronize the shared values between tags and readers: one is intercepting the response D from tag, and the other is to make the reader and the tag use different $n1$ and $n2$ to update their local data. The first approach will make the tag update its local data but the reader does not. However, since the tag keeps two entries of its local data (one for the old values and the other is the potential next values), the reader and the tag can still authenticate each other for such a situation, using the old values. The second approach does not work on our scheme, because it is infeasible for the attacker to change the transmission without being noticed.
6. **Resistance to replay attack**. The attacker may replay the response D from a tag. However, the reader will find the invalidity of the replay value, because the challenge random numbers $n1$ and $n2$ from the reader are different and independent each session. Another replay scenario is: an attacker may intercept the data D in one session, and then replay an old message $A \parallel B \parallel C$ (corresponding to an old *IDS*) from the reader. But, this scenario will not change any internal state of the tag, and the attacker gains no secret information of the tag. So, the attacker does not gain any secret information nor de-synchronize the reader and the tag.
7. **Resistance to man-in-the-middle attack**. The man-in-the-middle attack does not work on our scheme, because our scheme provides strong integrity and strong authentication on the data $A \parallel B \parallel C$ and D. Any modification on the

values A or B will cause, from the attacker's point of view, unpredictable changes on the values C and D, which makes the attacker hard to change the data without being noticed.

8. **Resistance to disclosure attack**. The key idea behind the disclosure attacks [6], [18], [19] on the previous ultralightweight protocols is that an attacker can slightly modify the challenge from the reader and then infer partial information from the response from the tag. However, the attack does not work on our scheme, because any slight modification on the transmission will be detected in our scheme.

4.2 Performance Evaluation

This section evaluates the performance of our proposed scheme in terms of computational cost, communication cost, storage requirement, and security. We first examine the storage requirement of the tag of our scheme. For each tag, it owns one static ID, and two entries for $(IDS, K1, K2)$. So, a ROM memory is required to store the 96-bit static identification, and 576-bit rewritable memory is required for storing the updatable keys and the pseudonym.

Regarding the computational cost, the tag involves only simple bit-wise operations: $\oplus$, AND, OR, +, and left rotate. These operations are very low-cost and can be effectively implemented on low-cost RFIDs and very low-cost RFIDs. Regarding the communication cost, we only need to count the messages in the mutual authentication phase, since this phase contributes most of the communication cost. In this phase, the tag and the reader transmit $A \parallel B \parallel C$ and D, which in total demand 384 bits. From the above analysis, we can see that our proposed scheme is very efficient and very low cost.

Our proposed scheme also owns the strongest security performance among the ultralightweight authentication protocols [18], [19], [23], [24], [25] (LMAP, M^{2}AP, EMAP, and our scheme). The previous schemes have been reported to be vulnerable to the de-synchronization attacks and the full-disclosure attacks, where the de-synchronize attack make the reader and the tag out-of-synchronization, and the full disclosure attack can compromise all the secret information of the tags. So, the previous schemes fail to commit the properties: mutual authentication, privacy, forward secrecy, and data recovery. But, due to its strong authentication, strong integrity, and synchronization confirmation, our scheme can withstand all of the possible attacks listed in Section 4.1. A simple comparison of ultralightweight authentication protocols is listed in Table 1.

5 Conclusion

In this paper, we have proposed a new ultralightweight authentication protocol. The new scheme provides strong authentication and strong integrity of the transmissions and of the updated data, and can withstand all the possible attacks that break the security of the previous schemes. The tag requires only simple bit-wise operations. These excellent features make it very attractive to low-cost RFIDs and very low-cost RFIDs.

Acknowledgments

This research is partially supported by the National Science Council, Taiwan, R.O.C., under contract no NSC 95-2221-E-260-050-MY2.

References

[1] G. Avoine, E. Dysli, and P. Oechslin, "Reducing Time Complexity in RFID Systems," *Proc. 12th Ann. Workshop Selected Areas in Cryptography (SAC),* 2005.

[2] S.C. Bono, M. Green, A. Stubblefield, A. Juels, A.D. Rubin, M. Szydlo, "Security Analysis of a Cryptographically-Enabled RFID Device," *Proc. 14th USENIX Security Symp.,* pp. 1-16, 2005.

[3] J. Bringer, H. Chabanne, and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attacks," *Proc. IEEE Int'l Conf. Pervasive Service, Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing,* 2006.

[4] H.-Y. Chien, "Secure Access Control Schemes for RFID Systems with Anonymity," *Proc. 2006 Int'l Workshop Future Mobile and Ubiquitous Information Technologies (FMUIT '06),* 2006.

[5] H.-Y. Chien and C.-H. Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards," *Computers Standards & Interfaces,* vol. 29, no. 2, pp 254-259, 2007.

[6] H.-Y. Chien and C.-W. Huang, "Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements," *ACM Operating System Rev.,* vol. 41, no. 2, pp. 83-86, July 2007.

[7] D.N. Duc, J. Park, H. Lee, and K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning," *Proc. 2006 Symp. Cryptography and Information Security,* 2006.

[8] EPCglobal, http://www.epcglobalinc.org/, 2007.

[9] H. Gilbert, M. Robshaw, and H. Sibert, "An Active Attack against HB+-A Provably Secure Lightweight Authentication Protocol," *Cryptology ePrint Archive,* Report 2005/237, 2005.

[10] A.D. Henrici and P. Mäuller, "Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers," *Proc. Second IEEE Ann. Conf. Pervasive Computing and Comm. Workshops,* pp. 149-153 2004.

[11] N.J. Hopper and M. Blum, "Secure Human Identification Protocols," *Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security,* pp. 52-66, 2001.

[12] A. Juels, "Strengthening EPC Tag against Cloning," *Proc. ACM Workshop Wireless Security (WiSe '05),* pp. 67-76, 2005.

[13] A. Juels, D. Molner, and D. Wagner, "Security and Privacy Issues in E-Passports," *Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05),* 2005.

[14] A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," *Proc. 25th Ann. Int'l Cryptology Conf. (CRYPTO '05),* pp. 293-308, 2005.

[15] S. Karthikeyan and M. Nesterenko, "RFID Security without Extensive Cryptography," *Proc. Third ACM Workshop Security of Ad Hoc and Sensor Networks,* pp. 63-67, 2005.

[16] S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri, and A. Kanai, "Privacy Enhanced Active RFID Tag," *Proc. Int'l Workshop Exploiting Context Histories in Smart Environments,* May 2005.

[17] S.S. Kumar and C. Paar, "Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID?" *Proc. Workshop RFID Security,* July 2006.

[18] T. Li and R.H. Deng, "Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol," *Proc. Second Int'l Conf. Availability, Reliability, and Security (AReS '07),* 2007.

[19] T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols," *Proc. 22nd IFIP TC-11 Int'l Information Security Conf.,* May 2007.

[20] D. Molnar and D. Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," *Proc. Conf. Computer and Comm. Security (CCS '04),* pp. 210-219, 2004.

[21] J. Munilla and A. Peinado, "HB-MP: A Further Step in the HB-Family of Lightweight Authentication Protocols," *Computer Networks,* doi:10.1016/j.comnet.2007.01.011, 2007.

[22] M. Ohkubo, K. Suzki, and S. Kinoshita, "Cryptographic Approach to 'Privacy-Friendly' Tags," *Proc. RFID Privacy Workshop,* 2003.

[23] 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," *Proc. Second Workshop RFID Security,* July 2006.

[24] 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," *Proc. OTM Federated Conf. and Workshop: IS Workshop,* Nov. 2006.

[25] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags," *Proc. Int'l Conf. Ubiquitous Intelligence and Computing (UIC '06),* pp. 912-923 2006.

[26] S. Piramuthu, "HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication," *Proc. CollECTeR Europe Conf.,* June 2006.

[27] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment," *Proc. Int'l Conf. Security in Pervasive Computing (SPC '05),* pp. 70-84, 2005.

[28] S.A. Weis, "Security and Privacy in Radio-Frequency Identification Devices," master's thesis, MIT, 2003.

[29] S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Security in Pervasive Computing,* pp. 201-212, Springer, 2004.

[30] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual Authentication Protocol for Low-Cost RFID," *Proc. Ecrypt Workshop RFID and Lightweight Crypto,* 2005.

[31] J. Yang, K. Ren, and K. Kim, "Security and Privacy on Authentication Protocol for Low-Cost Radio," *Proc. 2005 Symp. Cryptography and Information Security,* 2005.