Lightweight RFID Authentication Protocol without Asynchronous Flaw

[1]Shyh-Chang Tsaur, [2]Hui-Yu Chen and [3]Ju-Pei Pai

Abstract

Radio Frequency Identification (RFID) has been widely used in several applications and its security has become a critical issue in this field. So far, several secure protocols have been proposed to authenticate the legitimate reader and tag. However, in these protocols, if the transmitted parameters are lost, the shared counter can become inconsistent. In this condition, the authentication between the reader and the tag will fail and the tag has to be reset for using in this system. In this paper, we will propose a lightweight authentication scheme to overcome the asynchronous flaw and withstand the man-in-the-middle attack.

Keywords: RFID, authentication, asynchronous flaw, man-in-the-middle attack.

1. Introduction

Radio Frequency Identity System (RFID) consists of tag, reader, and back-end database. RFID tags come in three general varieties: passive, active, and semi passive, depending on whether there is an internal power supply. Furthermore, the frequency of RFID tags can be classified into three categories: low-frequency (LF, operating at 124 to 135 kHz), high-frequency (HF, operating at 13.56 MHz), and ultra high-frequency (UHF, operating at 860-960 MHz and sometimes 2.45 GHz). In this paper, we focus on the passive tags. Passive tags require no internal power supply, and it can operate in any different frequency bands. In order to be used in manufacturers to replace the traditional Universal Product Code (UPC), the cost of each tag should be reduced. Cents [9] the number of gates for a tag generally range between 7.5 thousand and 15 thousand. However, the gate number of a tag for security functionality is at most about 2 thousand. However, DES or AES encryption algorithm need range 5 thousand to 10 thousand. Thus, the symmetric and public-key cryptography is difficult to be implemented on passive tags. RFID can transmit at long distance, store much data, and many other advantages in comparison with traditional bar code. The basic operation procedures of RFID are as follows.

1). Reader sends the electromagnetic wave to tag.

2).Tag obtains the power from the conversion of electromagnetic waves. The power is supported to send messages back to the reader.

3).Upon receiving the transmitted message, reader decodes the data and sends to the back-end database.

In 2003, CENT (http://www.cnet.com/) assessed RFID as one of top ten most significant influences on technology. RFID applications include Avionics [5], mobile business [4], production process of an automotive industry supplier [13], and animal RFID chips etc..

In the many applications of RFID, security and privacy have become important issues. An illegal reader collects nearby information of tag maliciously,

[1]*Department of Computer Science and Information Engineering, Feng Chia University, Taichung, Taiwan*
Email: sctsaur@gmail.com
[2]*Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan*
Email:huiyuchen@nchu.edu.tw
[3]*Department of Information Science and Applications, Asia University, Taichung, Taiwan*
Email: rupai0718@gmail.com

and therefore the personal privacy is violated. For instance, the important data or information of personal possession tagged without security protection can be easily obtained by the illegal reader. For this, Garfinkel [6] proposed the "An RFID Bill of Rights" for the policy and legislation issues of the RFID, to protect the privacy of consumers. In addition, we still need to ensure the security of RFID so that the tag information would not be illegally stolen by the theft. The paper proposes an enhancement to patch an existing authentication protocol.

In order to make the RFID more widely used and more competitive, the cost of RFID tag must be reduced. However, the low-cost tags usually lead to limit the function of operation. The transitional encryption algorithms can not almost used in resource-constrained RFID tag so that the security in the system will be affected. In general, the attack types for RFID authentication protocols can be summarized as follows.

1). Passive attack: This type of attacks can only get information from tag, but cannot control the communication channel between the reader and the tag.
2). Active attack: This type of attacks not only can get the information from tag, but also allows to control the communication channel between the reader and the tag.
3). Man-in-the-middle attack: This type of attacks is a form of active attack, and the attacker can change the messages between the reader and the tag, so it will make the reader and the tag believe that they are talking to each other directly. In fact the whole conversation is fully controlled by the attacker who is able to intercept all messages going between the reader and the tag.

In order to withstand these attacks, many improved schemes have been proposed. In 2001, Hopper and Blum proposed HB scheme [8] to prevent passive adversaries, and use lightweight authentication protocols to reduce the computations for RFID tags. After that, a family of lightweight authentication protocols has been proposed. In 2005, Juels and Weis proposed HB+ scheme [10] to modify the HB scheme to resist against active attacks. Gilbert et al. [7] found the man-inthe-middle attacks to break the security of the HB and HB+ schemes. Then, several authors modified the HB+ scheme to withstand man-in-the-middle attacks. Bringeret al. proposed HB++ scheme [3] in 2006, Munills and Peinado proposed HB-MP scheme [12] in 2007. Leng et al. [11] found a problem, that the HB-MP scheme is not really secure withstand the man-in-the-middle attacks. They proposed the HBMP+ scheme modifing the HB-MP to withstand man-in-the-middle attack. The attacker has the opportunity to get the secret key in a repeat cycle time. Besides improving these security flaws, we found that HB-MP scheme has the situation of asynchronism. This situation not only lead to make the verification of the tag fail but also make the tag useless in the next rounds. The fault is due to the transmitted message might get lost and the shared parameters stored in the reader, these cause the tag inconsistent. For example, a tag sends a message to reader for verification, but the reader misses this message. The tag holds the message has been successfully sent to the reader and changes the shared parameters to next new one. However, the reader does not find out that the tag has changed the parameters and still keeps the old shared parameters. In this case, the tag arises the asynchronous flaw because the shared parameters between the reader and the tag are in consistent and thus it cannot pass the verification. In the previews papers, the HB-MP scheme solves the security flaw of man-inthe-middle

attack in HB+ scheme, and improves their effectiveness. However, the asynchronous flaw still existed in HB-MP scheme. In this paper, we improve the HB-MP scheme by proposing a lightweight authentication protocol to overcome this flaw. Furthermore, our scheme can withstand the man-in-the-middle attack. This paper is constructed as: Section 2 reviews the previous scheme and analyse the security of the previous scheme, and describes two RFID security attacks in this section. Section 3 describes protocol of the proposed scheme. Section 4 analyse the security of the proposed scheme, and compares the efficiency and security of the proposed scheme with others previous schemes. Section 5 concludes this paper.

2. Related Works

In 2001, Hopper and Blum proposed the HB [8] scheme, which is the beginning of a family of lightweight authentication protocols and only resists to passive attacks. In 2005, Juels and Weis proposed the HB+ scheme [10], which is to modify the HB scheme to resist against simple passive attacks. Bringer et al. further improved the HB+ scheme to overcome the man-in-the-middle attack, and proposed the HB++scheme [3] in 2006. Unfortunately, this scheme is more complicated than previous schemes. Then Munills and Peinado proposed an improvement of HB+ scheme, called HB-MP scheme [12], withstanding the man-in-the-middle attack and improving the performance of computation. Recently Leng et al. pointed out that the HB-MP scheme was not really secure against the man-in-the-middle attacks and proposed an improved scheme, called HB-MP+ scheme [11], to overcome this problem. In the following, we will briefly describe the processes of the HB-MP scheme. That would help distinguish the main difference between HB-MP scheme and this research.

2.1 The HB-MP scheme

HB-MP scheme was proposed by Munills and Peinado in 2007 [12], to modified the HB+ scheme to withstand man-in-the-middle attacks. HB-MP scheme can reduce the number of interchanged messages and thus the effectiveness of HB-MP scheme is better than the previous work. Before introducing the HB-MP scheme, the notations is used in HB-MP scheme and our research is described as follows.

1).x and y: Two secret keys shared between the reader and tag.

2).k: The length of the secret keys x and y.

3).m: The length of the messages exchanged.

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

5).a and b: Two random m-bit binary vectors.

6).v: The noise bit; v = 1 with probability ´2 [0; 1=2].

7).⊕: The operation of excursive OR.

8).a · x: The scalar product of vectors a and x. Rotate(x,w): The bitwise left rotate operator. The operand x is rotated w positions.

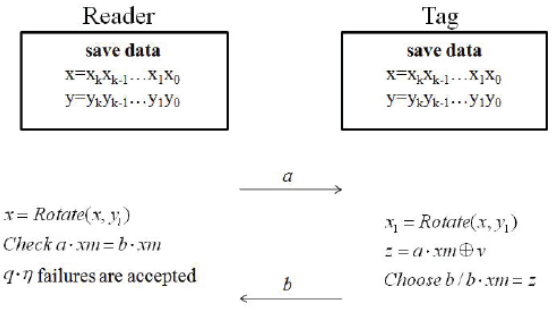

Figure 1: The *i*th round of the HB-MP authentic scheme

HB-MP scheme needs to perform q rounds. The ith round is illustrated in Figure 1 and described as follows.

Step 1: Reader picks a random m-bits binary vector a, and sends it to tag.

Step 2: Tag gets the random number a, then tag computes $x=Rotate(x; yi)$, where yi is the ith bit of the key y.

Step 3: Tag computes $z = a \cdot xm \oplus v$.

Step 4: Tag looks for a m-bit binary vector b such that $b \cdot xm = z$.

Step 5: Tag transmits the parameter b to the reader.

Step 6: Upon receiving the parameter b, reader computes $x = Rotate(x; yi)$.

Step 7: Reader verifies

$$a \cdot xm = b \cdot xm.$$

If the equation holds, the tag passed the verification.

2.2 Security flaws in HB-MP scheme

If an attacker randomly generates a random bit for one round response to the reader, the reader may accept an imposturous tag with probability 1/2 (probability with 0 or 1). After q rounds, an attacker only the probability $1/2^q$ can pass the verification. An attacker can observe $O(n)$ challenge-response pairs between the reader and the tag. The attacker can use Gaussian elimination to discover the secret x and masquerade as reader. In order to tolerate some errors in HB scheme, HB-MP scheme adds a noise bit $v$in the tag verification. HB-MP scheme allows tag to respond incorrectly with probability ´.

Since the tag is incorrect response, the attacker eavesdrop all challenge response pair. The pair is miscellaneous incorrect value, in that case the adversary can no longer simply use Gaussian elimination to learn the secret x. This is a problem of learning parity with noise (LPN) [2]; however, the problem of learning x becomes NP-Hard [1] in the wrong data, the security of this scheme will no longer be subject to strong protection unless $P = NP$.

The HB-MP scheme implements an authentication scheme based on the LPN problem, thus the HB-MP can resist to the passive attacks. The HB-MP scheme reduces the messages exchanged between the reader and the tag, and the scheme by using two messages instead of three messages interchanged in the HB+ scheme. This enhances the effectiveness of the operation. $Rotate(x, yi)$ is used in this protocol to rotated secret key yi positions in every round, so that each round of secret key x will not be the same. Therefore, the active attacker cannot know the correct key.

The HB-MP scheme claimed that their scheme can resist against passive attacks, active attacks, and the man-in-the-middle attacks. Since the xm is modified at every round, the man-in-the-middle attack can be resisted. However, the HB-MP+ scheme presents that the HB-MP scheme does not really resist the man-in-the-middle attack. When attackers collect enough data of verifications, attackers might find the repeated xm in the HB-MP scheme. In the following, we describe the security flaws in HB-MP scheme.

2.2.1 The Man-in-the-middle attack in HB-MP scheme

In 2008, Leng et al. [11] had shown that HB-MP scheme did not exactly resistant against to man-in-the-middle attack. An authentication session is composed of q rounds, the length of the secret keys x and y are k bits, and the secret key x is updated in every authentication session. When the attacker runs the protocol k rounds, the key x will be rotated n bits, and the n is the number of '1' in key y. Unfortunately, when the protocol runs k times, it means that the protocol exactly runs k^2 rounds. The key x will be

rotated n ¢ k times, and x will rotated back to its initial value. Therefore, HB-MP scheme is still possible attacked.

2.2.2 The asynchronous flaw in HB-MP scheme

Besides the man-in-the-middle attack, HB-MP scheme may arise the asynchronous flaw. In Figure 2, we will illustrate an example to show the situation in HB-MP scheme. In this example, suppose that the key x is 0110, and y is 0011, the notation xi is the key in the ith round, and yi is the ith bit of the key y, the key in this protocol is $x0$ initially. The authentication protocol runs from round 1 to round 2.

Step 1: Reader randomly picks a 4-bit binary vector $a1$, and sends it to tag.

Step 2: Tag receives the random number $a1$, then tag computes $x1 = Rotate(x0; y1)=1100$. In this time, reader and tag are to record round 1.

Step 3: Tag computes $z = a_1 \cdot x_1 m \oplus v$, and looks for a 4-bit binary vector b such as $b \cdot x_1 m = z$. Then tag transmits the b to reader, but the parameter b gets lost in the transmission process.

Step 4: In this time, reader is still to record round 1, but tag is record to round 2.

In the above example, the condition of counter inconsistency may arise. Therefore, we proposed a new scheme to prevent the system from the man-in-the-middle attack and the asynchronous flaw.

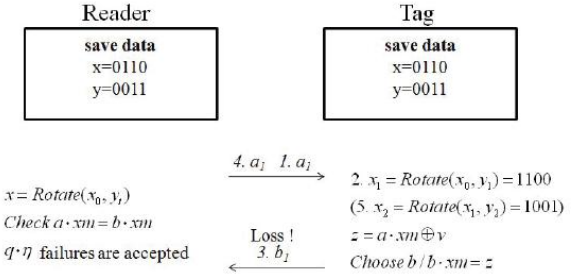

Figure 2: The asynchronous flaw in HB-MP scheme

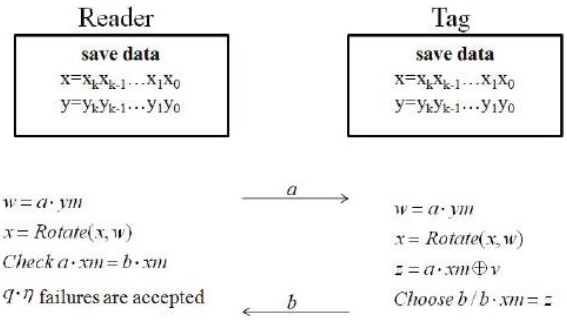

Figure 3: The *i*th round of the propose authentication scheme

3. Proposed Scheme

In this paper, we present a new scheme to withstand the man-in-the-middle attack and overcome the asynchronous flaw. The number of keys and the communication overhead in our scheme are the same as the HB-MP scheme. The protocol has to run q rounds, and the details of the ith round is illustrated in Figure 3 and described as follows.

Step 1: Reader picks a random m-bits binary vector a, and delivers it to tag.

Step 2: When tag receives the random number a, tag computes

$$w = a \cdot ym; \quad (1)$$

$$x = Rotate(x;w); \text{ and} \quad (2)$$

$$z = a \cdot xm \oplus v; \quad (3)$$

where xm and ym are the m less significant bits of x and y, and a ¢ xm and a ¢ ym are the scalar products.

Step 3: Tag looks for am-bits binary vector b such that b ¢ xm= z, and then tag delivers b to reader.

Step 4: Upon receiving the parameter b, the reader computes

$$w = a \cdot ym \text{ and} \quad (4)$$

$$x = Rotate(x,w): \quad (5)$$

Step 5: After that, the reader compares the two values of a ¢ xm and b ¢ xm. If the two values are equal, the tag passes the authentication.

4. Discussions

4.1 Security Analysis

1).*Secrecy*: In the proposed scheme, the authentication protocol is composed of *q* rounds challenge-response pairs. In order to increase the security of the protocol, some errors can be included in the responses *z* to make challenge response pair miscellaneous incorrect value. The error is noise bit with probability $\eta \in [0, 1/2]$. In that case the adversary can no longer simply use Gaussian elimination to learn the secret *x*. This is a problem of learning parity with noise (LPN), which let learning *x* becomes NP-Hard in the wrong data.

2).*Resist the man-in-the-middle attack*: The HB-MP+ scheme found a problem in HB-MP, that the HB-MP scheme is not really secure against the man-inthe-middle attack. Fortunately, our scheme does not have this problem. There as on is that the protocol includes conversion of $w = a \cdot ym$ and rotation of $x = Rotate(x,w)$ in each round. The computation of the key *x* is not the same, so the response $z = a \cdot xm$ is not the same too. If an unauthorized reader transmits a forged parameter *a0* which is modified from *a*, the unauthorized reader is not able to obtain the secret key *x* because the unauthorized reader does not know the key *y* and *xm*. Thus, our scheme is not same as the HB-MP, HB-MP is to rotate *x* by *yi*, *yi* is the *i*th of the key *y*, and *i* is determined by the number of round. However, our scheme is to rotate the *x* by *a*, the *a* is a random number generated by the reader, and our scheme will not have opportunity to allow attackers to obtain the secret key created according to the number of round. Even if the attacker changes the value of *b*, the calculation results are not the same between the reader and the tag, and it cannot be successfully verified.

3).*Overcome the asynchronous flaw*: In HB-MP scheme, the parameter *b* might get lost in the transmitted process of *i*th round. Since tag has delivered *b* to the reader, *i*+1th round is recorded by the tag as the current round. However, since the reader did not receive the parameter *b*, so the current round recorded by the reader is *i*th round. We can find that the counter is inconsistent between the reader and the tag. The verifications of the following rounds will fail. In our scheme, the secret key *x* is calculated by the random number *a*, where *a* is generated from the reader every round. Even if the transmitted message gets lost, the new random number *a* will be used by the reader and tag in the next round. Therefore, the message loss will not lead to the failed verification.

4.2 Comparisons

Table 1 shows the comparisons in number of secret key and response time with the previous schemes. Table 2 shows the how HB family schemes are compared insecurity requirements.

Table 1: Comparisons in the number of secret keys and response time

Schemes	secret keys	response tims
HB	1	1
HB^{+}	2	2
HB^{++}	4	2
HB-MP	2	1
Our scheme	2	1

Table 2: Security requirements comparisons among the HB family schemes (○: supported, ×: not supported)

Schemes	Secure of the security problems			
	Passive attack	simple active attack	man-in-the-middle attack	counter asynchronism
HB	o	x	x	o
HB^{+}	o	o	x	o
HB^{++}	o	o	o	x
HB-MP	o	o	x	x
Our scheme	o	o	o	o

As the results in the Table 1 and 2, HB scheme requires the least secret keys and response times of all. However, it is not secure against the attacks of simple active attack and man-in-the-middle attack. HB+ scheme is more complex than HB scheme, but this scheme can withstand the simple active attack. HB++ scheme has been able to resist the man-in-the-middle attacks, but this scheme is the most complex than the previous schemes. HB-MP scheme requires two secret keys and one response time, but it cannot withstand the man-in-the-middle attack. This indicate that HB-MP scheme has the asynchronous flaw. Our scheme also requires two secret keys and one response at each round. In particular, our proposed scheme can resist the passive attack, simple active attack, man-in-the-middle attack, and also overcome the asynchronous flaw.

5. Conclusion

This scheme is to improve the HB-MP scheme to resist the man-in-the-middle attack. Furthermore, our scheme can overcome the asynchronous flaw. As the compared results, we can find that the overall effectiveness of our scheme is indeed superior to previous schemes.

References

[1] E. R. Berlekamp, R. J. McElice, and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, vol. 24, pp. 384–386, May 1978.

[2] A. Blum, M. L. Furst, M. J. Kearns, and R. J. Lipton, "Cryptographic primitives based on hard learning problems," in *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, vol. 773,pp. 278–291, New York, USA, 1994. Springer-Verlag.

[3] J. Bringer, H. Chabanne, and E. Dottax, "HB++: a lightweight authentication protocol secure against some attacks," in *Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, pp. 28–33, Lyon, France, June 2006.

[4] R. Falk, F. Kohlmayer, A. Kopf, and M. Li, "High-assurance avionics multidomain RFID processing system," in *Proceedings of 2008 IEEE International Conference on RFID*, pp. 43–50, Las Vegas, Nevada, Apr. 2008.

[5] S. Gao, "RFID applications toward mobile business," in *Proceedings of2007 IEEE International Conference on the Management of Mobile Business*, pp. 65–66, Washington, DC, USA, July 2007. IEEE Computer Society.

[6] S. Garfinkel, "An RFID bill of rights," *Technology Review*, p. 35, Oct. 2002.

[7] H. Gilbert, M. Robshaw, and H. Silbert, "An active attack against HB+ -a provable secure lightweight authentication protocol," *Electronics Letters*, vol. 41, pp. 1169–1170, Oct. 2005.

[8] N. J. Hopper and M. Blum, "Secure human identification protocols," in *Proceedings of the 7th International Conference on the Theory and*

Application of Cryptology and Information Security, vol. 2248, pp. 52–66, London, UK,2001. Springer-Verlag.

[9] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381–394, Feb. 2006.

[10] A. Juels and S. Weis, "Authenticating pervasive devices with human protocols, "*Lecture Notes in Computer Science - Advances in Cryptology (CRYPTO2005)*, vol. 3621, pp. 293–308, Aug. 2005.

[11] X. Leng, K. Mayes, and K. Markantonakis, "HB-MP+ protocol: An improvement on the HB-MP protocol," in *Proceedings of 2008 IEEE International Conference on RFID*, pp. 118–124, Nevada, USA, Apr. 2008.

[12] J. Munilla and A. Peinado, "HB-MP: A further step in the HB-family of lightweight authentication protocols," *Computer Networks*, vol. 51, no. 9, pp. 2262–2267, 2007.

[13] L. Toth, P. Dobrossy, and D. Manik, "RFID application in production process of an automotive industry supplier," in *Proceedings of 10th International Conference on Intelligent Engineering Systems*, pp. 45–48, Sep. 2006.