Strengthen RFID Tags Security Using New Data Structure

Yan Liang and Chunming Rong

Department of Electrical Engineering and Computer Science, University of Stavanger, Norway
{yan.liang, chunming.rong}@uis.no

Abstract. RFID was first proposed as a technology for the automatic identification of objects. However, some recent RFID devices can provide additional objects information and can be used for other applications. Security requirement is essential in most of the applications. An essential research challenge is to provide efficient protection for RFID systems, in particular against tag cloning and information modification. A new data structure of RFID tags is introduced in this paper. Together with the Identity-based cryptography, this new data structure can provide efficient authentication and digital signature for RFID tags.

1 Introduction

Radio frequency identification (RFID) is a technology that using radio waves for automatic identification of objects. An ordinary RFID system includes two parts, RFID tags that attached to the objects and RFID readers that can read the information from tags. A RFID tag includes an integrated circuit that contains information about the object and an antenna to receive signals from RFID readers and transmit information to RFID readers. Recently more and more companies and organizations begin to use RFID tags rather than traditional barcode as RFID systems have many advantages over traditional barcode systems. With these characteristics and advantages, RFID tags have been widely adopted and deployed in different areas. Currently, RFID tags can be used in passports, transportation payments, product tracking, animal identification, inventory systems, RFID mandates, promotion tracking, human implants, libraries, museums and social retailing.

As described in [8], there are two problems about security in RFID system: privacy and authentication. One kind of attack to RFID privacy is physical tracking. RFID readers can sense the existence of RFID tags without be detected by owner of the tags. Since most RFID tags have unique identifiers, clandestine tracking a RFID tag is possible. In addition, since RFID tags can carry product information about the objects, attacker can change this information illegally by physically attacking the tags. If there are no efficient authentication methods, RFID reader can not recognize this modification. In addition, by capturing the information of the RFID tags, attackers can effectively make a clone one of the original RFID tag that can not be distinguished

from the real tag. For example, EPC tags that with no access control mechanisms are vulnerable to such attacks. To protect RFID tags from such attacks, authentication approaches both for information stored in RFID tags and RFID tags are needed. It is difficult for basic RFID tags that can not perform cryptographic operation to provide such kind of authentication. RFID tags which are capable of performing cryptographic operations can provide stronger authentication. Price of this kind of RFID tags is high since more memory and computation resource are needed. Key management is also a problem.

To provide efficient authentication for RFID tags, a new data structure is introduced in this paper. In our approach, an Identity-based cryptography [12] is used. With this mechanism, RFID system can provide authentication for RFID tags and at the same time can facilitate the key management.

2 Security in RFID networks

The most important security concern in RFID network is the protection of the RFID tags. If the information stored in RFID tags is leaked, it will bring problems both for the users and company. Ari Juels gives a survey about the recent research on the RFID security and privacy in [8]. From the perspective of security, RFID tags can be classify into three kinds. One is the basic RFID tags, which can not perform any cryptography; the second is symmetric-key based RFID tags, which can perform symmetric-key cryptography mechanism; the third is the public-key based RFID tags that can support traditional public–key cryptographic operations [6].

Most approaches about the security protection for basic tags focus on protecting consumer's privacy and can not provide authentication for RFID tags. In [7], [9], some approaches have been proposed to provide a certain kind of authentication to resist RFID tag cloning, but each of these approaches either easy to be attacked or brings some inconveniences to the consumers.

RFID tags that use symmetric-key can increase the difficulty of tag cloning by providing some efficient authentication methods and can provide better privacy protection by using encryption. For example, a kind of RFID card named MIFARD1 S50 smart card [16] has been wildly used as the payment card of public transportation. In this MIFAD system, to protect the security of cards, a three pass authentication scheme is adopted. As shown in figure 1, the authentication mechanism is realized by generating and checking random numbers.

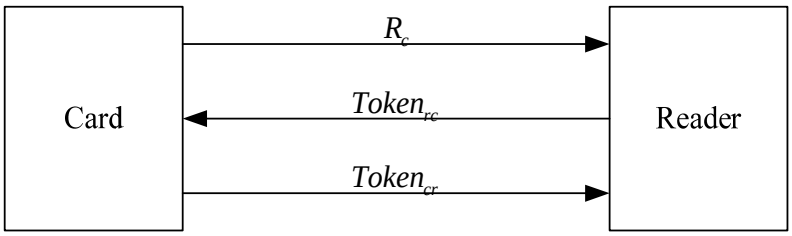

Fig. 1. MIFARE card authentication process

First, card sends a random number R_c to reader. Receiving R_c, the reader will send $Token_{rc}$ to card. The card will use secret key stored in its memory to decrypt this message and verify this message by compare the random number R_c it sent to the reader with R_c included in $Token_{rc}$. If two R_c match, card will send $Token_{cr}$ to reader. Reader will decrypt $Token_{cr}$ using secret key and compare the random numbers to verify this message.

Here, $Token_{rc} = E(K, R_c \| R_r \| B \| Text2)$, $Token_{cr} = E(K, R_r \| R_c \| Text4)$.

But in [18], three MIT undergraduate students show how they can hack subway systems that use this kind of cards. In their approach, they use FPGA to perform brute force attack and get the secret key of the system. Using this secret key, they can clone transportation cards that can pass the three pass authentication.

Texas Instruments developed another kind of RFID tags called Digital Signature Transponder that can be used as the automatic key for automobiles. This Digital Signature Transponder is also equipped with symmetric-key cryptography to provide authentication. Also as shown in [4], this Digital Signature Transponder can also be successfully cloned with little efforts and RF expertise.

Key management is another problem in symmetric-key based RFID system. In symmetric-key systems, to make the system safe, each pair of user should share a different secret key. Then in a RFID system, RFID reader needs to keep all these different keys for all RFID tags. Another problem about symmetric-key system is since the reader and tags have the same secret keys, so it can not provide digital signature service for authentication.

Recently, some approaches using traditional public-key system to protect RFID tags have been studied in [1], [4]. In the public-key system, every user has a pair of related keys, one public key and one private key. One key is used for encryption and the related other key is used for decryption. Besides encryption and decryption, the public-key scheme can provide digital signature function by signing the message with sender's private key, the receiver can use the sender's public key to verify this digital signature. Public-key scheme can also be used for key exchange, which will bring some conveniences for the key management. Another advantage for public-key cryptography is because only the user itself can know its private key, if the reader of the RFID system is compromised, the attacker can not get the private key information of the tags, thus the damage is easier to be recovered. Although public-key system can provide stronger security and more management efficiency for RFID applications, the high cost limits its implementation only to the high-end market. With the quick development of new technologies, the public-key security algorithm can be implemented in the RFID networks with a reasonable price [17].

3 RFID tags with new data structure and identity-based cryptography

3.1 New data structure of RFID tags

Currently, as different frequencies are used for RFID systems in different countries and many standards are adopted for different kinds of applications. Several kinds of RFID standards used today are introduced in [13]. These standards specify the physical layer and the link layer characteristics of RFID systems but do not cover the upper layers.

EPC standard was created by the MIT Auto-ID which is an association of more than 100 companies and university labs. EPC system is currently operated by EPCglobal [14]. There are two kinds of EPC format: EPC 64-bit format and EPC 96-bit format. In the most recent version [15], the 64 bits format has been removed from the standard. As shown in table 1, both the formats include four fields: a header, an EPC manager number, an object class and a serial number. The header and the EPC manager number are assigned by EPCglobal, the object class and the serial number are assigned by EPC manager owner. The EPC header identifies the length, the type, the structure version and the generation of the EPC. EPC manager number is the entity that responsible for maintaining the subsequent partitions of the EPC. The object class identifies a class of objects. Serial number identifies the instance.

Table 1. EPC basic format

Header	EPC Manager Number	Object Class	Serial Number

For the Contacless MIFARE1 S50 smart card used as the payment card of public transportation that developed by Philips Semiconductors. The manufacturer code is stored in the Block 0 of the memory. As shown in table 2, the data structure of block 0 is a little same with the data structure of EPC tags. It includes serial number of this card and some manufacturer data and the serial number check byte CB.

Table 2. Block 0 data structure of Mifare standard card

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Serial Number				CB	Manufacturer Data										

To strengthen the security of RFID tags, we proposed a new data structure for RFID tags.

Table 3. Proposed data structure of RFID tags

Serial Number	Encrypted Hash Code	Product Information

For our proposed data structure of RFID tags, as shown in table 3, it includes three parts: serial number, encrypted hash code and product information of item.The serial number is a random number that allocated by the system as the identity of this tag. The serial number of each tag should be unique in this system and this serial number is used as the public key of this tag. The encrypted hash code is generated using private key of this tag with hash function. Since the serial number of each tag is different, this hash code is different with others. The third part is product information, which includes different kinds of information according to different requirements.

3.2 RFID tags with Indentity-based cryptography

As mentioned above, in our proposed RFID tag data structure, the serial number which works as the identity of tag is used as the public key of this tag. Each tag also keeps a private key related with this public key. Using identity as user's public key is called Identity-based cryptography. Identity-based cryptography schemes were firstly proposed by Shamir [12] in 1984. But until 2001, the efficient approach of identity-based encryption schemes had been developed by Dan Boneh and Matthew Franklin [3] and Clifford Cocks [5].

Identity-based cryptographic scheme is a kind of public-key based approach that can be used for two parties to exchange messages and effectively verify each other's signatures. Unlike in traditional public-key systems that using the random string as the public key, in identity-based cryptography, user's identity that can uniquely identify the user such as its name or address is used as the public key for encryption and signature verification. By using identity-based cryptography, the system complexity can be greatly reduced since the two users do not need to exchange their public or private keys and the key directory is no longer needed. Another advantage of identity-based encryption is if all users in a system have been issued with keys by the trusted key generation center, the key generation center can be removed. For identity-based encryption and signature scheme, instead of generating a pair of public key and private key by the user itself, every user will use its identity as its own public key and only the trusted third party named PKG (public key generator) rather than the user will generate the relative private key.

Together with its advantages, there are some inherent weaknesses for the identity-based cryptography [2]. One problem related with it is the key escrow problem.. Another drawback of the identity-based cryptography is the revocation problem. One solution for this problem is to add a time period to the identifier as the public key [3], but it can not solve the problem completely.

For our proposed scheme, since the identity of RFID tag can be used to generate its public key, it is a kind of identity-based cryptography. We can assume that when RFID tags enter the system, each of them will be allocated a unique serial number as its identity. The process for the private key generation and distribution is shown in figure 1:

(1) PKG generates a "master" public key PU_{pkg} and a related "master" private key PR_{pkg} and saves them in its memory.

(2) RFID reader authenticates itself to PKG with its identity ID_{re}.

(3) If reader can pass the authentication, PKG will send PU_{pkg} to it.

(4) Each tag authenticates itself to PKG with its identity ID_{ta}.

(5) If the tag can pass the authentication, PKG generates a unique private key PR_{ta} for the tag and send PR_{ta} together with PU_{pkg} to the tag.

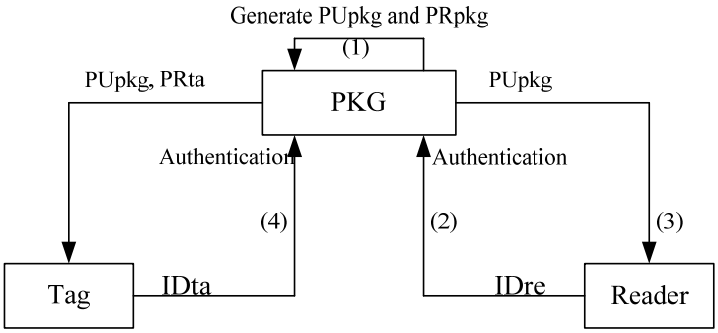

Fig. 2. Key generation and distribution

After key generation and distribution, every tag in the system will have its own private key. This private key will be used to generate the encrypted hash code for it. To generate this encrypted hash code, first system will apply SHA-1 algorithm to the product information of the tag and generate a hash code for this tag. Then system will encrypt this hash code using the private key of this tag and store the serial number, product information and encrypted hash code into the memory of tag. RFID reader, after scanning a RFID tag, will get all the information stored in the memory of RFID tag. To verify the integrity of the product information, first RFID reader will read serial number of tag and use this serial number and PU_{pkg} to generate the public key of this tag and use this public key to decrypt the encrypted hash code. Then this reader needs to apply SHA-1 algorithm to the product information of the tag and generate a hash code. By comparing this hash code with the decrypted hash code, RFID reader can verify the integrity of the product information. Since the encrypted hash code stored in the tag is generated using the private key of tag, this encrypted hash code can work as a digital signature of this tag. RFID tag can use this digital signature to authenticate itself to RFID readers.

3.3. Security of RFID tags with new data structure

RFID tags with this kind of data structure can provide authentication and digital signature for tags and this will bring many conveniences for both manufactories and users.

For example, one problem for RFID tags that use read/write memory is attackers can easily change the information stored on the tags. Without data authentication mechanism, RFID readers can not learn this modification. In order to protect the integrity of information, some RFID tags use read only memory. The information in this kind of RFID tags can not be changed after first written but this makes tags can not be reused. For our proposed data structure, attackers can modify the information of RFID tags. Without knowing the correct private key of tag, attacker can not generate the correct encrypted hash code and can not pass the reader's authentication.

For the subway system that using symmetric key, if the attacker can get the secret key by brute force attack, it will bring a big problem for these systems. Now days, more than 500 million MIFARE cards have been distributed [18]. If the secret key is divulged, it should be a hard work to update secret keys for all these cards. For our proposed scheme, every RFID tag has its own private key, and these keys are different form each other. If private key of a card is known by attackers, it will not bring a large affection to the subway system, since the attacker can not know private keys of other cards from this key.

Another important problem for the symmetric-key approach in RFID system is the key management. If every MIFARE card has a different key with each other, the key number should be very large and RFID reader needs a large memory to save all these secret keys in the system. Also if RFID reader receives a message from a card, since it can not know this message is from which card and therefore can not know which key it can use for message decryption, it needs to search from all the keys until find out the right one. Although some approaches [10], [11] have been proposed to reduce cost of key searching, the key searching is still a problem that waste of time and resources. While in RFID system using identity-based cryptography, knowing the serial number of cards, reader can easily generate related public keys.

In some RFID applications, digital signature is required. In our proposed scheme, the encrypted hash code can be looked as the digital signature of the tag. This digital signature is generated using tag's own private key and each signature should be different. RFID reader can easily verify this digital signature using the public key of tag. Although RFID systems that use traditional public-key cryptography can provide same function, but the system authority must remember all the keys and keep the key directory for certification. While in our proposed RFID systems, since the serial number of RFID tags can be used to generate their public keys, PKG dose not need to keep the key directory thus can reduce the resource requirements. Another advantage is the reader does not need to know the public keys of RFID tags in advance. If the reader wants to verify the digital signature of a RFID tag, it can read serial number of the tag, and use the public key generated from this serial number to verify digital signature. While in the traditional public-key systems, if RFID reader wants to know a RFID tag's public key, it must search in the key directory to find it.

For the revocation problem of the identity-based cryptography, in the RFID system, the identity of the tag is used to generate the public key. If the private key of one tag has been compromised, the system can allocate a new identity and create a new private key to the tag effortlessly.

4 Conclusion

In this paper, we introduced RFID technology and make an overview of the security considerations especially tag authentication problems in RFID systems. Also we depicted the data structure of some kinds of RFID tags that wildly used today and proposed our new data structure for RFID tags. Then we proposed how to create and use this new data structure to provide date authentication and digital signature for RFID tags. By comparing this approach with EPC tags and some RFID tags using symmetric-key based approach and public-key based approach, we can see that by using our new RFID tag data structure and scheme in RFID system, we can get benefits both in authentication and key management.

References

1. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede, "Public-Key Cryptography for RFID-Tags", Proceeding of the 5th International conference on Pervasive Computing and Communications Workshops, 2007
2. J. Beak, J. Newmarch, R. Safavi-Naini, W. Susilo, "A Survey of Identity-Based Cryptography", Proceeding of the 10th Annual Conference for Australian Unix and Open System User Group (AUUG 2004), pp 95-102, 2004
3. D. Boneh, M. Franklin, "Identity-based Encryption from the Weil Pairing Advances in Cryptology",Preceeding of Crypto'01, LNCS 2139, Springer-Verlag, 2001
4. S. Bono, M. Green, A. stubblefield, A.Juels, A. Rubin, M. Szydlo, "Security Analysis of a Cryptographically Enabled RFID Device", USENIX Security Symposium – Security '05, pp 1-16, 2005
5. C. Cocks, "An Identity-based Encryptoin Scheme Based on Quadratic Residues", Proceeding of 8th IMA International Conference on Cryptography and Coding, 2001
6. W. Diffie, M.Hellman, "New Direction in Cryptography", IEEE Transactions on Information Theory, Vol. 22. (1976), pp 644-654, 1976
7. A.Juels, "Yoking-Proofs for RFID tags", Workshop on Pervasive Computing and Communications Security. IEEE Computer Society , 2004
8. A. Juels, "RFID Security and Privacy: A Research Survey", Selected Areas in Communications, IEEE Journal, 2006
9. A. Juels, "Strengthening EPC tags against cloning", Proceeding in the 6th International Conference on Web Information Systems Engineering, 2005
10. D. Molnar, D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures", Proc. ACM Conf. Ubiquitous compute Security, pp 210-219, 2004
11. D. Molnar, A. Soppera, D. Wagner, "A scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of FRID Tags", The 12th Annual Workshop on Selected Areas in Cryptography, LNCS, 2005
12. A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Advances in Cryptology: Proceeding of CRYPTO 84, LNCS, pp47-53, 1984
13. J. Wiley & Sons. RFID Handbook. (2nd).
14. EPCglobal. http://www.epcglobalinc.org/, June 2005.
15. EPCglobal Tag Data Standards. Version 1.3.
16. Mifare Standard Card IC MF1 IC S50 Functional Specification.
17. NTRU. GenuID. http://www.ntru.com/products/genuid.html
18. http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf