An Improvement in HB-Family Lightweight Authentication Protocols for Practical Use of RFID System

Ziyi Lin and Joo Seok Song

Abstract—Radio frequency identification (RFID) is a booming technology which identifies objects automatically. As the low-cost passive tag in RFID system lacks computational, storage, power, and communication resources, lightweight authentication protocols are necessary for security and privacy issues. The HB-family has been developed since Hopper and Blum proposed the HB protocol in 2001, which is a lightweight authentication protocol for RFID system. Afterwards, many improvements have been developed based on the HB protocol, such as HB+ in 2005, HB-MP in 2007 and HB-MP+ in 2008. In this paper, we propose an improved protocol which is a secure and lightweight. We give the security and performance analysis to prove its advantages over past HB-family protocols and its practicality in reality.

Index Terms—RFID, authentication, lightweight protocol, HB-family.

I. INTRODUCTION

RFID (Radio Frequency Identification) is a technology that uses wireless radio waves to transfer data between an electronic tag and back-end database through a reader, for the purpose of automatically identifying and tracking the objects that tag is attached to. A typical RFID system consists of three parts: a reader, tags, and a back-end Database. Due to the database, more information of objects can be collected and stored and the communication between reader and tag is simplified since line of sight is not demanded [6]. In recent years, RFID system attracts growing interest among the researchers as its wide area of potential applications and it's confident in the replacement of bar-codes in the near future [7].

Passive tags are of very limited computational capabilities, which leads to the lack of resources for performing standard cryptographic operations inside the tag [8]. The security services required by RFID system are mainly the same as other systems: authentication, confidentiality, integrity, un-traceability and availability [12]. Authentication protocol is necessary for the identification of a legitimate tag to reader. Only if after the authentication process, legal participants can communicate with each other.

In 2001, Hopper and Blum proposed the HB protocol, which is the origin of the HB-family lightweight authentication protocols [1]. The HB protocol is

extraordinarily lightweight as it only takes the AND and XOR operations on binary vectors and a noise bit. Afterwards a family of lightweight authentication protocols has been proposed based on HB. All of them are called HB-family.

TABLE I: THE DEVELOPMENT PROCESS OF HB-FAMILY

Year	Topic of Paper	Protocol Name	Comment
2001	Secure Human Identification Protocols	HB	Origin of HB family protocol
2005	Authenticating Pervasive Devices with Human Protocols	HB+	Brief but not against man-in-the-middle attack
2006	A Lightweight Authentication Protocol Secure against Some Attacks	HB++	Not practical-Using a hash function and another function, Four keys
2007	A further step in the HB-family of lightweight authentication protocols	HB-MP	Import the idea of round key After k^2 rounds, key will repeat
2008	HB-MP+ Protocol: An Improvement on the HB-MP Protocol	HB-MP+	Emerge round key randomly Not practical because of the hash function
2009	HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System	HB-MP++	Complex and cost too much

In 2005, Juels and Weis applied this HB protocol in RFID system and proved that HB protocol is only resistant against passive attacks [2]. They proposed a modification protocol, named HB+ to resist the active attacks. Later in the same year, Katz and Shin broke the security proof of HB+ by providing the judgment that HB and HB+ has the parallel and concurrent security property [13]. Also, Gilbert et al. showed that the two protocols are all defenseless to man-in-the-middle attacks [9].

In 2007, the idea of round key is introduced by Munilla and Peinado and they proposed a new protocol called HB-MP [3]. This protocol made improvements on security and performance derived from HB+. However, in 2008, H. Gilbert, M. Robshaw, Y. Seurin proved that there's a very simple passive attack which the adversary simply eavesdrops the communication is possible to impersonate a valid tag [10].

Manuscript received November 10, 2012; revised December 24, 2012. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1B3004161).

Ziyi Lin is with the Department of Computer Science, Yonsei University, Seoul, 120-749, Korea (e-mail: linzy@emerald.yonsei.ac.kr).

Joo Seok Song is with the Department of Computer Science, Yonsei University, Seoul, 120-749, Korea (e-mail: jssong@emerald.yonsei.ac.kr).

In the same year, X. Leng, K. Mayes, and K. Markantonakis proposed HB-MP+ protocol depended on HB-MP, but this protocol only has an abstract description [4].

The development process and brief comments of HB-family is shown in Table I.

In this paper, we propose an improved protocol which has advantages in security and performance over past HB-family protocols.

This paper is organized as follows. In section II, related work is introduced. We will give a brief description about LPN problem, HB protocol, HB+ protocol, HB-MP protocol and their shortages. In section III, we will show the proposed protocol we design. In section IV and V, we will analyze security and performance of the proposed protocol.

II. RELATED WORK

A. LPN Problem and HB Protocol

All HB-family protocols rely on the computation hardness of the Learning Parity with Noise (LPN) problem to resist passive attacks. The LPN problem is known to be NP-Hard [5].

Definition. The LPN problem with security parameters q , k , and $\eta \in (0, 1/2)$ is defined as follows: given a random $q \times k$ binary matrix A , a random k -bit vector x , a vector v such that $|v| \leq \eta q$, and the product $z = A \cdot x \oplus v$, find a k -bit vector x' such that $|A \cdot x' \oplus z| \leq \eta q$, where $|v|$ denotes the Hamming weight of vector v .

All HB-family protocols are called a family because all of them rely on the computation hardness of the Learning Parity with Noise (LPN) problem [2].

In one authentication session of the protocol, q rounds are executed. It takes the noise bit v to apply the LPN problem. In one session, at most ηq errors are accepted.

In 2001, Hopper and Blum proposed a secure human identification protocol which in 2005, was adopted in RFID system and called the HB protocol [2]. To describe the HB protocol, some notations are introduced.

k : length of the secret key shared by the reader and the tag.

x : k -bit secret key shared by the reader and the tag.

a : random k -bit binary vector.

v : noise bit, $k = 1$ (error occurs) with probability $\eta \in (0, 1/2)$.

$\oplus$: XOR operation.

$a \cdot x$: inner product of vectors a and x .

Fig. 1. One round of HB protocol

One round is depicted in Fig. 1 and described as follows:

Step 1: The reader randomly generates a k -bit binary vector a and sends a to the tag as the challenge.

Step 2: The tag receives a and computes $z = a \cdot x \oplus v$. The tag sends z to the reader.

Step 3: The reader checks whether $z = a \cdot x$.

In this protocol, secret key x can be revealed by an adversary who is able to emerge and send fake challenges. The adversary selects the value of the challenge and sends the fake challenge to the reader. If a fixed challenge is sent several times, with high probability the adversary could get the exact value of $a \cdot x$. Then, the adversary can get some bit of secret key x from the fake challenge and value of $a \cdot x$.

B. HB+ Protocol

To solve the weakness of HB protocol, in 2005, Juels and Weis modified the HB Protocol and proposed the HB+ Protocol [2]. HB+ Protocol added another secret key y and a blinding vector b . To describe the HB+ protocol, some more notations are introduced.

y : k -bit secret key shared by the reader and the tag.

b : random k -bit binary vectors.

Fig. 2. One round of HB+ protocol

One round is depicted in Fig. 2 and described as follows:

Step 1: Tag randomly generates a k -bit binary vector b and sends it to reader as a blinding vector.

Step 2: Reader randomly generates a challenge a and sends it to tag.

Step 3: After tag computes $z = a \cdot x \oplus b \cdot y \oplus v$, z is sent to reader.

Step 4: Reader checks whether $z = a \cdot x \oplus b \cdot y \oplus v$.

This protocol has been proved vulunerable to man-in-the-middle attacks [9, 10]. In the second step, an active attacker intercepts a , changes it to a' such that $a' = a \oplus m$ and sends it to tag. The tag has no idea about the change, so it continues calculating z and sending z to reader. In one round, if the reader accepts tag, it means that $z' = z$. The attacker gets that $m \cdot x = 0$. If not, the attacker gets that $m \cdot x = 1$. By changing the value of m , attacker can get the value of secret key x .

C. HB-MP Protocol

In 2007, to defend the attack, the idea of round key is introduced by Munilla and Peinado and they proposed a new protocol called HB-MP [3]. This protocol made improvements on security and performance derived from HB+. To describe the HB-MP protocol, some more notations are introduced.

xm : m -bit binary vector consisting of the m less significant bits of x .

a, b : random m -bit binary vectors.

$\text{Rot}(p, u)$: bit-wise left rotation operator. The operand p is rotated u position.

Fig. 3. One round of HB-MP protocol

One round is depicted in Fig. 3 and described as follows:

Step 1: The reader randomly generates an m -bit binary vector a and sends a to the tag as the challenge.

Step 2: The tag receives a and computes $x = \text{Rot}(x, y_i)$, where y_i is the i th bit of the key y .

Step 3: The tag computes $z = a \cdot xm \oplus v$ and looks for a m -bit binary vector b such that $b \cdot xm = z$. The tag sends b to the reader.

Step 4: The reader receives b and computes the x in the i th round as $x = \text{Rot}(x, y_i)$.

Step 5: The reader checks whether $a \cdot xm = b \cdot xm$.

However, HB-MP Protocol also can not resist the man-in-the-middle attacks [4]. If in one authentication session, the protocol runs k rounds, x will be rotated p bits, where p is the number of '1' in y . If the attacker runs $k \times k$ rounds, the x will be rotated $p \times k$ times and xm will be definitely rolled back and generate a repeated xm . It is an affordable attack.

To solve the problem, in 2008, HB-MP+ protocol is proposed [4]. It uses a one-way hash function to update the round key. This scheme avoids the repeat update of round key, but the hash function is presented in an abstract way which makes this scheme impossible for practical use. What's more, in a tag, only 250-3000 logic gates are allocated for security-related tasks [7] and a hash function demands at least 5000 gates.

III. PROPOSED PROTOCOL

The proposed protocol has two secret keys x and y . x is used to encrypt the challenge value a to produce the response value z and y is used to update the secret key x before calculating the response in each round. The point in our scheme is that before updating secret key x , y is right rotated according to the random value a which tag receives in each round.

All the calculations in this protocol are in an environment of modular 2.

To represent the protocol, some notations are introduced.

k : length of the secret keys shared by the reader and the tag.

i : round number.

y_i : the i th bit of y .

x, y : k -bit secret keys shared by the reader and the tag.

a : random k -bit binary vector.

v : noise bit, $v = 1$ (error occurs) with probability $\eta \in (0, 1/2)$.

$\oplus$: XOR operation.

$a \cdot x$: inner product of vectors a and x .

$|v|$: Hamming weight of vector v .

$R(p, q)$: a right rotation operator, p is right rotated q bits.

Fig. 4. One round of the proposed protocol

One round is depicted in Fig. 4 and described as follows:

Step 1: Reader randomly generates a k -bit binary vector a and sends it to tag as a challenge value.

Step 2: The tag receives a and computes the secret key $y = R(y, |a|)$.

Step 3: Then tag updates its secret key $x = R(x, y_i)$.

Step 4: The tag computes $z = a \cdot x \oplus v$, and z is sent to reader as the response value.

Step 5: The reader receives z and computes the round key $y = R(y, |a|)$, $x = R(x, y_i)$.

Step 6: Reader checks whether $z = a \cdot x$.

We eliminate the vulnerability of HB-MP protocol by updating the secret key y in each round with a random value before it's used to generate the round key. The practical matter of HB-MP+ protocol is solved by describing the protocol concretely and hash function is not used in our protocol.

IV. SECURITY ANALYSIS

A. Resist Passive Attacks

Assume that a passive adversary is able to eavesdrop the communication between tag and reader, this attacker gets the challenge value a and the response value z . To get the secret value x , the attacker has to work out the LPN problem and it's NP-hard [11]. Thus the probability that an adversary responds with an exact z when challenge value a is got is the same as that in HB or HB+ protocol. So the proposed protocol is secure against passive attacks.

B. Resist Active Attacks

Before talking about the active attack, we will define the attacker's aim. In our system, tags do not care about where the messages are from, which means that tags do not authenticate the reader. So the attacker's significant goal is to reveal the secret key x and disguise a fake tag when reader tries to authenticate tags. We assume that the abilities of an

active adversary is to intercept the communication, to change the information sent between entities, to generate a fake challenge vector a' with some value and to send messages to tags.

In our protocol, the secret key y is updated with randomly generated vector a in each round before the i th bit of y is used to update the round key x . This design makes value of x updated irregularly and avoids the shortage of HB-MP protocol that the secret key will repeat after certain rounds.

As y is updated according to a which is a random value, y is also updated irregularly. Before the authentication process, attacker has no idea about value of y and the i th bit of y , so it does not know if secret key x is updated in each round.

According to A. Juels and S. Weis's attack [2], if the attacker challenges tag with a' such that there's only one "1" in some bit, he can get the corresponding bit of x in this round. Due to the usage of noise bit v , the adversary has to carry out several rounds of the protocol with this fixed a' to make sure the correctness of this bit in x . As we talked before, x is updated in each round and the attacker does not know the law how it is updated. As a result, even if the attacker gets some bit, he does not know where this bit belongs to in x .

If the attacker challenges tag with a' such that $|a'| = 0$, the attacker can make sure that the secret value y used to update the round key x will keep the same. As the secret key x is still updates in each round and $|a'| = 0$ means that number of '1' bits in the challenge is even, attacker still can get nothing from the fake challenge and response value.

In summary, our protocol defends against active attacks.

C. Data Confidentiality

Based on the earlier discussion, secret key x and y in our protocol can not be revealed to attacker, thus the proposed protocol confirms the confidentiality of data.

D. Data Integrity

AS one can observe, in the proposed protocol, if data transmitted has been tampered with, the authentication process will not be successful. Data integrity is reserved.

TABLE II: SECURITY ANALYSIS

	HB	HB+	HB-MP	HB-MP+	Proposed Protocol
Against Passive Attacks	Y	Y	N	Y	Y
Against Active Attacks	N	N	N	Y	Y
Confidentiality	N	N	N	Y	Y
Integrity	N	N	N	Y	Y
Synchronization	Y	Y	Y	N	Y

E. Synchronization

Since the proposed protocol takes advantage of the round key, synchronization problem should be considered. On reader side, before each authentication session, secret keys will be set to the initial value, so that it keeps the same pace with tags and this method solves the synchronization problem.

Table II shows the summary on the security aspects of several typical HB-family protocols and proposed protocol. Here 'Y' means 'yes' and 'N' means 'no'.

V. PERFORMANCE ANALYSIS

A. Calculation Cost of Tag

We can observe from the description of the proposed protocol that only bit-wise AND and XOR operations are used and they are appropriate for the low cost passive tags.

In an environment of modular 2, the Hemming Weight of vector a can be calculated when tag receives a on the bit fly. In fact, this is the bit-wise AND operation on each bit of a .

After getting $|a|$, function $R(p, q)$ is calculated. This is a right rotated function and it is also bit-wise.

HB+ protocol needs to calculate a more complexed formula to get the response value z compared with our protocol.

HB-MP and HB-MP+ protocols need to pick up a vector b before responding to reader and there's no need to do this operation in proposed protocol.

B. Communication Cost

HB+ protocol transmits two k -bit vectors before calculating response value. HB-MP and HB-MP+ protocol transmits a k -bit response value and our protocol only transmits 1-bit response value. Table III shows the comparison between these protocols about the cost of communication.

TABLE III: COMMUNICATION COST COMPARISON

	HB	HB+	HB-MP	HB-MP+	Proposed Protocol
Communication Cost	$k+1$	$2k+1$	$2m$	$2m$	$k+1$

VI. CONCLUSION

The proposed protocol provides a concrete design for the authentication process in RFID system and it belongs to the HB-family. It satisfies the requirements of low-cost tags with limited memory and computational abilities and has very low communication costs. Our protocol defends all passive and active attacks proposed for HB-family protocols of RFID systems till now.

This protocol is suitable for practical use because it is presented in detail and has advantages in security and performance over other HB-family protocols.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012 R1A1B3004161).

REFERENCES

- [1] N. J. Hopper and M. Blum, "Security human identification protocols," *Advances in Cryptology-ASIACRYPT, Lecture Notes in Computer Science*, vol. 2248, pp. 52-66, 2001.

- [2] A. Juels and S. Weis, "Authenticating pervasive devices with human protocols," *Advances in Cryptology-Crypto2005, Lecture Notes in Computer Science*, vol. 3621, pp. 293-308, 2005.
- [3] J. Munilla and A. Peinado, "HB-MP: A future step in the HB-family of Lightweight authentication protocols," *Computer Networks*, vol. 51, pp. 2262-2267, 2007.
- [4] X. Leng, K. Mayes, and K. Markantonakis, "HB-MP+ Protocol: An improvement on the HB-MP protocol," in *Proc. IEEE International Conference on RFID*, pp. 118-124, April 2008.
- [5] A. Blum, A. Kalai, and H. Wasserman, "Noise - tolerant learning, the parity problem, and the statistical query model," in *Proc. the Thirty-Second Annual ACM Symposium on Theory of Computing*, Portland, Oregon, 2000.
- [6] *International Organization for Standardization*, ISO/IEC 18000-3. Information Technology AIDC Techniques-RFID for Item Management, 2003.
- [7] *EPC Electronic Product Code Global inc.* [Online]. Available: <http://www.epcglobalinc.org>.
- [8] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the ASE algorithm," *CHES 2004.LNCS*, vol. 3156, pp. 357-370, 2004.
- [9] H. Gilbert, M. Robshaw, and H. Silbert, "An active attack against HB+- a provably secure lightweight authentication protocol," *ELECTRONICS LETTERS*, vol. 41, pp. 1169-1170, 2005.
- [10] H. Gilbert, M. Robshaw, and Y. Seurin, "Good variants of HB+ Are hard to find," *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, vol. 5143, pp. 156-170, 2008.
- [11] S. Piramuthu, "HB and related lightweight authentication protocols for secure RFID tag/ reader authentication," *COLLECTeR Europe Conference*, Basel, Switzerland, June, 2006.
- [12] N. J. Hopper and M. Blum, "A secure human-computer authentication scheme," Tech. Rep. CMU-CS-00-139, Carnegie Mellon University, 2000.
- [13] J. Katz and J. Shin, "Parallel and concurrent security of the HB and HB+ Protocols," Cryptology ePrint Archive, Report 2005/461, 2005.

Ziyi Lin was born in August, 29th, 1988 in Dandong, China. She received the B.S. degree in software engineering program from Jilin University, Changchun, China, in 2011. She is currently working toward the M.S. degree in computer science at Yonsei University, Seoul, Korea. Her research interests include wireless networks, communications, and security of RFID system.

Joo Seok Song received the B.S. degree in Electrical Engineering from Seoul National University, Seoul, Korea, in 1976, and the M.S. degree in Electrical Engineering from Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 1979. In 1988, he received the Ph.D. degree in Computer Science from University of California at Berkeley. From 1988 to 1989, he was an Assistant Professor at the Naval Postgraduate School, Monterey, CA. He was the president of Korea Institute of Information Security and Cryptology in 2006. He is currently a Professor of computer science at Yonsei University, Seoul. His research interests include cryptography and network security.