International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.211-220
http://dx.doi.org/10.14257/ijsia.2015.9.8.18

An Improved HB+ Protocol and its Application to EPC Global Class-1 Gen-2 Tags

Zhicai Shi, Jian Dai, Fei Wu, Yongxiang Xia, Yihan Wang and Changzhi Wang

School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, P. R. China
szc1964@163.com,1101196001@qq.com,{fei-wu1,x-free}@163.com, ehan@sues.edu.cn, 774936933@qq.com

Abstract

RFID is a key technology that can be used to create the pervasive society. The EPCglobal Class-1 Gen-2 specification is an important standard for RFID. The tags conforming to this standard have limited computing and storing resources, and no more attentions are paid to their security and privacy. So the application of these tags is not secure. HB+ protocol is one of the typical lightweight authentication protocols suitable to these low-cost RFID tags. But it is vulnerable to active attacks. For some scenarios with frequent active attacks the efficiency of HB+ protocol will be degraded seriously. In order to improve the security and efficiency of HB+ protocol for some scenarios with frequent active attacks, a novel detection-exit-restart mechanism is proposed to monitor the integrity of the exchanged messages between the reader and the tag. The improved HB+ protocol can resist active attacks and it is more efficient and secure than HB+ protocol. This protocol only uses the computing resources embedded in tags and it is very suitable to low-cost RFID systems.

Keywords: *RFID, Authentication protocol, HB+ protocol, Privacy, Security*

1. Introduction

Radio Frequency Identification (RFID) technique is a pervasive technology deployed in everyday life and it uses the wireless radio-waves to automatically identify objects, without visible light and physical contact. Today, RFID systems have been successfully applied to manufacturing, supply chain management, agriculture, communication and transportation, healthcare, electronic-payment, e-passport and other fields [1]. However, this promising technology may suffer from some privacy leakage and security threats. For example, businesses may have malicious competitors to collect unprotected RFID information, use forgery tags to provide some wrong information, or even launch denial of service attacks against RFID systems. On the other hand, as a consumer, it is naturally preferred that the information of his RFID-tagged products should be private. However, a reader can read the content of an un-protected tag, tracing the RFID-tagged product and even identifying the person carrying the RFID-tagged product. To protect the private information on the RFID tags, some special techniques can be used. Currently, these techniques are divided into two main categories: physical approach, encryption mechanism and protocol [2-3]. The current research results indicate that encryption mechanism and protocol is a more flexible and effective approach for ensuring the security and privacy of RFID systems. RFID authentication is a special encryption protocol which is widely deployed. Many authentication protocols for RFID systems have been proposed. Among these protocols, HB family protocols are some typical authentication protocols and they include HB, HB+, HB++, HB-MP, HB-MP+, and HB#. These protocols are very suitable to the resource-constrained RFID tags, but these protocols are provable to be vulnerable to some active attacks (*e.g.* man-in-the-middle

ISSN: 1738-9976 IJSIA

attack). EPCglobal Class-1 GEN-2 RFID specification (which is called the C-1 G-2 RFID specification for short) is one of the most important resource-constrained RFID standards proposed by EPCglobal and it can be considered as a "universal" standard for low-cost RFID tags. The C-1 G-2 RFID tags are very cheap and their effective transmitting range is about 2 to 10 meters. These tags provide PRNG function and CRC function. It is believed that the C-1 G-2 RFID tags will become the mainstream for developing the RFID systems [4]. But the C-1 G-2 RFID tags only have the limited computing and storing resources. They pay little attention to the security and privacy threats. In order to assure the security and privacy of the C-1 G-2 RFID tags, we improve HB+ protocol by means of the computing resources provided by the C-1 G-2 RFID tags and propose an improved HB+ protocol to resist against man-in the middle attacks. Our proposed protocol is a lightweight authentication protocol and it is very suitable for some scenarios with frequent active attacks.

The paper is organized as follows. In Section II, the LNP problem and HB family protocols are introduced and analyzed, we describe the weakness and vulnerability of HB family protocols. In Section III, we improve HB+ protocol by means of CRC function embedded in the C-1 G-2 RFID tags. We propose a novel lightweight authentication protocol: IHB+ protocol, which is special suitable to resist against frequent active attacks. In Section IV we compare our proposed protocol with other HB family protocols and we give secure analysis of our proposed protocol. In Section V, we conclude our work and point out the advantages of our proposed protocol over other HB family protocols.

2. HB Protocol and its Variants

An RFID system usually consists of three components: Radio Frequency(RF) tags, RF readers and a backend server. The function of an RFID authentication protocol is that the tag authenticates the reader before it is accessed. Then the authenticated readers can get the content of the legitimate tags. Moreover, private information would not be leaked to un-authenticated entities.

An RFID authentication protocol is a special cryptographic protocol, where resource-constrained RFID tags are involved. This kind of protocol is called the lightweight authentication protocol. For the RFID tags, conventional authentication protocols that concern symmetric key computations or even public key computations are not applicable. So some special lightweight authentication protocols are proposed successively in order to satisfy the special conditions of RFID tags. HB protocol and its improved protocols are some typical lightweight authentication protocols, which are called HB family protocols. All HB family protocols rely on the computation hardness of the Learning Parity with Noise(LPN) problem to resist against passive attacks. The LPN problem is NP-Hard and currently no polynomial algorithm is known to solve the LPN problem.

Definition. The LPN problem with security parameters q, k, η with $\eta \in (0, 1/2)$ 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 t such that $|A \cdot t \oplus z| \leq \eta q$, where $|v|$ denotes the Hamming weight of vector v.

Based on LPN problem, Hopper and Blum proposed a secure human identification protocol in 2001, which is called HB protocol[5]. The protocol is composed of r rounds and the tag shares the secret key x with the reader. One round of the protocol is depicted in Figure1.

In Figure1, x is a k-bit secret key shared by the reader and the tag. a is a random k-bit binary vector. v is a noise bit, $v=1$ (error occurs) with probability $\eta \in (0,1/2)$. $\oplus$ represents XOR operation. $a \cdot x$ represents the inner product of vectors a and x.

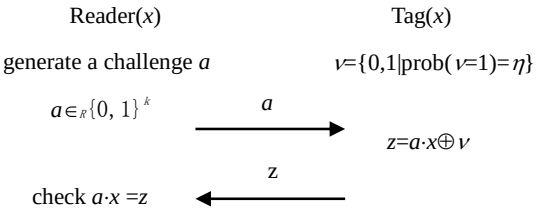

Figure 1. The Diagram of HB Protocol

One round of HB protocol is 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 $z= x \cdot a \oplus \nu$. The tag sends z to the reader.

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

Each authentication consists of r rounds to repeat the process described above, the reader then authenticates the tag after r rounds if the tag's response is incorrect less than ηr. The purpose which the tag injects noise ν into its response is to prevent passive eavesdroppers to reveal the secret key x. If an eavesdropper would like to obtain the secret key x from the observed challenge-response pairs he has to solve LPN problem.

But the HB scheme is not secure against active attacks. The 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. Once k equations with linearly independent a's have been acquired, the secret key x can be revealed by Gaussian elimination [6].

To overcome the weakness of HB protocol, in 2005, Juels and Weis improved HB protocol and proposed HB+ protocol [7], as shown in Figure 2. HB+ protocol added another secret key y and a blinding vector b. HB+ protocol used the vector b to blind the secret key y so as to increase the difficulty to reveal the secret keys.

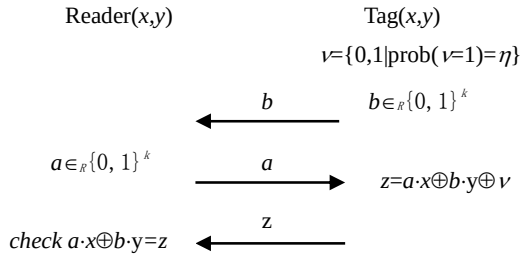

Figure 2. The Diagram of HB+ Protocol

In Figure 2, y is another k-bit secret key shared by the reader and the tag. b is a random k-bit binary blinding vector. One round of HB+ protocol is described as follows:

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

Step 2: The reader randomly generates a challenge a and sends it to the tag.

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

Step 4: The reader computes $x \cdot a \oplus y \cdot b$ and checks whether the result equals z.

This protocol has been proved vulnerable to some active attacks (*e.g.* man-in-the-middle attacks) [8-9]. Henri Gilbert, Matthew Robshaw, and Hervé Sibert proposed a simple active attack against HB+ protocol, which is called GRS attack later. It is supposed that the adversary is capable of tampering challenges sent by a legitimate reader to a legitimate tag during the authentication process, and he can check whether the authentication results are successful or not. Figure 3 depicts the detail procedure of this attack. The adversary chooses a k-bit constant vector δ and uses $a'=a \oplus \delta$ to replace each challenge a sent by a legitimate reader to the tag for each round authentication. If the

authentication process is successful, then we can conclude $\delta \cdot x=0$ with overwhelming probability. If authentication doesn't succeed then $\delta \cdot x=1$ with overwhelming probability. For all r round authentication the same δ is used and the authentication results will reveal one bit information of secret key x. To get the k-bit secret x, it is enough to repeat the whole protocol k times with linearly independent δs. Once x has been derived, the adversary can either impersonate the tag by using b=0, or the adversary can derive and recover the k-bit secret key y by using the similar approach. Once the secret key x or y is disclosed the privacy of the tag's identity is also compromised.

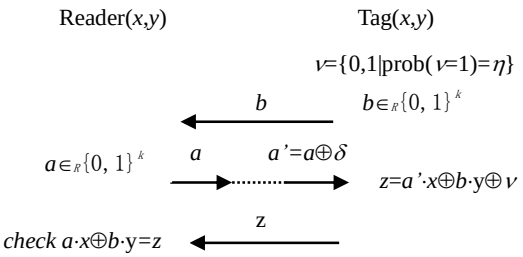

Figure 3. The Diagram of an Active Attack to HP+ Protocol

In 2006, Julien BRINGER and Herv´e CHABANNE improved HP+ protocol so as to thwart GRS attack, which is called HP++ protocol[10]. HP++ protocol is shown as Figure 4.1 and 4.2. Each tag shares a unique secret Z with the reader. At the beginning phase of each authentication, two challenges are exchanged between the reader and the tag. These challenges are computed under the secret key Z by a universal hash function $h()$ to obtain the secret keys x, x', y and y'. The secret keys are then used to perform the subsequent authentication. The i^{th} round of the authentication protocol is depicted in Figure 4.2.

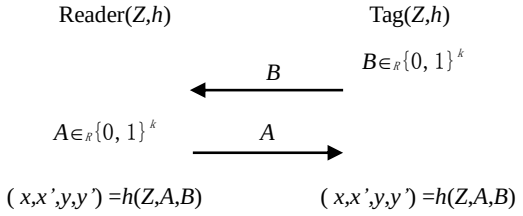

Figure 4.1. The Secret Key Generating Phase of HP++ Protocol

During the authenticating process two function $f()$ and $rot()$ with a low complexity are used to guarantee the integrity of a and b. HP++ protocol is also three step authentication protocol. In the last step of each round authentication, the tag sends z and z' to the reader. Moreover, the secrets are renewed after each entire authentication. Julien BRINGER proved that HP++ protocol is at least as secure as HP+ protocol. For HP++ protocol, some new secret keys are generated by a hash function and this guarantees each authentication to use the different secret keys. But this increases the complexity of the protocol. A and B are transferred by plaintext. If A or B is tampered the secret keys between the tag and the reader are different and this compromises the further authentication between them. Otherwise, z' is dependent on the current round number of each authentication and this maybe result in the synchronization problem between the tag and the reader.

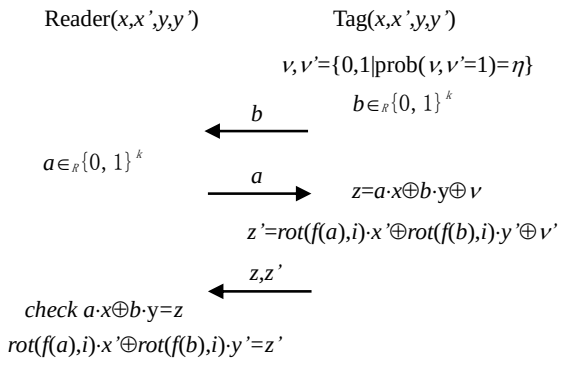

Figure 4.2. The Authenticating Phase of HP++ Protocol

In 2007, to defend the active attack, J. Munilla and A. Peinado introduced the idea of round key to improve the security and performance of HB+ protocol. They proposed a new protocol called HB-MP [11]. HB-MP protocol uses two secret keys x and y. Each round authentication uses the i^{th} bit of y to simultaneously rotate x by the tag and the reader. If the tag or the reader cannot finish the updating of the key x and it is easy to result in the synchronization problem between the tag and the reader. Otherwise, for one complete authentication, 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, then x will be rotated $p \times k$ times and x_m will be rotated back to its initial value. A repeated x_m is generated, where x_m is the m-bit binary vector consisting of the m least significant bits of x. To solve the problem, in 2008, Xuefei Leng *et al.* proposed HB-MP+ protocol and gave the abstract description of this protocol [12]. This protocol uses an one-way function to randomize the rotation of the key x and to make the change of the key x unpredictable. This scheme avoids the repeated occurring of round key, but the use of the one-way function increases the complexity of the protocol and it takes much time to find another vector b which equals a. Like HB+ protocol, HB-MP+ protocol has to run many rounds and there are still too much data to be transmitted for each authentication. The transmission cost is too heavy for current low-cost RFID systems. When the challenge vector a is tampered the calculation of the key x_s of the tag and the reader is not synchronous. So HB-MP+ has the synchronization problem. Otherwise, HB-MP+ protocol did not indicate how to calculate the threshold t.

In 2008, Henri Gilbert, Matthew J. B. Robshaw and Yannick Seurin proposed their analysis on HB protocol families, and proposed a new protocol called RANDOM-HB# and its optimized version HB#[13]. RANDOM-HB# avoids many practical drawbacks of HB+ protocol and it is also provably resistant to a broader class of active attacks. However, RANDOM-HB# is required to store two random matrices as the secret keys X and Y, which need the heavy storage costs for the tags. HB# enhanced RANDOM-HB# by using Toeplitz matrices to improve the performance. But later Khaled Ouafi *et al.* [14] presented an effective attack against Random-HB# and HB#, where the adversary is given the ability to modify all messages by eavesdropping the sessions between the reader and the tag. They proved that both Random-HB# and HB# are vulnerable against this kind of man-in-the-middle attack.

There are still new versions in the HB family protocols. Ghaith Hammouri and Berk Sunar used a physical unclonable function to propose PUF-HB protocol [15]. But they did not give any proof of security against man-in-the-middle attacks. Julien BRINGER and Herv´e CHABANNE improved HB+ protocol and proposed Trusted-hb protocol to achieve resistance against man-in-the-middle attacks [16]. But D. Frumkin and A. Shamir constructed several complicated attacks and showed why Trusted-hb protocol cannot be trusted [17].

The protocols described above retain some of the successful properties of HB protocol, and enhance the ability of HB or HB+ protocols against attacks, and improve their secure

performances. But the integrity of the session messages between the tag and the reader is not protected. Tags or readers do not know whether their received messages are tampered. Hence the adversary has a chance to impersonate legitimate tags or readers to send some counterfeiting messages. If some measurements are taken to assure the integrity of the exchanged messages the man-in-the-middle attacks will be prevented effectively.

3. The Improvement of HB+ Protocol for C-1 G-2 RFID Tags

By analyzing above it is observed obviously that if an attacker can slightly modify or tamper the exchanged messages between the tag and the reader the authentication results will be disturbed seriously. This may result in the authenticating failure and even the reveal of the secret keys in tags. So it is very important to prevent these exchanged messages to be modified or tampered. The C-1 G-2 RFID tags provide an on-chip CRC function and this function can assure the integrity of the messages. Therefore, by utilizing CRC function to the challenges and responses of HB+ protocol the drawback of this protocol can be overcome effectively. Therefore, we propose an improved HB+ protocol on the base of the C-1 G-2 RFID tags, which is simply called IHB+ protocol. Because HB+ protocol has an elegant secure property, our work is concerned with its practicality and not its proofs of security. But it is obvious that IHB+ protocol is stronger than HB+ protocol on the security and privacy.

For some scenarios with frequent active attacks, the initial several rounds of HB+ protocol may be attacked frequently to make the probabilistic distribution of the authentication results lose its regularity so that the authentication fails frequently, which means that DOS attack occurs. It is obvious that HB+ protocol is not suitable to some scenarios with frequent active attacks. On the base of the simplicity of HB+ protocol and the on-chip computing resource of EPCglobal C-1 G-2 tags, we propose a detection-exit-restart mechanism to improve HB+ protocol. The mechanism monitors the sessions between the tag and the reader. Once it finds the sessions are tampered it exits and starts next round authentication. Hence the mechanism can find active attacks as early as possible and avoid the further meaningless authenticating rounds so as to improve the authenticating efficiency.

Supposed each tag shares its secret keys x and y, CRC function: $CRC()$ and pseudorandom generator: $PRNG()$ with the reader. Before the sender(a tag or a reader) sends the message to the receiver it will generate the signature of the message by CRC function and the secret keys. Then the message and its signature are sends to the receiver together. Therefore the receiver can detect whether the message is tampered when it receives the message. At the last step of the proposed IHB+ protocol, z is sent to the reader after it is signed by CRC function, the secret keys, a and b. IHB+ protocol is also a r round protocol, which is shown in Figure 5, and the used symbols during authenticating process are listed in Table 1. One round of this protocol is described as follows:

Step 1: tag to reader

The tag calls the pseudorandom generator, PRNG(), to generate a k-bit random binary vector b. Then it calls $CRC()$ to generate the signature of b, $m1=CRC((x \oplus y)||b)$. The tag sends $b||m1$ to the reader.

Step 2: reader to tag

After the reader receives $b||m1$ it uses the same CRC function, $CRC()$, to calculate $m1' = CRC((x \oplus y)||b)$. Then it compares m1' with m1. If they are not equal the authentication fails. Otherwise the reader calls the pseudorandom generator, $PRNG()$, to generate another k-bit random binary vector a. Then it calls the same CRC function as the tag to calculate the signature of a, $m2= CRC((x \oplus y)||a)$. The reader sends $a||m2$ to the tag.

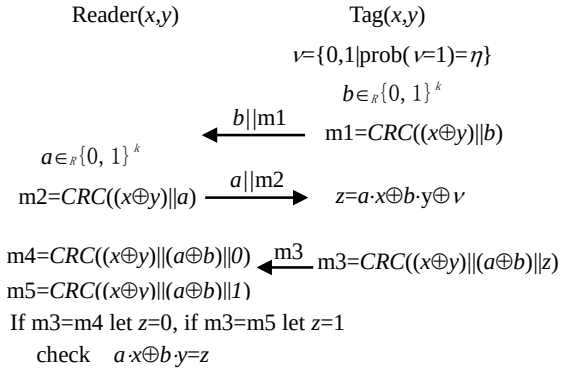

Figure 5. The Diagram of One Round for the IHB+ Protocol

Table 1. The Related Symbols for the IHB+ Protocol

Notation	Description
a,b	k-bit random binary vector
x,y	secret key shared by the tag and the reader
PRNG()	the pseudorandom generator
CRC()	CRC function
⊕	XOR operator
||	concatenation operator

Step 3: tag to reader

After the tag receives *a*||m2 it calls its CRC function to calculate m2'= *CRC*((*x*⊕*y*)||*a*). Then the tag compares m2 with m2'. If they are not equal then the authentication fails. Otherwise, the tag computes $z=x\cdot a \oplus y\cdot b \oplus \nu$ and m3=*CRC*((*x*⊕*y*)||(*a*⊕*b*)||*z*) and it sends m3 to the reader, where ν is a noise bit and the probability η of $\nu=1$ is $\eta\in(0,1/2)$.

Step 4: reader

The reader receives m3, then it computes m4= *CRC*((*x*⊕*y*)||(*a*⊕*b*)||*z*), where z is 0, and m5=*CRC*((*x*⊕*y*)||(*a*⊕*b*)||*z*), where z is 1. The reader compares m3 with m4 and m5 respectively. If they are not equal the authentication fails. Otherwise, z is set to 0 when m3=m4 or z is set to 1 when m3=m5. Then the reader calculates $x\cdot a \oplus y\cdot b$ and it checks whether the result is equal to *z*. If they are equal the current round authentication returns "accept". If not "reject" is returned. Then the authentication enters next round

Once a tag or a reader finds out the sessions to be tampered it terminates the current authentication and start next new authentication. After all *r* rounds of IHB+ protocol are completed, the number of $x\cdot a \oplus y\cdot b$=z is more than $r\eta$ then the authentication successes, if not the authentication fails.

4. Analyzing for the Privacy and Security of IHB+ Protocol

IHB+ protocol is proposed on the base of HB+ protocol and it can resist against active attacks such as man-in-the-middle attacks. It can prevent the leakage of its secret keys effectively by protecting the integrity of the exchanged messages. At the last step of IHB+ protocol the signature of *z* is transferred so as to avoid to be tampered. So IHB+ protocol has the stronger security than HB+ protocol and it is very suitable to some scenarios with frequent active attacks.

- Resist passive attacks

Assume that a passive adversary is able to eavesdrop the communication between the tag and the reader, it can get all challenges and their responses. To get the secret *x* and *y*,

the attacker has to work out the LPN problem, but it is NP-hard. Thus the probability that an adversary can reveal the secret keys is as the same as that in HB or HB+ protocol. So IHB+ protocol is secure against passive attacks.

- Resist active attacks such as man-in-the-middle attacks

Supposed an adversary is able to eavesdrop the exchanged messages between the tag and the reader, it can tamper, terminate and replay these messages. Its goal is to reveal the secret keys of tags so that he can disguise a legitimate tag to get the authentication from the reader. But each challenge or response is simultaneously sent with its signature information. Once these messages are tampered the protocol can detect the change quickly and terminate the current authentication. So it is impossible for the adversary to reveal the secret keys of tags.

- Data confidentiality and privacy

Based on the discussion above, no matter what types of adversary(passive or active) attacks the proposed protocol, secret key x and y in our protocol cannot be revealed. Thence the proposed protocol confirms the confidentiality of data.

- Data integrity

As it is observed, for HB family protocols, there is no way to check whether the exchanged messages were tampered. But in our proposed protocol, if the exchanged messages are tampered, the authentication protocol can find out the changes in time and terminate itself. Thence data integrity is assured.

- Resist desynchronized attacks

In order to enhance the difficulty to reveal the secret keys some HB family protocols change their secret keys for each round authentication, which makes these protocols vulnerable to desynchronized attacks. For our proposed protocol the secret keys are fixed so desynchronized attacks are resisted.

Table 2 shows the summary on the security aspects of several typical HB family protocols and our proposed protocol for some scenarios with frequent active attacks [6,18].

Table 2. The Comparison of the Different Authentication Protocols for Some Scenarios with Frequent Active Attacks

protocol	passive attacks	active attacks	confidentiality	integrity	desynchronized attacks	efficiency
HB	yes	no	no	no	yes	low
HB+	yes	no	no	no	yes	low
HB-MP	no	no	no	no	no	low
HB-MP+	yes	yes	yes	no	no	low
IHB+	yes	yes	yes	yes	yes	high

5. Conclusion

It is obvious that IHB+ protocol retains the simplicity of HB family protocols and inherits their advantages. It is at least as secure as HP+ protocol. For HB+ protocol, it has to run all r rounds for each authentication, whether it is normal or abnormal. It cannot sense the attacks as early as possible to terminate the current meaningless authentication. So it will taste much time. But IHB+ protocol can sense the active attacks as quickly as possible, and it can terminate the current invalid authentication in time and start next authentication. IHB+ protocol is very suitable for some scenarios with frequent active attacks and it has higher efficiency than HB+ protocol or its variants. IHB+ protocol only uses CRC function embedded in tags and it is suitable for low-cost tags.

Acknowledgements

We are appreciated to anonymous reviewers for their constructive suggestion to this paper. The relative work about this paper is supported by National Natural Science Foundation of China (No. 61272097), the Science and Technology Innovation Project of Shanghai Education Committee (No. 12ZZ182).

References

[1] A. N. Nambiar, "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science, vol. 2, (**2009**) October 20-22; San Francisco, USA.
[2] A. Juels, "RFID Security and Privacy: A Research Survey", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 24, no. 2, (**2006**), pp. 381-394.
[3] S. E. Sarma, S. A. Weis and D. W. Engels, "Radio-frequency Identification: Secure risks and challenges", RSA Laboratories Cryptobytes, vol. 6, no. 1, (**2003**), pp. 2-9.
[4] L. Gao, M. Ma, Y. Shu and Y. Wei, "An Ultralightweight RFID Authentication Protocol with CRC and Permutation", Journal of Network and Computer Applications, vol. 10, (**2013**), pp. 1-20.
[5] N. J. Hopper and M. Blum, "Security Human Identification Protocols", Advances in Cryptology-ASIACRYPY, LNCS, vol. 2248, (**2001**), pp. 52-66.
[6] Z. Lin and J. S. Song, "An Improvement in HB-Family Lightweight Authentication Protocols for Practical Use of RFID System", Journal of Advances in Computer Networks, vol. 1, no. 1, (**2013**), pp. 61-65.
[7] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols", Advances in Cryptology-Crypto2005, LNCS, vol. 3621, (**2005**), pp. 293-308.
[8] H. Gilbert, M. Robshaw, and H. Silbert, "An Active Attack against HB+: a Provably Secure Lightweight Authentication Protocol", ELECTRONICS LETTERS, vol. 41, (**2005**), pp. 1169-1170.
[9] H. Gilbert, M. Robshaw, and Y. Seurin, "Good Variants of HB+ Are Hard to Find", Financial Cryptography and Data Security, LNCS, vol. 5143, (**2008**), pp. 156-170.
[10] J. Bringer, H. Chabanne and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attack", Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06), (**2006**) June 29; Lyon, France.
[11] J. Munilla and A. Peinado, "HB-MP: A Future Step in the HB-family of Lightweight Authentication Protocols", Computer Networks, vol. 51, (**2007**), pp. 2262-2267.
[12] X. Leng, K. Mayes and K. Markantonakis, "HB-MP+ Protocol: An Improvement on the HB-MP Protocol", Proceedings of IEEE International Conference on RFID, (**2008**) April 16-17; Las Vegas, Nevada, USA.
[13] H. Gilbert, M. J. B. Robshaw, and Y. Seurin, "HB#: Increasing the Security and Efficiency of HB+, Nigel P. Smart, editor", Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, (2008)April 13-17; Istanbul, Turkey, LNCS, 4965, (**2008**), pp. 361-378.
[14] K. Ouafi, R. Overbeck and S. Vaudenay, "On the Security of HB# against a Man-in-the-Middle Attack", Josef Pieprzyk, editor, Advances in Cryptology - ASIACRYPT 2008, LNCS, vol. 5350, (**2008**), pp. 108-124.
[15] G. Hammouri and B. Sunar, "PUF-HB: A Tamper-resilient HB Based Authentication Protocol", Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors. The 6th International Conference on Applied Cryptography and Network Security-ACNS 2008, (2008) June 3-6; New York, NY, USA, LNCS, vol. 5037, (**2008**), pp. 346-365.
[16] J. Bringer and H. Chabanne, "Trusted-hb: A Low-cost Version of hb+ Secure Against Man-in-the-middle Attacks", IEEE Transactions on Information Theory, vol. 54, no. 9, (**2008**), pp. 4339-4342.
[17] D. Frumkin and A. Shamir, "Un-trusted-hb: Security vulnerabilities of Trusted-hb", In Workshop on RFID Security (RFIDSec), (**2009)**.
[18] C.-M. Lin, S.-C. Tsaur, Y.-C. Chen and I.-C. Lin, "HB Family RFID Mutual Authentication Protocol", The 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (**2011**) October 14-16; Dalian, China.

Authors

Zhicai Shi, he received his Ph.D. degree from Zhejiang University, China. He is currently the Professor of School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, China. His research aims to create novel technologies for network analysis and RFID authentication. He is the author of 7 books, more than 80 publications in journals and conferences.

Fei Wu, he received his Ph.D. degree from National University of Defense Technology, China. He is currently the Professor of School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, China. His interests are distributed computing system and information intelligent processing.

Yongxiang Xia, he received his M.S. degree from Donghua University, China. He is currently the associate professor of School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, China. His research interest is network and information security. He is the author of 4 books, more than 20 publications in journals and conferences.