The RFID Mutual Authentication scheme Based on ECC and OTP Authentication

Chunling CHEN, yang WANG, Han YU and Xiao-Hui Qiang
School of Computer Science & Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
Jiangsu Branch Of National Computer network Emergency Response technical Team/Coordination Center of China

Abstract-**In the RFID environment with limited storage and computing resources, it is necessary to adopt appropriate and effective lightweight authentication technologies to ensure the security of RFID operating environment. After studying existing RFID authentication scheme and analyzing its security, a mutual authentication scheme *based* on ECC and OTP authentication is proposed. In this scheme, authentication information introduces a random number and a time stamp based on the traditional OTP authentication, and ECC is used to encrypt the authentication process for the its information confidentiality. The safety analysis shows that it meets basic security requirements and resists tracking, replaying, counterfeiting and other kinds of attacks. At the same time, it achieves mutual authentication between the tags and the database sides, which improves the security of RFID environment well.**

Key words: **RFID;ECC;OTP;mutual ;authentication ;**

I. INTRODUCTION

In the field of Internet of things technology,the Radio Frequency Identification (RFID) technology is an important technical basis for acquiring and exchanging information on-the-fly in the sensing layer[1]. RFID equipment have limited storage and computing resources because of the simple design, so the traditional authentication and encryption technology cannot meet the requirements of RFID. In RFID environment, appropriate and effective lightweight security authentication mechanism is inadequate, which makes RFID equipment physically damaged easily, and subject to forgery attacks, impersonation attacks, replay attacks, information tampering[2]. They seriously threaten the security of RFID applications.

For the authentication application issues in the RFID, there are already relevant research carried out in the literature at present. One of these classic forward authentication protocol --Hash-Lock protocol [3] is mainly used for tags to guard against malicious tracking, namely using one-way hash function to replace the label identification information to avoid the information leakage or be traced. However, since the one to one mapping relationship has always remained unchanged between metaID and ID, malicious trackers can still track tags through the metaID. In the meantime, because the authentication information is transmitted through the clear text, the replay attack and the counterfeit attack cannot be prevented. Ding Zhenhua et al. also proposed a hash-based RFID authentication scheme [4] where the label executes two hash operations, which is more in line with the RFID environment for the lightweight requirements. However, the analysis shows that the program does not have the forward security. Chen Y submitted algorithm based on public key encryption[5] involving public-key encryption function, Hash functions, and random number generation function. But it takes more memory and computation cost resources, and proved unable to provide location privacy and susceptible to replay attacks. Y. K. Lee et al. considered algorithms based on elliptic curve discrete logarithm problem and put forward a kind of on Elliptic curve cryptography (ECC) based authentication protocol [6]. It is safe in the general model, and has reduced calculation through their analyses. But then the protocol was pointed out that it is vulnerable to tracking attack and replay attack, meanwhile the database side cannot avoid impersonation attack because of the one-way authentication. Wang Haichun et al. proposed a scheme of RFID authentication scheme[7] based on chaotic encryption, which generates hash values by chaotic encryption technology. She emphasized security and lightweight of the chaotic encryption in the analysis. However, in the authentication scheme, the random number generated by the tag and the database is transmitted through the transparent text. That may lead to the failure of authentication because the attacker can easily fake ones.

Considering the existing problems of known authentication scheme such as lightweight and low security, this paper proposes a RFID mutual authentication scheme based on ECC and One Time Password (OTP).

II. KEY TECHNOLOGIES

A. Elliptic Curve Cryptography

An elliptic curve E on the finite field Fp is defined as: $y^2 = x^3 + ax + b$,which meets the conditions:p>3 and odd, $a,b \in F_p$, $4a^3 + 27b^2 \neq 0(\bmod p)$. The point set E (Fp) is composed of pairs of points (x,y) satisfying the equation on the finite field and the point at infinity O, with conditions: $x \in F_p, y \in F_p$.

The computational intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP) is over a finite field, that ensures security of the cryptosystem. Namely, simple to find Q if we know the m and the point P in the equation : mP=Q, whereas the known point Q and P is quite difficult to find m. The best solution complexity of the problem is exponential time, which guarantees security of elliptic curve cryptosystem.

B. OTP Authentication Technology

OTP is a digest authentication, it compresses variable-length text as input into a fixed length message as the

978-1-5090-1317-3/16/$31.00 ©2016 IEEE

output. The abstract function has the characteristic of unidirectionality, which guarantees the information security [11].

There are server side and client side in a typical OTP authentication scheme namely S/Key one-time password scheme. The client calculates the one-time password according to the user traffic and the challenge information received from the server. The server generates challenge information, verifies one-time password sent by the client, and stores the last successful authentication password as well as the serial number in the data record.

III. RFID MUTUAL AUTHENTICATION SCHEME

As can be seen from the above, there are problems to balance two main performance of security and lightweight in the existing RFID authentication scheme. Some schemes cannot be applied to the RFID system environment appropriately under the premise of ensuring the security of the system. Otherwise, some authentication schemes meet the lightweight requirements but cannot guarantee the safety of the system environment. Regarding that, this paper proposes a mutual authentication scheme that is applied into the RFID device, namely, RFID Mutual Authentication Scheme Based on ECC and OTP (RMASBEO). RMASBEO achieves mutual authentication between the RFID tag and the database server, and in addition, introduces elliptic curve public key encryption algorithm to ensure the confidentiality of the information in the certification process. ECC is suitable for RFID authentication environment of limited computing and storage resources because of its fast computing speed and high strengthened security. The authentication scheme in this paper is mainly composed of two stages: the registration and the certification. For convenience of description, symbol definitions are shown in TABLE I.

TABLE I
symbol annotation for RFID authentication scheme

symbol	annotation	symbol	Annotation
id	Tag verification code PW in the reverse	k_{DS}	The private key of the database.
pw	Tag verification code bound with the label in factory	k_{UP}	The public key of RFID tag
$T_{i\text{-}1}$	Time-stamp used for registration, and also used as first authentication password factor	k_{US}	The private key of RFID tag
T_i	Times-tamp used for last time authentication	$Ek()$	Elliptic curve encryption function
T_{i+1}	Times-tamp used for next time authentication	$Dk()$	Elliptic curve decryption function
H()	Hash function for tag, reader, database sharing	R	Random number
k	The random number generated by the database is used as the private key of the database.	ECC	The main parameter sets of ECC, including elliptic curve E_p (a,b) basic point G (x_G, y_G)
k_{DP}	The public key of database	A=?B	whether A is equal to B
A←B	B instead of A	||	Connector

A. Registration Process

The specific process of registration is shown in Figure 1.

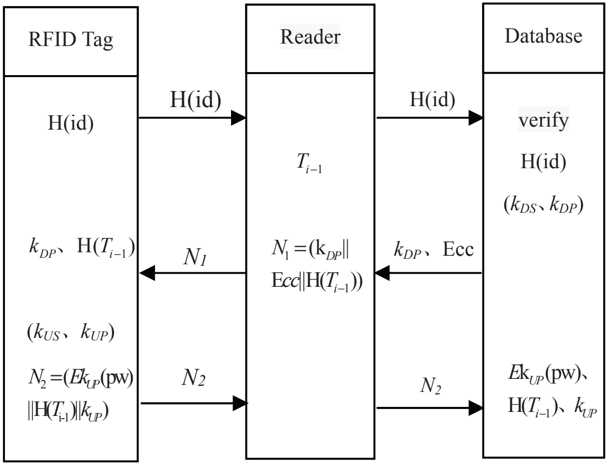

Figure 1 Schematic diagram of the registration phase

The specific steps in the registration phase are as follows:

a.RFID tag does a self-hash operation on its own id, and then sent it as a registration request information to the RFID reader. After receiving the registration request, the RFID reader catches and stores the current T_0 times-tamps, and then forwards H(id) from tag to the database.

b. After receiving H(id), the database checks the existing registration list in order to determine whether the tag has been registered. If it finds the same id, the registration stops. Else the database stores the H(id), then generates a secure elliptic curve E_p(a, b) and selects a point G(x_G, y_G) on it, then generates a random number as their own private key k_{DS}. Their public key k_{DP} is calculated by k_{DP} = kG at the same time. Finally, the database sends k_{DP}, E_p(a,b) and the point G to RFID reader.

c. The $T_{i\text{-}1}$ is hashed once after RFID reader receives the message from the database, and then H($T_{i\text{-}1}$) together with k_{DP} and ECC form the message N_1 that is $N_1 = (k_{DP}\|ECC\|H(T_{i-1}))$ .After that, RFID reader sends N_1 to tag side.

d. Receiving the message N_1 later, RFID tag stores H ($T_{i\text{-}1}$) and the public key of database and then generates own private key k_{US} and public key k_{UP} according to the relevant parameters of the elliptic curve. The unique identity authentication code of tag is encrypted by its private key, which is consistent with the elliptic curve encryption method. Then the encrypted identity code along with H($T_{i\text{-}1}$) and the public key of tag compose the message N_2 that is $N_2 = (Ek_{UP}(pw)\|H(T_{i-1})\|k_{UP})$. After that, the tag sends message N_2 to RFID reader.

e.The database side receives the message N_2 from RFID reader after, disassembles the message and stores Ek_{UP} (pw), H ($T_{i\text{-}1}$), k_{DP}.

B.Authentication Process

After successful registration, the tag must first pass the authentication before connecting with the database server. The specific authentication process is shown in figure 2.

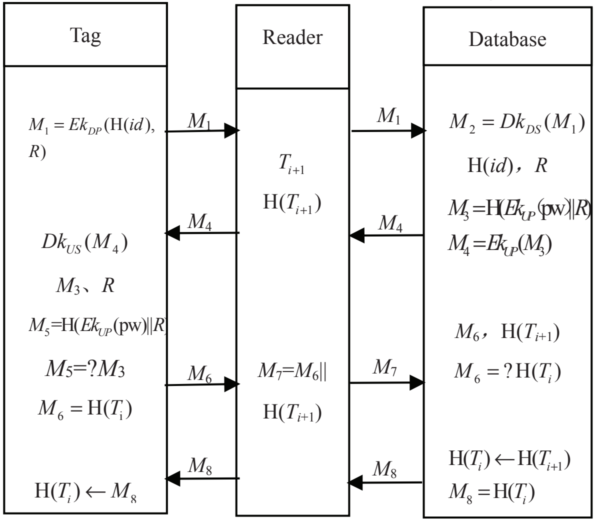

Figure 2 Schematic diagram of the certification phase

Specific authentication process is as follows:

a.A random number R generated by RFID tag and tag id form the message M_1 after which was encrypted by public key of database, the message M_1 that is $M_1 = Ek_{DP}(\mathrm{H(id)}, R)$. Then it is forwarded to database server by RFID reader. When the reader receives the message, it extracts the current timestamp T_{i+1} and stores it after making its hash as $\mathrm{H}(T_{i+1})$.

b. The database server extracts id and random number R after decrypting the message M_1 using its own private key, that as $M_2 = Dk_{DS}(M_1)$. After that, the server queries the $\mathrm{Ek_{UP}(pw)}$ and $\mathrm{H}(T_{i+1})$ bound to the tag id .

c. The database connects the $\mathrm{Ek_{UP}(pw)}$ with the random number R, and makes a hash operation to get the massage M_3, namely $M_3 = \mathrm{H}(Ek_{UP}(\mathrm{pw})\|R)$. Then database server encrypts M_3 by the public key of tag as this: $M_4 = Ek_{UP}(M_3)$, and sends the message M_4 to tag side by reader forwarding.

d.The tag side receives the message M_4 from the reader and decrypts it through its own private key to obtain the information M_3. Then tag uses own public key to encrypt the unique identity authentication code pw and hashes it with random number R to get massage M_5, that is $M_5 = \mathrm{H}(Ek_{UP}(\mathrm{pw}\|R)$ .After that, tag side verifies whether the M_5 and M_3 are equal. If there is equality, the database server would be legitimate. Otherwise, the side terminates communication with database server, and the authentication fails.

e. If the database server is valid, the tag side will extract stored H (T_i) as the message M_6. Whereafter, RFID tag sends M_6 to the reader side. When receiving the message M_6, RFID reader adds the staged H (T_{i+1}) to form message M_7 as $M_7 = M_6\|\mathrm{H}(T_{i+1})$ and transmits it to the database side.

f. After receiving the message M_7,the database side disassembles this message to get M_6. Then database side verifies whether the information and the stored $\mathrm{H}(T_i)$ are equal. If they are equal, the legitimacy of tag would be proved. After that, the database server updates $\mathrm{H}(T_\mathrm{i})$ with value of $\mathrm{H}(T_{i+1})$ and stores the new $\mathrm{H}(T_\mathrm{i})$. At the same time, it sends the new $\mathrm{H}(T_i)$ as the message M_8 to tag side, that is shown in Fig 2. Otherwise, the communication with the tag would be terminated, namely, the authentication fails. Of courses the authentication ends.

h. If the tag side receives the message $\mathrm{M_8}$, it will update the time stamp H (T_i) in tag according to the value of M_8 . So far the authentication succeeds.

IV. Safety Analysis

RMASBEO is proposed based on the research of RFID authentication scheme and the existing loopholes in authentication environment, the scheme of security analysis is as follows:

a.Mutual authentication

After the database server side receives the random number R sent by tag side, it is associated with $\mathrm{Ek_{UP}(pw)}$ stored in the side to do a hash operation and sends the result to the tag side. The unique identity code of tag pw is encrypted with the public key of the tag and hashed together with the R when the tag side receives the message from the database side. And then it compares the information of M_5 and M_3 shown in the Figure 2. If the two results are the same, then the server is legal. The database determines whether the tag side is legal based on verifying $\mathrm{H}(T_i)$. Thus the mutual authentication ends. The mutual authentication technology ensures the legitimacy of the communication between the two sides.

b. Confidentiality

RMASBEO authentication scheme uses the elliptic curve encryption algorithm to encrypt the information in authentication process, which ensures that sensitive information will not be stolen and tampered. Moreover, the tag's unique identification codes also are encrypted by public key of tag after, then stored in the database side. In addition to the tag itself, other people cannot get information of the unique identification codes. That ensures the confidentiality of the tag information.

c.Prevent decimal attack

This authentication scheme does not use the method of iterative hash to achieve authentication in the OTP authentication scheme, so the attacker cannot modify the number of iterations to achieve decimal attack. The authentication just introduces a random number, but the attacker fails to get the one because of encrypted transmission.So the decimal attack cannot be implemented.

d.Forward-security

The database server side and tag side use the Hash function with forward directional characteristics. For instance, $\mathrm{Ek_{UP}(pw)}$ and the random number R are hashed in authentication process by the sides, just as one of the authentication factor of the time stamp T_i is stored after the hash operation. The tag never stores previous authentication messages and time stamps. So even if the attacker gets the current time stamp T_i, it could not calculate the previous time stamp because of the one-way Hash function. And even if the attacker wins the previous authentication information, it would not recovery Ek_{UP}(pw) and the R that without hashing because of the one-way characteristic of Hash. Therefore, this scheme has forward security.

e. Backward-security

Due to the introduction of random number R in the certification process, even if the attacker stole the current authentication information Ek_{UP}(pw) and R, it could not use stolen information to calculate the next round of authentication password. So the scheme has backward-security.

f.Refuse to counterfeit attack

It assumes that the attacker prepares to fake database server to authenticate with tag side. The tag encrypts the random number R by the public key of the database and transmits it to database side. Because the attacker cannot get the private key of the database to decrypt the stolen message from tag side to get the R, it can only generate a random number R' by itself, and then the R' does hash operation with Ek_{UP}(pw). After receiving the message, the correct random number R does hash operation again with Ek_{UP}(pw) in the tag side. Because of the results of the two are different, the tag refuses to communicate with faker. So the attacker fake database server failed.

The assumption that the attacker prepares to fake tag for authentication. But the attacker cannot get the encrypted time stamp T_i as authentication factor, so it cannot be authenticated with the database. So far, the attacker fails to counterfeit attack.

g.Refuse to replay attack

The random numbers generated by the tag are not same in every process of authentication, even if the attacker intercepted the previous information M_4 and send it to tag side for authentication.but the current effective authentication information in tag side is that current random number R does hash operation with Ek_{UP}(pw), the values of the two are different. Authentication fails.

At the same time, because the timestamp of each authentication is constantly varying. Even if attacker attempts to intercept the previous timestamp for authentication with database server, the database server could verify imparity of the timestamp and its current timestamp. So the authentication fails. At this point, the replay attack fails.

h.Refuse to track attack

The random number is introduced in the authentication scheme, and it is randomly generated in tags. So there is no connection between each other. So even if the attacker intercepted two authentication message M_1 successively, it could not make use of the analysis of the connection between the two messages to track the tag location information because the adoption of two random number have no any connection. At the same time, the unique identification code of tag is encrypted by the public key of tag, the attacker fails to decrypt it without the private key. The comparison of security between RMASBEO and schemes in references is shown in TABLE II.

TABLE II

Comparison of safety performance of each authentication scheme

scheme safety	lit. 3	lit. 4	Lit .5	lit. 6	lit. 7	RMAS BEO
mutuality	√	√	√	○	√	√
secrecy	○	√	√	√	○	√
forward-security	√	○	√	√	√	√
backward-security	√	√	√	√	√	√
dis-counterfeit	○	√	√	○	○	√
dis-replay	○	√	○	○	√	√
dis-track	○	○	○	○	√	√

√：Secure ○：Unsecure

V. CONCLUSION

Because of its own particularity and limitation, the RFID system brings many security issues, among which the security and reliability of authentication is particularly acute. Due to the special nature of RFID environment, the current study focused mostly on lightweight authentication. But it cannot be ignored that the security and confidentiality of the authentication process. This paper proposed a mutual authentication scheme that be suitable for RFID based on both lightweight and security. But with in-depth study, the scheme remains to be further optimized such as the lightweight. In order to improve its application efficiency in RFID environment.

REFERENCES

[1] Strategy, I. T. U., and Policy Unit. "ITU Internet Reports 2005: The internet of things." *International Telecommunication Union (ITU) (2005)*,Geneva,2005.

[2] Yang Guang, Geng Guining, Jing, et al. “Security threats and measures in Internet of things.” *Journal of Tsinghua University*,vol. 51, pp. 19-25, October, 2011.

[3] Sarma, Sanjay E., Stephen A. Weis, and Daniel Engels. “Radio frequency identification: secure risks and challenges.” *Cryptobytes*，vol. 6, pp.2-9, January,2003.

[4] Ding Zhenhua, Li Jintao, Feng Bo. “Research on security authentication protocol of RFID based on Hash function.”*Journal of Computer Research and Development*,vol. 46, pp.583-592, April,2009.

[5] Chen Y, Chou J S, Sun H M.“A novel mutual authentication scheme based on quadratic residues for RFID systems.” *Computer Networks*, vol. 52, pp.2373-2380, December,2008.

[6] Y. K. Lee, L. Batina and I. Verbauwhede, “EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol.”*2008 IEEE International Conference on RFID*, Las Vegas, NV,2008, pp. 97-104.

[7] Wang Haichun, Li Jun, Deng Shan,”Authentication protocol design-of RFID base on chaotic encryption.” *Digital Technology and App lication*,vol. 10, pp.206-208, 2015.

[8] JIN Chen-hui, Zheng Haoran, Zhang Shaowu, et al. *Cryptography*. Beijing, 2009, pp.122-124.

[9] ZHU Yue-fei, ZHANG Ya-juan, *Elliptic curve public key cryptosys tem*. Beijing, 2006, pp. 32-35.

[10] Ye Xijun, Wu Guoxin, Xu Yong, et al. “Analysis and improvement of one-time password authentication technology.” *Computer Engineering*, vol. 26, pp. 27-29, September, 2000.

[11] Xiao Youan. *Research on Elliptic Curve Cryptography*.Wuhan,2006, pp. 98-101.