An Elliptic Curve Based Authentication Scheme for RFID

Changsheng Wan, Lin Zhou, Jie Huang
School of Information Science and Engineering
Southeast University
Nanjing, Jiangsu
e-mail: wan.changsheng@163.com

Juan Zhang
Accounting Department
Nanjing University
Nanjing, Jiangsu
e-mail: zjtider@163.com

***Abstract*—To solve the problems of consumers' security and privacy, a new RFID authentication method based on the elliptic curve is proposed. Comparing with other asymmetric cryptography, this method has stronger security, shorter key length, less computation. This scheme makes the reader and the writer being able to complete the certification process for the reader through interact with the protocol of label. Moreover, this scheme can provide anti-replay and privacy-preserving protection for tags.**

Keywords-elliptic curve; authentication; RFID

I. Introduction

RFID (Radio Frequency Identification, RFID) system [1] is a non-contact automatic identification system, the system comprises tags, readers and the back-end database. Reader-writer obtains the information in the tags through wireless signal. Due to the nature of the automatic identification, RFID systems to be more widely used in various fields of production, logistics management, access control systems, traffic pay. However, a wealth of data provided by tags is likely to lead to users' privacy and security issues [2,3]. Majority tags do not have the anti-counterfeiting and anti-illegal read function because of cost constraints, an attacker can easily read or tampered with label information to counterfeit labels, and can even track the owner through the label. In order to design an efficient and secure RFID authentication protocol, [3,4,5] proposed public key based schemes for RFID authentication.

The current RFID security authentication methods can be mainly divided into three categories.

Security method based on hashing and random function: the hash function ensures that the integrity of the communication data and the communication data can't be changed, adding the random number generated by a pseudo-random function to the communication data can against replay attacks, and also ensure that the response of each query label are different, so as to achieve the anonymity of labels.

Security methods based on the shared key and the random function: the main principle of the method is using the pseudorandom function based on pre-shared key to realize the authentication, at the initial period, between the server-side database and each label need to share a key in advance. Although so far, have not found that this method has obvious security loopholes, but in order to support this approach, must contains two functional modules which realize the generation of random number and secure pseudo-random function in tag circuit, so it does not apply to the low-cost RFID system.

Security methods based on symmetric or asymmetric cryptographic algorithm: the difference between the hash function and the security method based on Hash function is that use AES function replaced with Hash function.

This paper proposes a security authentication method of RFID based on the elliptic curve and technology of symmetric cryptography, the method makes reader-writer able to complete the certification process for the reader through interact with the protocol of label, at the same time the method can also anti-replay attacks, and protect the privacy of tags.

The beneficial effects of the method are as follows:

The authentication method of RFID based on elliptic curve technology either can enhance the security of the RFID certification, or can provide more higher performance than the authentication technology based on quadratic residue; generating a session key based on nonce value (non-repeating random numbers) to avoid occurring the replay attack; at the same time, labels do not need to send their own identification through the empty while doing authentication, so as to solve the privacy issues of labels.

II. Our Scheme

To solve the problems mentioned in the introduction, the paper proposes a security authentication method of RFID based on the elliptic curve and technology of symmetric cryptography, the method makes reader-writer able to complete the certification process for the reader through interact with the protocol of label, at the same time the method can also anti-replay attacks, and protect the privacy of tags.

The invention solves the technical problems with the following technical solution:

The invention relates to a security authentication method of RFID based on the elliptic curve and technology of symmetric cryptography, which includes the following steps:

1) The initialization of the device and process; create the elliptic curve, and generate their own public and private key pairs;

2) The initialization process of tags; allocate and verify the public key and the public and private key pairs for tags, and at the same time allocate the signature;

3) The initialization process of reader-writer; create a public and private key pair for the reader-writer, and sign the public key of reader-writer, and allocate its own public key in the reader-writer at the same time, the reader-writer obtain the permissions of reading and writing tags through the signature;

4) The interaction of RFID authentication protocol; use the bilinear technology to verify the signature, and use Diffie-

Hellman algorithm of elliptic curve to generate the symmetric key to protect the security of subsequent communications.

The method contains four major contents which are shown in Fig. 1: (1) the initialization process of the device; (2) the initialization process of tags; (3) the initialization process of reader-writer; (4) the interaction process of RFID authentication protocol.

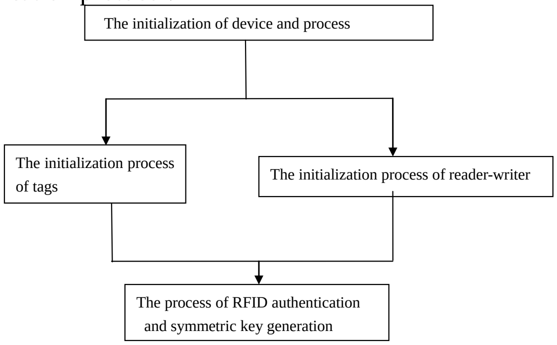
The initialization of device and process
The initialization process of tags
The initialization process of reader-writer
The process of RFID authentication and symmetric key generation

Figure 1. Four major contents in this scheme

Our schema includes four phases:

1) the initialization process of the device;
2) the initialization process of tags;
3) the initialization process of reader-writer;
4) the interaction process of RFID authentication protocol.

Phase 1) The initialization process of the device

In the initialization process of the device, the scheme references the way in [6] to create elliptic curve, and generate its own public and private key pair.

This solves the following problem: initializing the device first initializes the password system of RFID, the subsequent authentication and symmetric key generation algorithms are based on the password system. The specific initialization process is shown in Fig. 2.

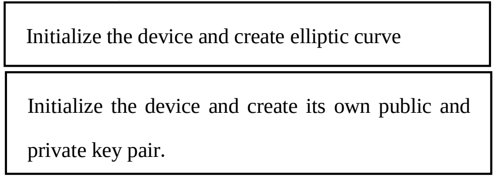
Initialize the device and create elliptic curve
Initialize the device and create its own public and private key pair.

Figure 2. The specific initialization process of device

In this step, fist of all initialize the device, according to the method in [6] to create the elliptic curve. Where the parameters of the elliptic curve includes: (p, a, b, n, G). In which p is a large prime number, a and b are the coefficient of the elliptic curve (both are positive integers), n is the band of an elliptic curve (is an integer), G is the bps of the elliptic curve bps (is one point on the plane, forms such as (x y), in which x and y are both positive integers and less than p). The specific method of creation can reference the literature Elliptic Curve Cryptography.

Then initialize the device, according to the method in [6] to create their own public and private key pair (Ks, Gs). In which Ks is a positive integer and less than p, Gs is the point on the elliptic curve (in the form such as (x, y)), Gs = Ks G (Note: KS G is a point multiplication operation as specific defined is in [6]).

In this step, initializing the device and creating an elliptic curve provide a basis for the generation of subsequent authentication and symmetric key. At the same time, initializing the device and creating its own public and private key pairs, so as to provide a basis for the subsequent signature.

Phase 2) The initialization process of tags

In the initialization process of tags, the scheme references the way in [6] to verify and configure a public key and a public and private key pair for tags, at the same time, to configure signature.

The purpose of defining the initialization process of tags is: reader can authenticate tags, at the same time to provide a basis material for the subsequent generation of symmetric key. The specific initialization process is shown in Fig. 3.

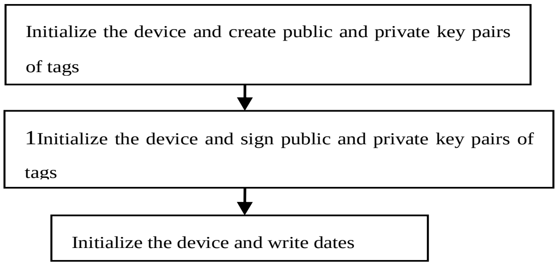
Initialize the device and create public and private key pairs of tags
1Initialize the device and sign public and private key pairs of tags
Initialize the device and write dates

Figure 3. The specific initialization process of tags

In this step, first of all initialize device and randomly generate a positive integer Kl whose value is less than n, according to the method in [6] to calculate: Gl = KlG. And (kl, Gl) constitute public and private key pairs of label l. In which, Kl is the public key and Gl is the private key.

Then initialize the device and calculate the signature of the public key of tags Sl = Ks Gl.

At last initialize the device and write (Kl, Gl, Sl) in the label, and complete the initialization process of tags.

Phase 3) The initialization process of reader-writer

In the initialization process of reader-writer, the scheme references the way in [6] to create a public and private key pair for reader-writer. And sign the public key of the reader-writer, at the same time configure its own public key to the reader-writer. Signature allows the reader has permission to read and write tags.

The purpose of defining the initialization process of reader-writer is: tags can certificate the reader-write, at the same time to provide a basis material for the subsequent generation of symmetric key. The specific initialization process is shown in Fig. 4.

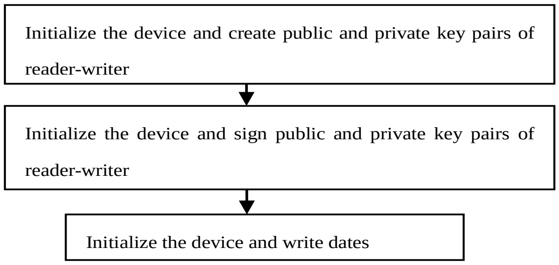
Initialize the device and create public and private key pairs of reader-writer
Initialize the device and sign public and private key pairs of reader-writer
Initialize the device and write dates

Figure 4. The specific initialization process of reader-writer

In this step, first of all initialize the device and generate a positive integer km which is less than n, according to the method in [6] to calculate Gm=kmG, then (km, Gm)constitute public and private key pair of the reader-writer m, in which km is the private key and Gm is the public key.

Then initialize the device and calculate the signature of the public key of the reader-writer Sm = Ks Gm.

At last initialize the device and write (Kl, Gl, Sl) in the reader-writer, and complete the initialization process of the reader-writer.

Phase 4) The interaction process of RFID authentication protocol

In the interaction process of RFID authentication protocol, the scheme references the way in [7] to verify the signature by the bilinear technology, at the same time using the Diffie-Hellman algorithm of elliptic curve to generate symmetrical key, so as to protect the subsequent communications.

The purpose of defining RFID authentication and the generation process of symmetric key are: when the reader-writer wants to read and write the label, the two sides complete the certification process, and at the same time generate a shared key. And which provides security protection for subsequent read and write operations. The specific process is shown in Fig. 5.

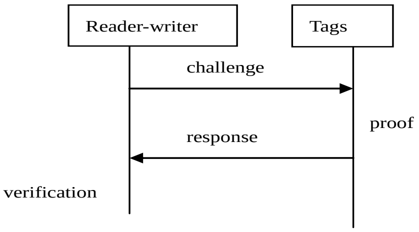

Figure 5. The specific initialization process of RFID authentication protocol

In this step the reader-writer first generates a random number nocne1 then sends (Gm, Sm, nonce1) to the label.

After the label receiving dates of the reader-writer, first of all, uses the bilinear method in [7] to verify the correctness of Sm: e(G, Sm) = e(Gs, Gm) (Note: e(G, Sm) = e(G, ksGm) = e(ksG, Gm) = e(Gs, Gm)); then generates a random number nocne2 then calculates Gr = (nonce1 * nonce2 *kl) Gm, and then uses the definition of conversion method of point to integer in [6] to changer the point Gr which is on the elliptic curve into key k.

Then the tags send (Gl, Sl, nonce2) to the reader-writer m.

After all the reader-writer m first verify the correctness of Sl: e(G, Sm) = e (Gs, Gm) (Note: e (G, Sl) = e(G, ksGl) = e(ksG, GI) = e(Gs, Gl)); then calculates Gr '= (nonce1 * nonce2 * km) Gl. Because of Gr '= (nonce1 * nonce2 * km) Gl = (nonce1 * nonce2 * km * kl) G = (nonce1 * nonce2 * kl) (km G) = (nonce1 * nonce2 * kl) Gm = Gr, so the reader-writer can also get k from Gr.

This step completes the following two things:

1) Authentication. By bilinear pairing algorithm verify the correctness of signature of the public key, and complete the authentication between the reader-writer and the tag.

2) Generate the symmetric key. By Diffie-Hellman algorithm based on Elliptic Curve generate the public key k, so as to protect subsequent communication security.

In the four major should first define the initialization process of the device, and then define the initialization process of tags and the reader-writer initialization process, at last design the authentication method based on elliptic curve, and generate a shared key. In the process, the labels do not need to interact with their own identity, which play an effect of hiding themselves. Besides the generation techniques of the shared key which are based on random nonce value can solve the problem of replay attacks.

III. Security Analysis

A. Comparison

In symmetric encryption system, because of that encryption protocol based on symmetric algorithm is not so many, to some extent, the security protocol based on the tiny encryption algorithm (TEA) can protect data secrecy, integrity, authenticity and prevent leakage of user privacy, but there is also a serious problem of key distribution: all tags and reader-writers in systems all use the same key, so if there is a key of the label being break or leaked, the keys of the entire RFID system are all invalidated. Although there were security authentication methods based on hashing and random function, in these methods, when the reader sends access request to the tag, which the tag returned to the reader is not a fixed ID, but one Hash value of its ID value, but the disadvantage of this method is also very evident, the data integrity, authenticity, and user privacy protection are not guaranteed.

Although the algorithm of RSA in public key encryption system has been widely used, but its key length is generally to be maintained at more than 1024bits, moreover with the enhancement of safety performance requires a corresponding faster growth in key length, leading to implement on higher hardware requirements, therefore it does not suitable for use in RFID chip.

B. Security Analysis

In our scheme, tags do not send its own identification information to the reader-writer while doing authentication, so as to realize hiding the label information.

In our scheme, each authentication uses a randomly generated nonce value, to ensure that the generated key k is different each time, and prevent attacker reproducing an expiration of the data packet, and attacking the tag. So as to achieve the immunity to replay attacks.

In summary, The authentication method of RFID based on elliptic curve technology either can enhance the security of the RFID certification, or can provide more higher performance than the authentication technology based on quadratic residue; generating a session key based on nonce value (non-repeating random numbers) to avoid occurring the replay attack; at the same time, labels do not need to send their own identification through the empty while doing authentication, so as to solve the privacy issues of labels. So as to solve the problems of the existing technique, making tags and readers can achieve the authentication process through the combination method of symmetric key and asymmetric key, and generating a symmetric key, used to protect subsequent communication security.

IV. Conclusion

Because of that sometimes in certain circumstances, the authentication protocol based on a symmetric key system has been unable to fully meet the requirements, and the authentication protocol based on a public-key system which applies to RFID system is also less, research on RFID security protocol has very important significance. In this paper, we proposed a security authentication method of RFID based on the elliptic curve and technology of symmetric cryptography. Tt has a higher level of safety performance, and the security issues of data secrecy, integrity, security, authenticity as well as the protection of user privacy in current RFID systems are guaranteed.

ACKNOWLEDGMENT

This paper is supported by the NSFC (No. 61101088), the Chinese 863 plan (No.2013AA014001), the Fundamental Research Funds for the Central Universities, and the project “security detecting service for wireless intelligent terminal”.

REFERENCES

[1] Miles S B, Sarma S E, Williams J R. RFID Technology and Applications[M]. New York, USA: Cambridge University Press, 2008.

[2] Weis S, Sarma S, Rivest R, et al. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C]//Proc. of the 1st International Conference on Security in Pervasive Computing. Boppard, Germany: [s. n.], 2003.

[3] Zhang Hengshan, Chang Jun,Guan Huisheng,A multi-encryption-technic based authentication method for RFID [J]. Computer Engineering, 2011, 37(1): 134-136.

[4] Chen Yalin, Chou Jue-Sam, Sun Hung-Min. A Novel Mutualauthentication Scheme Based on Quadratic Residues for RFID Systems[J]. Computer Networks, 2008, 52(12): 2373-2380.

[5] Yeh Tzu-Chang, Wu Chien-Hung, Tseng Yuh-Min. Improvement of the RFID Authentication Scheme Based on Quadratic Residues[J]. Computer Communications, 2011, 34(3): 337-341.

[6] SECG, "Elliptic Curve Cryptography," SEC 1, 2000.

[7] Qian Wang, and Et.Al., “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, pp.847-859, may 2011.