A Strong RFID Authentication Protocol with Confidentiality and Anonymity for EPCglobal Class-1 Gen-2 Tags

Zhicai Shi, Yihan Wang, Changzhi Wang, Shitao Ren

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

szc1964@163.com

Keywords: RFID, Authentication protocol, CRC, Security and Privacy

Abstract. RFID systems are some typical resource constraint systems and lightweight authentication is considered as one effective method to ensure their security and privacy. The EPCglobal Class-1 Gen-2 tags are popular RFID tags and this kind of tags has some on-chip computing resources. Based on these on-chip resources, a lightweight authentication protocol is proposed. The protocol ensures the integrity and freshness of the sessions among RFID systems by means of *CRC()* and pseudorandom number generator. The protocol uses concatenation operation to overcome the linear drawbacks of *CRC()* and exclusive OR operator. It provides forward security and it can resist against eavesdropping, tracing, replay and de-synchronization attack. It completes the strong authentication to tag by twice authentication. This protocol only uses the computing resources embedded in tags and it is very suitable to low-cost RFID systems.

Introduction

Radio Frequency IDentification(RFID) technique is a pervasive technology and it uses the wireless radio signals to identify objects, without visible light and physical contact. Today, RFID systems have been successfully applied to manufacturing, supply chain management, agriculture, transportation and other fields[1]. But RFID tags only have limited computing resources and they use open wireless wave to communicate. It is easy for an adversary to attack RFID systems. The research shows that software encryption and authentication is the most flexible and effective method to solve the security problems of RFID systems. So many lightweight authentication protocols have been proposed to suit for the special environment of RFID systems. Some typical protocols use the one-way property of Hash function to ensure the confidentiality and anonymity of RFID systems[2-3]. But Hash function usually costs more computing resources. EPCglobal Class-1 GEN-2 RFID tags, which is simply called the C-1 G-2 tag, is the most popular low-cost tags. The tags provide pseudorandom number generator and CRC function. Some protocols use these functions to complete the authentication for RFID systems. But they still have some secure drawbacks[4-5]. Now, we propose an authentication protocol by means of CRC function in the C-1 G-2 tags, not Hash function. Our protocol can resist against the common attack and it does not require extra computing resources. It can overcome the linear drawback of CRC function and exclusive OR operation. It is very suitable for RFID systems with the C-1 G-2 tags.

The paper is organized as follows. In Section II, the RFID system, its security and privacy model are introduced. In Section III, we propose a strong authentication protocol by means of CRC function in the C-1 G-2 RFID tags. In Section IV, we analyze the security of our proposed protocol. In Section V, we conclude our work and point out the advantages of our proposed protocol.

The RFID System, Its Security and Privacy Model

An RFID system consists of three components: Radio Frequency(RF) tag, RF reader and backend server, as shown in Figure 1. A tag is a silicon chip with antenna and a small storage. There are two types of tags: active tag and passive tag. Active tags include batteries and they are capable to transmit data over longer distance. Passive tags don't have any battery and they are activated by the RF signal from the reader. This kind of tags is very cheap and they are usually called low-cost tags. A reader is a device capable of sending and receiving data in the form of radio frequency signal. This device communicates with tag and reads its identifier. A backend server is used to store the detail information about the tagged objects, and it cooperates with reader to implement the authentication to tag. It searches the information about the tagged objects according to the tag's identifier and sends the information to the reader.

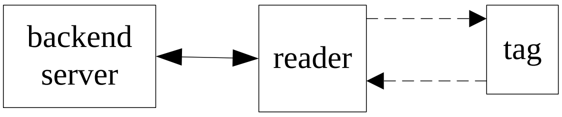


Figure 1. The component of An RFID System

As an important component of RFID systems, the tag usually has very limited computing and storage resources and it is difficult to implement some complicated cryptographic algorithms. But backend server and reader are usually considered to be resource-abundant and they can implement conventional cryptographic protocols. So the channel between backend server and reader is secure and they are usually considered as a single entity, which is called the reader. However, because of the limited resources and the open wireless communication mode the channels between tag and reader are insecure. Most secure problems of RFID systems are resulted from these insecure channels.

As a typical resource constraint system, an RFID system is very vulnerable to some secure threats. Eavesdropping, impersonating, tracing, replay and de-synchronization are some popular secure threats. Otherwise, a secure RFID system must satisfy forward security and anonymity.

A Lightweight RFID Authentication Protocol for C-1 G-2 RFID Tags

A secure RFID system can provide forward security and resist against common attacks. The C-1 G-2 RFID tags provide an on-chip CRC function and this function can ensure the integrity of the sessions between reader and tag. The confidentiality and anonymity communication between reader and tag can be ensured by flexible utilizing CRC function, pseudorandom number generator and bitwise operation. The linear drawback of CRC function and XOR operation is effectively overcome by means of concatenation function.

For our proposed protocol, the tag stores its secret keys *k1* and *k2*. The reader stores the current secret keys of each tag, *k1c* and *k2c*, the secret keys of the last successful authentication, *k1p* and *k2p*. The length of all secret keys is *L* bits. Before the authentication begins, let *k1c=k1p=k1 and k2c=k2p=k2*. The tag and the reader can implement *CRC* function, pseudorandom number generator and bitwise operation. The used symbols in the protocol are listed in table 1. This protocol is shown in figure 2 and it is described as follows:

Table 1. The symbols used in the protocol

Notation	Description
k1,k2	The tag's secret keys
k1c,k1p, k2c,k2p	The current secret keys of all tags and their last secret keys stored in the reader
CRC()	CRC function
r1,r2	Two random numbers generated by the reader and the tag
||	Concatenation operation
⊕	Bitwise XOR operation

(1) reader to tag: The reader generates a pseudorandom number *r1* and a query "*hello*", then it sends *r1||hello* to the tag.

(2)tag to reader: The tag generates a pseudorandom number *r2* and computes *m1=CRC(k1||(r1⊕r2))* and *m2=CRC((k1⊕r1)||r2)*. Then it sends *r2||m1||m2* to the reader.

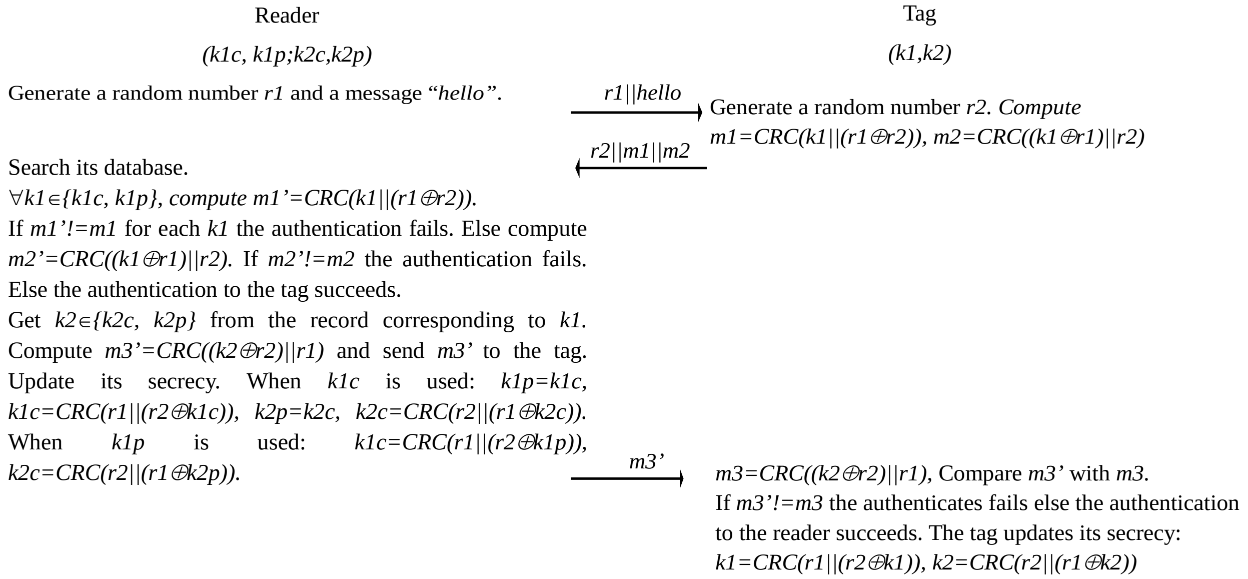
(3)reader to tag: After the reader receives *r2||m1||m2* it searches its database and gets each *k1∈{k1c,k1p}* to compute *m1'=CRC(k1||(r1⊕r2))* . If *m1=m1'* it computes *m2'=CRC((k1⊕r1)||r2)*.

If the result equals $m2$ the reader completes the authentication to the tag. If not, it will get next $k1\in\{k1c,k1p\}$ from the database and repeats the above computation. If $m1!=m1'$ or $m2!=m2'$ for each $k1\in\{k1c,k1p\}$ the authentication to the tag fails.

Once the reader completes the authentication to the tag it computes $m3'=CRC((k2\oplus r2)\|r1)$, where $k2$ is replaced by $k2c$ or $k2p$ depending on $k1$, and sends $m3'$ to the tag. Then it begins to update its secrecy as follows:

When the authentication succeeds $k1c$ is used, let $k1p=k1c$, $k1c=CRC(r1\|(r2\oplus k1c))$, $k2p=k2c$, $k2c=CRC(r2\|(r1\oplus k2c))$. When the authentication succeeds $k1p$ is used, let $k1c=CRC(r1\|(r2\oplus k1p))$, $k2c=CRC(r2\|(r1\oplus k2p))$.

(4)Tag: The tag computes $m3=CRC((k2\oplus r2)\|r1)$ and it compares $m3'$ with $m3$. If they are equal the tag implements the authentication to the reader. If not, the authentication of the tag to the reader fails. If the authentication of the tag to the reader succeeds the tag updates its secret keys: $k1=CRC(r1\|(r2\oplus k1))$, $k2=CRC(r2\|(r1\oplus k2))$.



Generate a random number $r1$ and a message "*hello*".

Generate a random number $r2$. Compute $m1=CRC(k1\|(r1\oplus r2))$, $m2=CRC((k1\oplus r1)\|r2)$

Search its database.
$\forall k1\in\{k1c, k1p\}$, compute $m1'=CRC(k1\|(r1\oplus r2))$.
If $m1'!=m1$ for each $k1$ the authentication fails. Else compute $m2'=CRC((k1\oplus r1)\|r2)$. If $m2'!=m2$ the authentication fails. Else the authentication to the tag succeeds.
Get $k2\in\{k2c, k2p\}$ from the record corresponding to $k1$. Compute $m3'=CRC((k2\oplus r2)\|r1)$ and send $m3'$ to the tag. Update its secrecy. When $k1c$ is used: $k1p=k1c$, $k1c=CRC(r1\|(r2\oplus k1c))$, $k2p=k2c$, $k2c=CRC(r2\|(r1\oplus k2c))$. When $k1p$ is used: $k1c=CRC(r1\|(r2\oplus k1p))$, $k2c=CRC(r2\|(r1\oplus k2p))$.

$m3=CRC((k2\oplus r2)\|r1)$, Compare $m3'$ with $m3$.
If $m3'!=m3$ the authenticates fails else the authentication to the reader succeeds. The tag updates its secrecy: $k1=CRC(r1\|(r2\oplus k1))$, $k2=CRC(r2\|(r1\oplus k2))$

Figure 2. The diagram of the authentication protocol

Security Analysis of Our Proposed Authentication Protocol

Our proposed authentication protocol only uses the on-chip resources of the tag. It costs less computing resources and provides stronger security than some previous typical protocols[2-6]. It can resist eavesdropping, tracing, replay, de-synchronization attack. Moreover, it ensures forward security by means of updating the secret keys after each successful authentication.

- Eavesdropping attack. For our protocol, the secret keys of the tag are not transferred by plaintext. An adversary can eavesdrop and intercept each sessions between tag and reader. But these sessions are processed by *CRC()* after they are randomized. It is very difficult for an adversary to reveal the tag's secrecy from his intercepted sessions. An adversary cannot acquire any useful information by eavesdropping.
- Tracing attack. For each authentication, the tag generates a different pseudorandom number $r2$ and it uses $r2$ to randomize the response, $m1$ and $m2$, to "*hello*" from the reader. So the responses of the tag to the reader are different for each authentication. The reader cannot trace a tag by eavesdropping or intercepting the responses from the tag.
- De-synchronization attack. By analyzing the authentication process of the protocol, it is obviously observed that the tag updates its secrecy if and only if it receives the right message $m3'$ from the reader. Only situation is that the reader has updated its secrecy, but $m3'$ is tampered or blocking by an attacker. Under this case, the reader updates its secrecy and the tag does not. But the

current secret keys of the tag, *k1p* and *k2p*, are still reserved in the reader. They can use these secret keys to complete the later mutual authentication.

- Replay attack. Supposed an adversary is able to eavesdrop and intercept all sessions between tag and reader. An adversary can disguise a legitimate tag to re-send the intercepted sessions to a reader. But for each authentication the tag and the reader generate two different random numbers and use these random numbers to randomize the sessions between them. After each successful authentication the secret keys are updated. If an attacker impersonates a legitimate tag and replays his intercepted sessions he cannot be authenticated by the reader. Because the reader cannot find the matched *m1* and *m2*. So replay attack is prevented effectively.
- Forward security. Forward security means that an adversary cannot reveal the previous sessions even if he gets the current secret keys of RFID systems. For our protocol, the secret keys of RFID systems are updated after each successful authentication. For different authentication process, sessions are generated by different secret keys. Although an adversary can reveal the current secret keys he cannot derive the last secret keys. So he cannot get any useful information from the previous intercepted sessions.
- Data confidentiality and privacy. As described above, our protocol uses a pseudorandom number generator and *CRC()* to randomize and encrypt the secrecy of the tag. An adversary cannot reveal the sessions intercepted by him. It can effectively resist the information leakage. Thence the protocol ensures the confidentiality and privacy of RFID systems.

Summary

It is a great challenge to design a lightweight authentication protocol which is secure and efficient for the low-cost RFID systems. In this paper, we propose a lightweight authentication protocol for the C-1 G-2 RFID tags. The protocol only uses the on-chip resources of the tag. The protocol uses *CRC()* to ensure the integrity of the sessions between tag and reader. It can resist against tracing attack and replay attack by randomizing the sessions. After each successful authentication the tag's secret keys are updated so as to provide forward security. While updating the tag's secrecy the current and last secret keys are reserved so as to resist against de-synchronized attack. So our protocol can provide forward security and it can resist against eavesdropping, tracing, replay and de-synchronized attack. It completes the strong authentication to tag by twice authentication. It only uses the on-chip resources of the tag. So the protocol is suitable for low-cost FRID systems with the C-1 G-2 RFID tags.

References

[1] Pilli-Sihvola Eetu, et. al. The European approach to addressing RFID privacy, International Journal of RFID Technology and Applications, vol.4, no.3(2014), p.260-271

[2] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. Proc. of the 1st International Conference on Security in Pervasive Computing, Boppard, Germany, March 12-14, 2003.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita. Hash-chain Based Forward Secure Privacy Protection Scheme for Low-cost RFID. Proc. of the 2004 Symposium on Cryptography and Information Security, Sendai, Japan, January 27-30, 2004.

[4] Daewan Han, Daesung Kwon. Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards. Computer Standards & Interfaces, 31(2009), p.648-652

[5] Eun-Jun Yoon. Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard. Expert Systems with Applications, 39(2012), p.1589-1594