International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 2, March - April 2016 **ISSN 2278-6856**

A lightweight RFID authentication protocol based on Rabin cryptosystem

Zhicai Shi

School of Electronic&Electrical Engineering, Shanghai University of Engineering Science Shanghai 201620, China

Abstract

RFID is an important technology that can be used to create the ubiquitous society. An RFID system uses open radio wave to transfer information and this leads to pose a serious threat to its privacy and security. The current mainstream RFID tags are some low-cost passive tags. They usually have very limited computing and memory resources and this makes it difficult to solve their security and privacy problems. Lightweight authentication protocols are considered as an effective approach to assure the security and privacy of the low-cost RFID systems. Some typical authentication protocols usually use Hash functions so that they require more computing and memory resources. Rabin cryptosystem is a simple encryption function and it needs less computing and memory resources than Hash functions. Based on Rabin cryptosystem, we propose a lightweight authentication protocol. This protocol provides forward security and it can prevent information leakage, location tracing, eavesdropping, replay attack, spoofing, and DOS-attack effectively. It is very suitable to some low-cost RFID systems.

Keywords: RFID, Authentication protocol, Security and privacy, Rabin cryptosystem

1. INTRODUCTION

With the development of Internet of Things(IoT), Radio Frequency IDentification(RFID) technique gets the broad attention. RFID is a pervasive technology deployed in everyday life in order to identify objects using radio-waves, without visible light and physical contact. Today, the RFID system has been successfully applied to manufacturing, supply chain management, agriculture, transportation, healthcare, electronic-payment, e-passport and other fields[1]. But, RFID is simple and it uses wireless wave to communicate. It has very limited computing and memory resources. So it is easy to be attacked. Some malicious competitors can collect unprotected RFID information and use forgery tags to provide some wrong information, or even launch denial of service attacks against the RFID system. Once the RFID system are broken through the user's privacy will be leaked and their security will be threaten. To protect the private information on the RFID tag, some special techniques are used to prevent malicious readers from accessing the tag. Currently, these techniques are divided into two main categories: physical approaches, encryption mechanism and protocols[2-3]. Some recent research results indicate that encryption mechanism and protocol is a more flexible and effective approach for ensuring the security and privacy of the RFID system. The lightweight authentication is such a special encryption protocol. Now, many lightweight authentication protocols have been proposed. But they usually use some complicated functions(e.g. Hash function) and they need more computing and memory resources. In order to satisfy such special requirement as RFID we use Rabin cryptosystem to propose a lightweight authentication protocol. Our protocol assures forward security and it can prevent information leakage, location tracing, eavesdropping, DOS attack and replay attack. This protocol only needs less computing and memory resources than Hash functions. So it is very suitable for the low-cost RFID system.

2. THE RFID SYSTEM, ITS SECURITY AND PRIVACY

A RFID system consists of three components: Radio Frequency(RF) tags, RF readers and a backend server[4], as shown in Figure 1. A tag is basically a silicon chip with antenna and a small memory that stores its unique identifier known as EPC(electronic product code). A reader is a device capable of sending and receiving data in the form of radio frequency signal. This device is basically used to read EPC from the tag and to send it to the backend server. A backend server is used to store the information related to the objects being tagged by the RFID tag and cooperates with reader to finish managing and displaying the information about the tag.

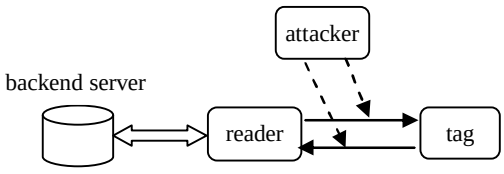

Figure 1 The components of an RFID system

For an RFID system, a tag is a special device. Its computing and memory resource is very limited. There are two types of tags: active tag and passive tag. Active tags include miniature batteries used to power the tag and they are capable to transmit data over longer distance. The other is passive tag which does not have a battery, it needs to be activated by the RF signal beamed from the reader. Passive tags are smaller, less expensive and used for a shorter range. Passive tags have become the mainstream

tags because they are very cheap. In general, conventional cryptographic protocols can be effectively implemented on backend server and reader because they are resource-abundant. It is usually assumed that the channels between backend server and reader are secure. However, because of the limited resources in tag and the open wireless communication between tag and reader it has to assume that the channel between tag and reader is insecure. Most secure problems of the RFID system are resulted from the insecure channel. These secure problems involve forward security, information leakage, location tracing, eavesdropping, DOS attack and replay attack[5].

3.THE RELATED RFID AUTHENTICATION PROTOCOLS

An RFID authentication protocol is a special cryptographic protocol where resource-constrained RFID tags are involved. This kind of protocol is called as the lightweight authentication protocol. For this case, conventional authentication protocols that concern public key computations or even symmetric key computations are not applicable.

Many research works have been done for RFID authentication and they use the one-way property of Hash function to protect the security and privacy of the RFID system. But most of them have serious security problems. Such classical authentication protocols are Hash-Lock protocol, Randomized Hash-Lock protocol, Hash-chain protocol, and so on.

Sarma proposed Hash-Lock protocol which attempts to provide mutual authentication and uses a pseudonym: metaID to replace the actual tag's ID to keep its privacy[6,7]. During the authenticating process the plaintext of the tag's ID is transferred and metaID is invariable. So an adversary easily compromises mutual authentication by simply eavesdropping and replaying these messages communicated between tag and reader. Moreover, the tag's holder is easily traced by an adversary because of its invariable metaID.

Randomized Hash-Lock protocol is proposed by Weis et al. which uses the pseudorandom number generator (PRNG) to randomize the messages transferred between tag and reader[5]. In this protocol, the tag's ID is also transferred by plaintext and it is easy to be eavesdropped. Hence, it is vulnerable to spoofing attack and replay attack. Once the tag's ID is intercepted the tag's holder is easily traced.

Ohkubo et. al. proposed Hash-chain protocol[8]. It uses two different Hash functions H( ) and G( ). This protocol provides one-way authentication. It is also vulnerable to spoofing and replay attack. This protocol uses two different Hash functions and this makes it not suitable to the low-cost RFID system.

Lee et. al. proposed an authentication protocol for RFID system, Semi-Randomized Access Control (SRAC)[9]. It also uses a pseudonym, MetaID, to replace the tag's ID like Hash-Lock protocol. It provides mutual authentication, forward security and it can protect the RFID system from many attacks, such as tracing, cloning and denial of service. However, it is vulnerable to replay attack. The adversary can simply eavesdrop and reuse *MetaID* to be authenticated successfully. Later, Lee et. al. proposed another protocol(LCAP)[10]. This protocol provides mutual authentication and guarantees the location privacy of tag's holder. It also provides untraceability by changing the tag's identification dynamically. Nevertheless, it does not provide forward security.

Cho et al.[11-12] proposed a new Hash-based authentication protocol to solve the security and privacy problems for the RFID system. However, Kim et al.[13] demonstrated that this protocol is vulnerable to DOS attack. He pointed out that Cho et al.'s protocol is vulnerable to traffic analysis and tag/reader impersonation attacks. An adversary can impersonate a valid tag or reader with probability *1/4*. Finally, an adversary can obtain some information about the secret values of the tag in the next session with probability *3/4*.

As described above, many lightweight RFID authentication protocols use Hash functions. It seems to be the best choice to use Hash function to protect the security and privacy of the RFID system. Unfortunately, these Hash functions are primarily designed to be collision resistant in order to prevent forgery of digitally signed documents. Collision resistant is a very difficult requirement and makes these functions too complicated for the RFID tag[14]. So it is necessary to choose a dedicated one-way function more suitable for RFID applications, which are not necessarily collision resistant.

4.AN RFID AUTHENTICATION PROTOCOL BASED ON RABIN CRYPTOSYSTEM

The authentication protocol usually uses some encryption functions to protect the secrecy and privacy of the RFID system. In general, the functions should be some one-way functions, but not necessarily some collision-resistant Hash functions since a collision is not a security threat in the RFID authentication. Rabin cryptosystem is such an excellent function as described above. After Rabin cryptosystem is optimized it requires less computing and memory resources than Hash functions[14-15]. Rabin Cryptosystem is described as follows:

Supposed m is a message and it is sent after it is encrypted by computing the ciphertext $c = m^2 \pmod{k}$. k is the secret key and it is the product of two unknown prime factors p and q, $k=pq$. $c = m^2 \pmod{k}$ is an excellent one-way function, but definitely not a collision resistant function. Now we take the challenge-response mechanism and use this function to construct a lightweight authentication protocol suitable for the low-cost RFID system.

Supposed *ID* is an identifier of the tag and it only identifies a tag. *L* is the length of the secret key *k*. *ID-new* and *k-new* are the values of *ID* and *k* which are used in the current authentication process. *ID-old* and *k-old* are the

values of *ID* and *k* which are used in the last authentication process.

The authentication process of our proposed protocol is described as follows:

(1)Key generation

Randomly choose two large Blum primes *p* and *q*, and compute $k=pq$. The public key is thus the modulus *k*, while the private key consists of its factorization (*p*, *q*).

(2)The initialization of the tag and reader/server

Before the authentication begins, ID and k are stored in the tag. ID-new, ID-old, k-new and k-old are stored in the server/reader. ID-new=ID-old=ID, k-new=k-old=k. The server/reader and the tag can call Rabin cryptosystem and the pseudorandom number generator f( ). Otherwise, they can call two other functions as follows:

high(x): its value is the high *L* bits of *x*.

low(x): its value is the low *L* bits of *x*.

(3)The mutual authentication

The authentication protocol is shown in Figure 2 and it is described as follows:

1. reader/server to tag

The reader/server calls the pseudorandom number generator *f( )* to generate a random number *r1* and it constructs the message $m1=r1||challenge$. It sends the message *m1* to the tag.

2. tag to reader/server

After the tag receives the message $r1||challenge$ it calls the pseudorandom number generator *f( )* to generate another random number *r2*. Then the tag uses Rabin cryptosystem to generate some messages as follows:

$$m2=(ID\oplus r1)||r2)^2 \bmod k \quad (1)$$
$$m3=(ID\oplus r2)||r1)^2 \bmod k \quad (2)$$

The tag constructs the message $m6=m4||r2$ and sends *m6* to the reader/server.

3. reader/server to tag

After the reader/server receives m6 from the tag and it abstracts m4. Then it calculates m4' and m5' for (ID, k)$\in${(ID-new, k-new), (ID-old, k-old)} by the following equations:

$$m2'=(ID\oplus r1)||r2)^2 \bmod k \quad (5)$$
$$m3'=(ID\oplus r2)||r1)^2 \bmod k \quad (6)$$
$$m4'=high(m2')||low(m3') \quad (7)$$
$$m5'=low(m2')||high(m3') \quad (8)$$

First, (ID-new, k-new) is used to replace (ID, k) in the equation (5) and the equation (6). Then it will get m4'. If m4' equals m4 in the message m6 the authentication of the reader/server to the tag succeeds. If m4' does not equal m4 (ID-old, k-old) is used to replace (ID, k) in the equation (5) and the equation (6), it will get another m4'. If m4' equals

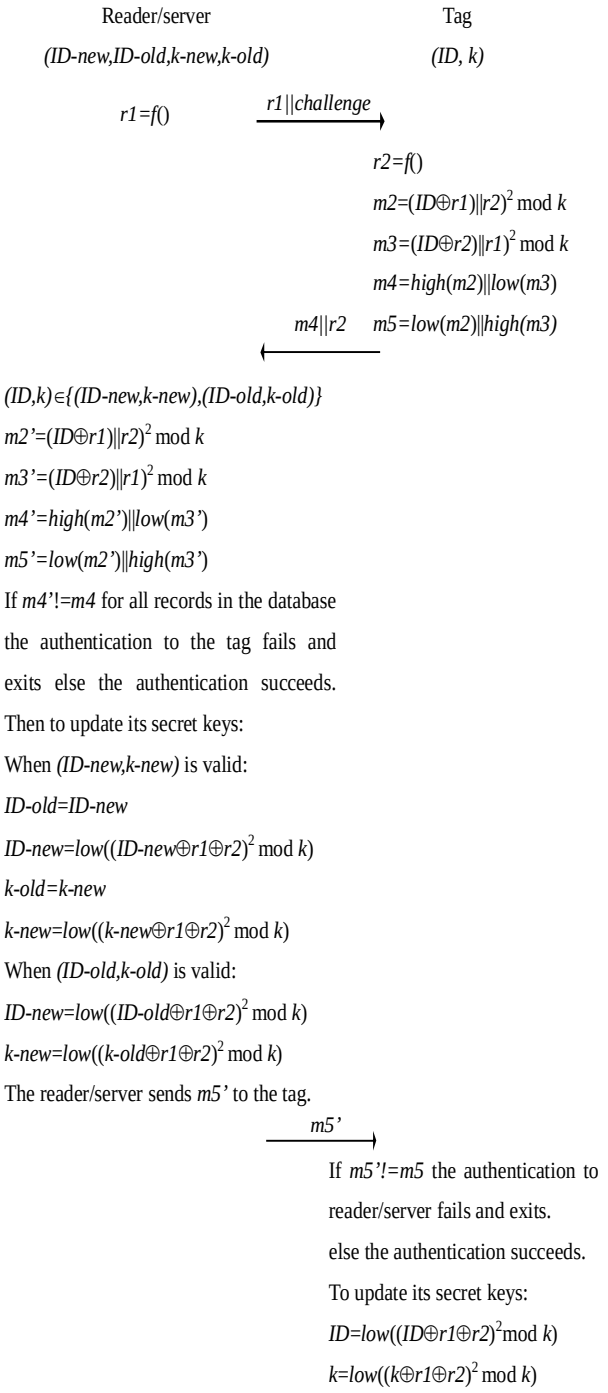

Figure 2 The diagram of our proposed protocol

m4 the authentication of the reader/server to the tag succeeds. If m4' dose not equal m4 for each {(ID-new, k-new), (ID-old, k-old)} the authentication to the tag fails and the RFID system exits.

If the authentication to the tag succeeds the reader/server sends the message m5' to the tag. Then it begins to update its secret information.

When (ID-new, k-new) is used for the current successful authentication the reader/server begins to update its secret keys as follows:

$$ID\text{-}old=ID\text{-}new$$
$$ID\text{-}new=low((ID\text{-}new\oplus r1\oplus r2)^2 \bmod k)$$

$k\text{-}old = k\text{-}new$
$k\text{-}new = low((k\text{-}new \oplus r1 \oplus r2)^2 \bmod k)$

When *(ID-old, k-old)* is used for the current successful authentication the tag begins to update its secret keys as follows:

$ID\text{-}new = low((ID\text{-}old \oplus r1 \oplus r2)^2 \bmod k)$
$k\text{-}new = low((k\text{-}old \oplus r1 \oplus r2)^2 \bmod k)$

- **tag:**

After the tag receives the message *m5'* from the reader/server it compares *m5* with *m5'*. If they are not equal the authentication to the reader/server fails and the RFID system exits. Otherwise the tag successfully completes the authentication to the reader/server and it begins to update its secret keys as follows:

$ID = low((ID \oplus r1 \oplus r2)^2 \bmod k)$
$k = low((k \oplus r1 \oplus r2)^2 \bmod k)$

5. THE SECURITY ANALYSIS OF THE PROPOSED PROTOCOL

Our proposed protocol only uses Rabin cryptosystem, not Hash function, to encrypt all sessions during the authentication process so as to assure the confidentiality and privacy of the RFID system. All sessions are randomized by different random numbers and the freshness of the sessions is assured. After each authentication is finished all secret information are updated. So our proposed authentication protocol can assure the privacy and forward security of the RFID system, and it can prevent eavesdropping attack, tracing attack, replay attack and de-synchronized attack. Now we analyze the security of the proposed authentication protocol.

- Eavesdropping: During the authentication process, all messages transferred between tag and reader are encrypted by Rabin cryptosystem. Attackers can intercept all sessions between tag and reader. But they cannot decrypt them and they cannot get any useful information about the tag from their intercepted data. Eavesdropping to the communication between tag and reader is invalid. The privacy of the RFID system is protected.
- Tracing attack: If a tag is traced the privacy of the holder's location may be encroached upon. To prevent this type of attack, a pseudorandom generator is used to assure that each session between tag and reader is variable so as to make attackers not to distinguish where their received data is sent from.
- Replay attack: This type of attack means to re-send data acquired by eavesdropping to compromise the RFID system. In order to prevent replay attack each authentication generates a different pseudorandom number to randomize sessions between tag and reader. If an attacker re-sends his received message in the late authentication process this message has not any meanings because new authentication uses a new pseudorandom number.
- Forward security: This security means that although attackers reveal the current secret key they cannot discover any useful information from previous sessions. In order to provide forward security, the secret information stored in reader/server and tag are updated after each authentication is finished. Although attackers can get the secret information for the current authentication they cannot decrypt the previous sessions. Because the secret keys of the RFID system have been changed. Attackers cannot guess the tag's past behaviors.
- Spoofing: The protocol ensures the user's anonymity and privacy by using Rabin cryptosystem to encrypt all messages exchanged between reader and tag. An attacker cannot get the identity information of a tag or reader, so it cannot impersonate a valid tag or reader.
- De-synchronized attack: De-synchronization attack means the backend server/reader and the tag cannot update their secret keys synchronously so that they possess different secret keys. This makes future authentication impossible. Our proposed protocol stores *ID-old* and *k-old* in the backend server. *ID-old* and *k-old* are the values of *ID* and *k* for the last successful authentication. If the tag cannot synchronously update its secret information the backend server can use *ID-old* and *k-old* to complete the authentication so as to resist against de-synchronization attack.

The comparison of the proposed protocol with some typical Hash-based authentication protocols is listed in Table 1.

Table 1: The comparison of the different protocols

Protocols	eaves-dropping	tracing attack	replay attack	forward security	spoofing
Hash-Lock	x	x	x	x	x
Randomized Hash-Lock	x	x	x	x	x
Hash-chain	√	√	x	√	x
SRAC	√	√	x	√	√
LCAP	√	√	√	x	√
The proposed protocol	√	√	√	√	√

6. CONCLUSIONS

The RFID systems based on low-cost passive tags are some typical resource-constrained systems and their computing and memory resources are very limited. So some lightweight authentication protocols have to be proposed to meet the special requirements of the RFID systems. Our proposed protocol uses Rabin cryptosystem, which is simpler and needs less computing and memory resources than Hash function, to encrypt all sessions between tag and reader/server. This assures the confidentiality and privacy of the RFID system. At the same time, our proposed protocol uses random numbers to randomize the sessions between tag and reader so as to

assure their freshness. The secret key of the last successful authentication is kept so as to resist against de-synchronized attack. After each successful authentication the secret key is updated in time for assuring forward security. So our proposed protocol can resist against eavesdropping, tracing attack, replay attack, de-synchronized attack. It only uses Rabin cryptosystem and a pseudorandom generator. Rabin cryptosystem is simple and its completeness only needs less computing and memory resources. So our proposed protocol is very suitable for the low-cost FRID system.

References

[1]. A. Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, 24(2), pp.381-39, 2006

[2]. P. Peris-Lopez, J. C. Hemandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, "RFID systems: A Survey on Security Threats and Proposed Solutions," Lectures Notes in Computer Science, Vol.4217. pp. 159-170, 2006.

[3]. Arun N. Nambiar, "RFID Technology: A Review of its Applications," In Proceedings of the World Congress on Engineering and Computer Science, Vol. II, San Francisco, USA, pp. 1-7, 2009.

[4]. Soo-Young Kang, Deok-Gyu Lee, Im-Yeong Lee, "A Study on Secure RFID Mutual Authentication Scheme in Pervasive Computing Environment," Computer Communications, Vol.31, pp. 4248-4254, 2008.

[5]. S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," In Proceedings of the 1st International Conference on Security in Pervasive Computing, pp. 201-212, 2004.

[6]. S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications," In Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. pp. 454-469, 2003.

[7]. S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-frequency Identification: Secure Risks and Challenges," RSA Laboratories Cryptobytes, pp. 2-9, 2003.

[8]. M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain Based Forward Secure Privacy Protection Scheme for Low-cost RFID," In Proceedings of the 2004 Symposium on Cryptography and formation Security, pp. 719-724, 2004.

[9]. Yong Ki Lee, Ingrid Verbauwhede, "Secure and Low-cost RFID Authentication Protocols," In Proceedings of the 2nd IEEE Workshop on Adaptive Wireless Networks, pp. 1-5, 2005.

[10]. Su Mi Lee, Young Ju Hwang, Dong Hoon Lee, Jong In Lim, "Efficient Authentication for Low-Cost RFID Systems," Lecture Notes in Computer Science, vol. 3480, pp. 619-627, 2005.

[11]. Cho, Jung-Sik, Yeo, S.S., and Kim, S. K., "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," Computer Communications, 34, pp.391–397, 2011.

[12]. Cho Jung-Sik, Jeong Young-Sik, and Sang Oh-Park, "Consideration on the Brute-force Attack Cost and Retrieval Cost: A Hash-based Radio-frequency Identification (RFID) Tag Mutual Authentication Protocol," Computers and Mathematics with Applications. 8, pp.1-8, 2012.

[13]. Kim, H., "Desynchronization Attack on Hash-based RFID Mutual Authentication Protocol," Journal of Security Engineering, 9(4), pp.357–365, 2012.

[14]. Shamir A. "SQUASH-A new MAC with provable security properties for highly constrained devices such as RFID tags," In Proceedings of Fast Software Encryption, pp.144-157, 2008.

[15]. Gosset F,Standaert F X,Quisquater J J, "FPGA implementation of SQUASH," In Proceedings of the 29th Sysp on Information Theory in the Benelux, pp.1-8, 2008.

AUTHOR

Zhicai Shi 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 some novel technologies for network security analysis and RFID authentication.