Comput Syst Sci & Eng (2020) 4: 299–305

International Journal of
Computer Systems
Science & Engineering

Security of Chip Bank Card in Remote Payment Based on Risk Feature

Zheng Fang[1]*, **Junyun Cai**[1] **and Lifang Tian**[2]

[1] *School of Economics and Management, Nanjing University of Science and Technology, Nanjing City, Jiangsu Province, 210094, China*
[2] *School of Information Engineering, Huanghuai University, Zhumadian, Henan 463000, China*

Payment is a necessary thing in people's daily life, and the development of the Internet makes it possible that people can shop at home. As for chip bank card, it is an important payment method that has been developed in recent years and plays a key role in remote payment. In this study, firstly, the risk features of chip bank cards were analyzed from the general remote payment scheme. Then, based on the security technology theory, a chip bank card remote payment model using elliptic curve hybrid encryption algorithm and identity authentication technology was constructed. In terms of security testing, the National Institute of Standards and Technology (NIST) randomness test was used to illustrate the high randomness of the key, and cryptographic security formal verification method based on Hoare logic was used to illustrate the convergence of the key to the defect, which verified the high security of the chip bank card in the remote payment process.

Keywords: remote payment, chip bank card, risk features, security research, elliptic curve hybrid encryption algorithm, identity authentication

1. INTRODUCTION

Bank cards were an important payment tool and were popular with people for their unique storage capabilities. Financial Integrated Circuit (IC) card, also known as a chip bank card, is a bank card with a chip as a medium. It has a large capacity and can store information such as keys, digital certificates, fingerprints, etc. It also has a built-in micro terminal to provide cardholders with the convenience of multi-application in one card [1]. Due to its high security and convenience, banks have gradually promoted chip bank cards for magnetic stripe cards in recent years. Although its confidentiality coefficient has been greatly improved, it is not without loopholes, and its security research is very necessary [2]. There are a variety of classification methods for payment. From the perspective of payment distance, it can be divided into short-range payment and remote payment. Among them, short-range payment has good technical conditions and has received more attention and produced a lot of research results. Alexiou et al. [3] proposed a general framework that used formal analysis to verify the flexibility of the noise feedback coding (NFC) protocol short-range payment protocol for relay attacks. Zhao et al. [4] proposed a mobile payment management system based on short-distance visible light communication, which made short-range payment more secure and lower in cost. Remote payment is more difficult to study because its attributes are more complex. Slade et al. [5] conducted research on the empirical use of remote mobile payment and described in detail the development direction of remote payment. Hu et al. [6] suggested to use block-chain delay tolerance to provide banking services to remote communities. In the study, firstly, the generalized remote payment scheme was given. Then the risk features of the chip bank card were analyzed. Based on the existing security technology, a chip bank card remote payment model using elliptic curve hybrid encryption algorithm combined identity authentication technology was constructed. Finally, the National Institute of Standards and Technology (NIST) randomness test and the cryptographic security formal verification method based

*Email: lfzkaa@163.com

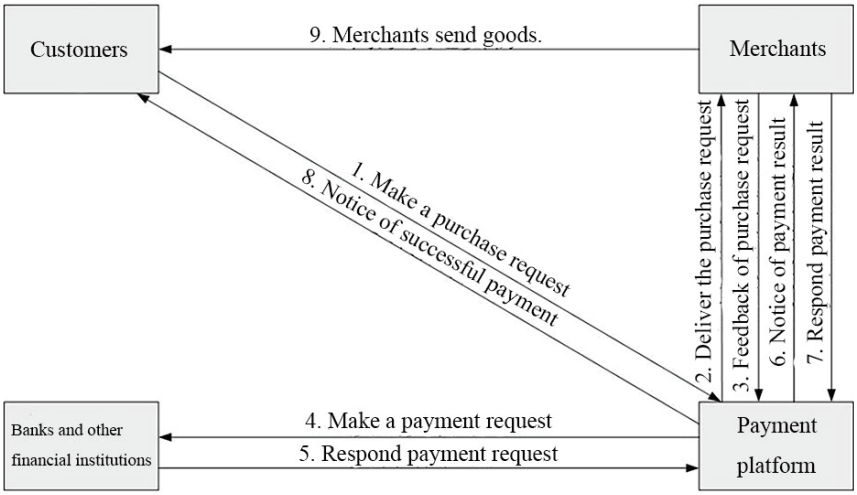

Figure 1 Remote payment plan

on Hoare logic were used for the security research. The high randomness and the convergence characteristics of the defects of the remote payment model were illustrated, providing a certain theoretical basis for the application of chip bank card in the field of remote payment.

2. INSIGHT INTO THE RISK FEATURES OF CHIP BANK CARDS WITH A GENERALIZED REMOTE PAYMENT SCHEME

Remote payment refers to the payment behavior of a person or institution by sending a payment instruction, such as online payment, telephone payment, stock trading terminal, etc., to a remote server directly or indirectly through an information operation terminal [7]. The flow of a generalized remote payment scheme is shown in Figure 1.

It is easy to know from Figure 1 that process involved in the process of remote payment in the chip bank card mainly involves that the point of sale (POS) machine reads the bank card related information, inputs the corresponding password and transmits the bank account related information. The risk features that exist in these processes are described as follow.

The security risk of password entry. The password is a security guarantee for payment, and its existence is very necessary. In the remote payment process, after using the chip bank card to swipe the POS machine, a password is needed to enter on the physical keyboard or virtual keyboard for verification. But nowadays computer viruses are invincible, and some related virus software that can record key sequence or illegally obtain passwords in other ways has been derived, which makes it possible for passwords of consumers to be stolen when making payments.

The risk of reading and transmitting transaction information. Even in the case where the password is passed the security authentication, chip bank cards still have security risks. In the process of generating an order, it is necessary to read the account information, consumption information, identity authentication information, etc. of the chip bank card and upload them to the network to provide certain credentials for the transaction process. In the process of reading and transmitting, various types of network viruses and attack software may invade and steal transaction information and data, which is disadvantageous to consumers.

3. CHIP BANK CARD RELATED SECURITY TECHNOLOGY AND REMOTE PAYMENT MODEL DESIGN

3.1 Chip Bank Card Related Security Technology

In response to the risk features of chip bank cards, scholars and experts have proposed many effective and effective means of security protection.

The first one is identity authentication technology [8]. From the authentication method, the identity authentication technology can be roughly divided into information secret-based identity authentication, trust object-based identity authentication and biometric-based identity authentication. In real life, the merged authentication method is often used. The authentication of the chip bank card belongs to the identity authentication based on the trust object. It has a digital certificate issued by a third-party authoritative certification authority (CA), uses public key management to provide authentication by binding the user's public key and the unique identification information and utilizes the non-reproducibility of smart IC cards to ensure that users' information cannot be spoofed.

The second one is digital signature technology and hash function [9]. Digital signature refers to that the sender uses a private key and a one-way function, usually a hash function, to perform a certain cryptographic transformation on the transmitted data and the receiver uses the public key to interpret the signature to verify the integrity of the data and the legitimacy of the signature. This technology not only ensures the integrity of the data, but also makes the data uninterpretable.

The third one is data encryption technology [10]. Data encryption essentially uses a secret key and encryption algorithm

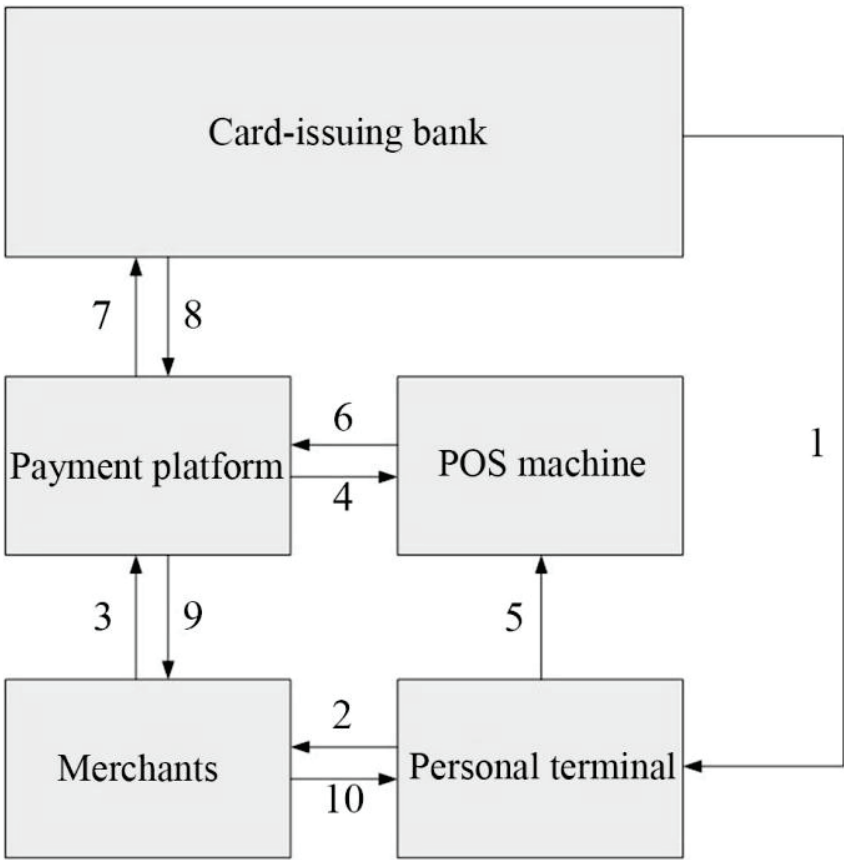

Figure 2 The flow chart of chip bank card remote payment

to encrypt plaintext into ciphertext and send it. The receiver uses the decryption function and the decryption key to restore the ciphertext to plaintext. Usually, technical means, including symmetric encryption, asymmetric encryption and hybrid encryption, are used.

3.2 Remote Payment Model of Chip Bank Card Design

Based on the above-mentioned security and confidentiality means, this study intends to use the composite design to construct the remote payment model. The elliptic curve hybrid encryption algorithm combined identity authentication technology to establish a safe and efficient path between multiple payment terminals and improve the security of the user terminal as much as possible. The flow chart of chip bank card remote payment is shown in Figure 2.

As shown in Figure 2, the issuing bank firstly sends the public key personal communication application (PCA) to the personal terminal for loading into the chip bank card as the authentication mark. When generating consumer demand, the personal terminal first transmits the purchase information to the merchant and selects the method of remote payment by the chip bank card. The merchant contacts the payment platform and simultaneously transmits the consumption information and the user information. The payment platform converts the purchase request into a purchase list and sends it to POS machine. The user checks the card after the check is made. When the public key PCA matches the user information, the POS machine feeds the information back to the payment platform. The payment platform initiates a payment request to the bank and obtains the confirmation. The payment platform feeds back the successful payment information to the merchant. Merchants hand over goods to individuals.

The key generation process of composite identity authentication technology of elliptic curve hybrid encryption algorithm [11] is as follows.

First the parameter domain is judged, and the cubic polynomial coefficient equation of the elliptic curve can be set as:

$$\begin{cases} y^2 = x^3 + ax + b \\ 4a^3 + 34b = 0 \end{cases} \tag{1}$$

and

$$y^2 + xy = x^3 + a^2x + b \tag{2}$$

A prime number p, the length of which is less than the data encryption length, but larger than 64 bits of data length of one frame, is taken, and the following equation is obtained after calculation by SEA algorithm:

$$M = \#E(F_p). \tag{3}$$

An integer m that can be exactly divided by p is selected again, $m \geqslant 2^{64}$, and as for a and b, a set of number that can satisfy Equation (1) and (2) are randomly selected. After the parameters are determined, both parties need to send the parameters to CA in real time to configure a valid key for both parties. The parameter

$G \in E(F_p)$ is generated, and Schiol algorithm is used to generate public key $B(x_Q, y_Q)$:

$$B(x_Q, y_Q) = Schol(a, b, m, p, G). \tag{4}$$

After the encryption party receives the public key $B(x_Q, y_Q)$, a random number l is generated. $0 < l < m$ is set, and Satoh algorithm is used to generate private key:

$$D = Schol(a, b, m, p, G, P). \tag{5}$$

The authoritative CA can use the Elliptic Curve Digital Signature Algorithm (ECDSA) signature technology [12] to generate a one-to-one correspondence between the public key and the private key when generating the public key. ECDSA digital signature technology can link these entities by generating unique ECDSA digital identifiers for parameters, public keys and private keys.

4. SIMULATION EXPERIMENT OF CHIP BANK CARD REMOTE PAYMENT SECURITY RESEARCH

The following part firstly introduced the method of security test and conducted simulation security experiments based on the chip bank card remote payment model which was established in the third section to draw conclusions.

4.1 Security Test Method

This study would take the NIST randomness test to illustrate the randomness of the generated key [13], also known as the Special Publication 800-22 test package, which contained 16 test methods and could be used to test the randomness of the binary sequence of any length generated by a secret random or pseudo-random number generator.

At the same time, this study would use cryptographic security formal verification method based on the Hoare logic [14] to detect the defect degree of the generated key. The Hoare logic is a formal system whose central feature is the Hoare triple. This triple describes how the execution of a piece of code changes the state of the calculation. The main role of the cryptographic security test in this study is to provide a screening criterion for defect inspection through strict mathematical logic reasoning.

4.2 Steps of Simulation Experiments

For the NIST randomness test, the simplest initial key and the initial vector generated by C++ were all as "0", and the number of key words was 40,000 key stream sequences. A binary representation of the keystream file P.txt can be run to obtained. In the Linux system, the location of the C compiler gcc was modified and the lists where the test package was located were entered, then the makefile was run to compile, and finally the file was imported to test all 16 items.

For cryptographic security formal verification method based on the Hoard logic, the main content was based on the screening criterion provided by Hoare logic, and the defects of the key were found through principal component analysis. Specific steps are as follows:

The principal component was determined. First, $X = (X_1, X_2, \ldots, X_n)^T$ was set to be the n-dimensional random vector of the key running, the running matrix could be obtained and expressed as W^T, and the linear transform could obtain $Y = (Y_1, Y_2, \ldots, Y_n)$, which is a linear set of password running. K could be set as the covariance matrix of the n-dimensional random vector. Then, when $W^T = H$, Y_i is the i-th principal component, and $i = 1, 2, \ldots, n$. It was easy to know that they were mutually independent. The n-dimensional random vector was set to constitute the feature space of secret key operation. The training data set are divided into m subsets. X^i is the sample matrix of i-th secret key operation data, which includes t samples $(X_1, X_2, \ldots, X_t)$, and there is $X_j = (X_{j1}, X_{j2}, \ldots, X_{jn})$, $j = 1, 2, \ldots, t$. Then, the covariance matrix of key operation data subsets is:

$$K_x^i = \frac{1}{t-1} \sum_{j=1}^{t} (X_j - \overline{X}^i)(X_j - \overline{X}^i)^T, \tag{6}$$

where $\overline{X}^i$ refers to the central vector of the key operation data class. Through the above operation, the principal component space of the key operation data matrix was obtained, and the principal component analysis expression is:

$$M = W^T (X - \overline{X}^i) \cdot K_x^i. \tag{7}$$

Defect screening indicators were established through Hoare logic and the results were tested. The logic model is $C = (Q, M, Q_0, T)$, where Q is the state collection of key operation, Q_0 is the initial operation condition, and $T \subseteq Q \times M \times Q_0$ is the migration relationship. Whether the key subset conforms to logical relation C is checked. If it is not,

$$safe = P_i * C + \lambda \tag{8}$$

is marked, where P_i is the protection process and the mark of the fault K_i', and λ is the number of marks. The expression of security verification result is:

$$F = (P_i + K_i') \cdot C + \delta, \tag{9}$$

where δ is the attribute value of the secret key, and F is the fault category. In this study, 2048 training dataset tests were conducted, and defect types were classified as serious threats, threats, impact operations, security risks and other issues. After the results were obtained, they were summarized into tables.

Feedback adjustment was based on marker P_i, the relevant covariance matrix K_i' was found, and the sample size t and the number m of set were adjusted to amend principal component space. Then the detection process was repeated twice to obtain the results, which was summarized in the list to obtain the analysis of key defect degree.

4.3 Results and Analysis

Firstly the results of NIST randomness test were summarized, as shown in Table 1.

Table 1 NIST randomness results of elliptic curve hybrid encryption algorithm.

Test items	P-value
Frequency test	0.316353
Block frequency test ($m = 128$)	0.787651
Cumulative sums test-forward	0.329699
Cumulative sums test-reverse	0.544568
Runs test	0.251430
Longest run test of ones in block	0.105261
Rank test for a binary matrix	0.696002
Discrete Fourier transform test	0.108547
Non-overlapping template matching tests ($m = 9$, $B = 000000001$)	0.395475
Overlapping template matching test ($m = 9$)	0.696210
Universal general statistical test	0.321845
Approximate entropy test ($m = 10$)	0.109098
Random excursions test ($x = +1$)	0.147746
Random excursions variant test ($x = -1$)	0.362478
Linear complexity test ($M = 500$)	0.544872
Serial test ($m = 16$)	0.109280

Table 2 Analysis of the defect degree of the key.

Defect types of keys	The defect number of the first round	The defect number of the second round	The defect number of the third round
Serious threats	20	11	8
Threats	33	23	18
Impact operation	12	12	11
Security risks	8	7	6
Other issues	2	2	2
Total	75	55	45

The significance level in this study was $\alpha = 0.01$. The condition of passing the tests was that all the sequence P-values in the tests should satisfy $0.01 \leqslant P \leqslant 1$. As shown in Table 1, P-values of 16 test items were all larger than the significance level $\alpha = 0.01$, which meant that the key stream sequence had very good random features. It was known in the further observation, P-values of 5 items, including block frequency test, cumulative sums test, rank test for a binary matrix, overlapping template matching test and linear complexity test, were larger than 0.5, indicating that the security performance of the encryption system were relatively good in the five aspects.

The analysis results of defect degree of the key obtained using cryptographic security formal verification method based on Hoare logic are shown in Table 2.

Table 2 shows that the number of types, serial threats and threats, were relatively more in the first round defect, which was accounted for more than half of the total amount of defects. After feedback adjustment, the defect numbers of all types of keys had a trend of decreasing, indicating that the constructive method of keys was relatively reasonable and had good convergence. Also, when facing with interference, it could record the situation, adjust in time to reduce the risk of system and increase the security performance.

The percentage form of different types of defects is shown in Figure 3.

It is obvious in Figure 3 that in the feedback adjustment, the percentage of two types of the defects, serious threats and threats, decreased; the percentage of defects of serious threats were even lower than that of impact operation after being repaired, indicating that the two types of key defects, serious threats and threats, would be recognized first and repaired. Thus, it indicated that the secret key system had good amendment logic and could do the right steps when facing the interference and repair the critical loophole first to ensure the operation of the system.

In order to verify the reliability of the chip bank card remote payment model designed in this study, the model was applied in Network Mall A. Three experiments were carried out, and three transactions were conducted each time. The transaction amount was below 200, 200–1000 and more than 1000, respectively. The test results of the model are shown in Table 3.

As shown in Table 3, the average POS feedback time was 0.37 s, the card swiping processing time was 0.86 s, the message feedback time was 9.11 s, which could all meet the requirement of remote payment. Moreover POS would give the hint that the payment exceeds monetary limitation and please choose other payment means" when the transaction amount exceeds 1000, which indicated the reliability of the system.

5. DISCUSSION

Payment system plays an important role in daily life [15]. With the development of economy and the improvement of people's living standards, there are more and more payment methods [16], and people pay more and more attention to payment security issues, such as authentication [17], user anonymity, fair exchange [18], etc. Chip bank card with high security and convenience has been more and more widely used in payment, and further analysis of its security has very important practical value.

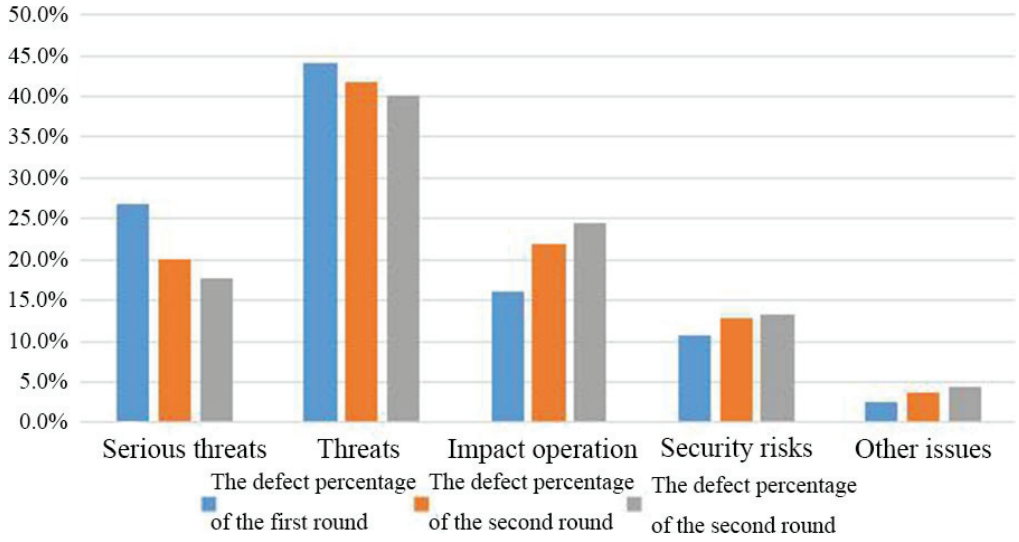

Figure 3 Percentage statistical chart of different types of defects of keys

Table 3 Model testing results.

	The 1st experiment			The 2nd experiment			The 3rd experiment		
Transaction amount/yuan	121	864	1578	11	745	1564	56	647	2017
POS feedback time/s	0.2	0.3	0.4	0.3	0.3	0.6	0.4	0.3	0.5
Card swiping processing time/s	0.7	1.1	0.8	0.9	1.2	0.8	0.9	0.2	1.1
Message feedback time/s	6	7	15	17	5	6	9	6	11

Firstly, the risk characteristics of chip bank card were analyzed, then a remote payment model of chip bank card based on elliptic curve hybrid encryption algorithm and identity authentication technology was designed. In order to verify its security, NIST randomness test was carried out first. According to the test results shown in Table 1, it was found that all the test results satisfied significance level $\alpha = 0.01$, which verified that the model had very good random characteristics. In addition, the model had excellent confidentiality performance in frequency test, cumulative and test, rank test of binary matrix, overlapping template matching test and linear complexity test, which showed that the model was reliable in the aspect of confidentiality. In the formal verification of cryptographic security based on Hoare logic, it was found from Table 2 that the degree of key defects gradually decreased with the adjustment of the model, which indicated that the model could improve security by adjusting and had a good reliability in practical application. Figure 3 proves the repair performance of the model, which was beneficial to the normal operation of the system.

Compared with other algorithms, the elliptic curve hybrid encryption algorithm and identity authentication technology used in this study had higher processing efficiency, lower resource consumption, stronger applicability in mobile terminal devices with effective storage capacity and bandwidth resources, further strengthened confidentiality and security, and better performance in the process of remote payment.

Although some achievements have been made in this study, there are still some shortcomings, such as how to drive POS more effectively to feedback financial information to users, how to further optimize encryption algorithm, and how to further verify the security of the model, which are the direction of future works.

6. CONCLUSION

In this study, the security research of chip bank card based on risk feature in remote payment was performed. Firstly, the risk features of chip bank card were analyzed based on the general remote payment scheme. Then the existing security technology was analyzed and the elliptic curve hybrid encryption algorithm combined with the identity authentication technology for the chip bank card remote payment model was constructed. Finally, the NIST randomness test was used to illustrate the high randomness of the key. The cryptographic security formal verification method based on Hoard logic was used to illustrate the convergence characteristics of the key for its defect. This work proves the security guarantee of chip bank card in the process of remote payment and provides a basis for the promotion of chip bank card.

REFERENCES

1. Dan S, Gang Z. Research on relay attack of non-contact IC card. Chinese Automation Congress. 2016.
2. Meng L, Shamsi K, Meade T, et al. Provably Secure Camouflaging Strategy for IC Protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016, PP(99):1–1.
3. Alexiou N, Basagiannis S, Petridou S. Formal security analysis of near field communication using model checking. Computers & Security, 2016:S0167404816300244.
4. Xiaomeng Z, Junjie Z, Center T I. Management System of Mobile Payment Based on Short-range Visible Light Communication. Computer & Telecommunication, 2017.

5. Slade E, Dwivedi Y, Williams M, et al. An Empirical Investigation of Remote Mobile Payment Adoption. Let's Get Engaged! Crossing the Threshold of Marketing's Engagement Era. 2016.
6. Hu Y, Manzoor A, Ekparinya P, et al. A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain. 2018.
7. Slade E L, Dwivedi Y K, Piercy N C, et al. Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust. Psychology & Marketing, 2015, 32(8):860–873.
8. Chen X. Research on User Identity Authentication Technology for Virtual Laboratory System. Sixth International Conference on Intelligent Systems Design & Engineering Applications. 2016.
9. Husni E, Leksono B, Rosa M R. Digital signature for contract signing in service commerce. International Conference on Technology. 2016.
10. Zhu W, Guo Q. Data Security and Encryption Technology Research on Smart Grid Communication System. Eighth International Conference on Measuring Technology & Mechatronics Automation. 2016.
11. Martínez G, Encinas H, Muñoz M. A Comparative Analysis of Hybrid Encryption Schemes Based on Elliptic Curves. Open Mathematics Journal, 2013, 6(1):1–8.
12. Rijswijk-Deij R V, Jonker M, Sperotto A. On the adoption of the elliptic curve digital signature algorithm (ECDSA) in DNSSEC. International Conference on Network & Service Management. 2017.
13. Zhu S, Yuan M, Lin J, et al. More Powerful and Reliable Second-Level Statistical Randomness Tests for NIST SP 800-22. International Conference on the Theory & Application of Cryptology & Information Security. 2016.
14. Bernot G, Comet J P, Khalis Z, et al. A Genetically Modified Hoare Logic. Theoretical Computer Science, 2018, 9308:8–12.
15. Abdulrahman A, Alrawais Arwa, Song Tianyi, et al. QuickCash: Secure Transfer Payment Systems. Sensors, 2017, 17(6):1376.
16. Tellez Isaac J, Sherali Z. Secure Mobile Payment Systems. IT Professional, 2014, 16(3):36–43.
17. Chaudhry S A, Farash M S, Naqvi H, et al. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electronic Commerce Research, 2016, 16(1):113–139.
18. Djuric Z, Gasevic D. FEIPS: A Secure Fair-Exchange Payment System for Internet Transactions. The Computer Journal, 2015, 58(10):2537–2556.