Mobile Payment Security in the Context of Big Data: Certificateless Public Key Cryptography

Tianhong Yang
(Corresponding author: Tianhong Yang)

Changchun Finance College
Changchun, Jilin 130028, China
(Email: t221h7@163.com)

(Received Mar. 3, 2019; Revised and Accepted Jan. 28, 2020; First Online June 14, 2020)

Abstract

The development and popularization of wireless networks and mobile terminals dramatically facilitates people's lives. Moreover, online business activities gave birth to mobile payments and extended to offline. Mobile payment has been promoted because of its convenience, so its security has been paid great attention. This study briefly introduced the mobile payment and certificateless public key cryptography technology, applied the certificateless public key cryptography technology to the mobile payment system, and simulated the security and efficiency of the mobile payment system in the wireless LAN built in the laboratory. The results showed that users and cloud platform could encrypt and decrypt information through two-way identity authentication and some private keys and public parameters in the process of mobile payment. When attackers attacked mobile payment, whether they pretended to be users or cloud platforms, decryption would fail due to lack of identity authentication and some private keys, to ensure the security of mobile payment. Moreover, they could maintain standard processing and resist the decryption from the third party when processing a large amount of payment information. Compared with public key infrastructure (PKI) based mobile payment and wireless public key infrastructure (WPKI) based mobile payment, mobile payment had higher payment efficiency.

Keywords: Certificateless Public Key Cryptography; Internet; Mobile Payment; Payment Security

1 Introduction

With the rapid development of Internet technology and wireless communication technology, our daily life has changed dramatically in recent years. The popularity of various intelligent mobile terminals makes it easier for people to access the Internet anytime and anywhere [9]. Moreover, after combining Internet technology, the traditional service industry has gradually transformed into the online digital service industry, thus promoting the development of mobile payment [2]. With the help of mobile terminals, mobile payment can initiate transactions anytime and anywhere, and the content of transactions is diverse, which significantly facilitates users. Because of the "anytime and anywhere" feature of mobile payment, users do not need to carry a large amount of cash, which is relatively safer when they go out. Compared with money, mobile payment is more convenient and secure, but it also faces similar security problems [12].

In the process of execution, mobile payment often contains a lot of private information when sending payment information to the third-party institutions such as banks and merchants. When the popularity of the mobile network is not high, the problem is not apparent. However, with the popularization of mobile networks and the progress of computer technology, the consequences are unimaginable once the user's payment information is intercepted. Therefore, the security of mobile payment is fundamental to ensure the healthy development of the online service industry. Abughazalah *et al.* [1] provided a protocol for NFC mobile phones to meet the security requirements of mobile payment, formally analyzed the protocol using CasperFDR, and found no feasible attack. Madhoun *et al.* [7] proposed to add a new security layer to strengthen the protocol against the security vulnerability of the European MasterCard protocol (EMV), and verified the security of the improved EMV using a security verification tool named Scyther.

Thammarat *et al.* [13] proposed a new NFC mobile payment protocol, which could provide fair exchange and information security in the POS transaction process and found through experiments that the protocol had more effective protection and fairness than other protocols. This study briefly introduced the mobile payment and certificateless public key cryptography technology, applied certificateless public key cryptography technology to the mobile payment system, and carried out simulation experiments on the security and efficiency of the mobile payment system are simulated in the wireless LAN built in the laboratory.

2 Mobile Payment

The basic framework of the mobile payment system is shown in Figure 1. The mobile payment system can be basically divided into six parts, from bottom to top.

The first part is the bearer network [10], including various forms of mobile networks, such as 3G, 4G, WiFi, *etc.*, which are usually provided by local communication companies and is the basis of the system and whose quality directly affects the stability of the system.

The second part is an access platform which provides various interfaces for connecting the bearer network for payment system to realize the unified interface of different kinds of payment services and integrate the payment function.

The third part is security authentication [15], which is the core component for the mobile payment system to ensure payment security and provides the system with functions such as data encryption and identity authentication. Security authentication covers the three platforms introduced later in the order, i.e., authentication is not an independent platform, but is integrated into the three platforms introduced then to ensure its security.

The fourth part is the management platform, which has functions of business support, management support, and system support for respectively managing business transaction content, merchant customer information, and system data.

The fifth part is a business platform, which includes a business system and payment system; the former provides various business services on the loose end, and the latter offers different forms of payment function [11].

The sixth part is the application platform, which is the top layer of the mobile payment system and undertakes the function of information interaction with users and merchants.

3 Certificateless Public Key Cryptography

The security of mobile payment system was ensured by the certificateless public key cryptography in this study. The certificateless public key cryptography [3] is based on the assumption of a difficult problem. No algorithm can solve the problem quickly in mathematics so that the security can be guaranteed. The algorithm of certificateless public key cryptography can be divided into seven steps:

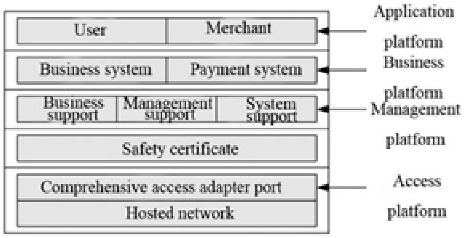


Figure 1: The basic framework of the mobile payment system

1) Firstly, through the key generation center (KGC) [5], master secrete key (msk) and public parameter [6] are obtained according to security parameter k;

2) Then msk, $params$, and ID for indicating user identity are input into KGC to obtain some private key D. D is transmitted to the corresponding user through the secure channel of the mobile network;

3) $params$ and ID are input into KGC to obtain secrete value x;

4) $params, D$ and x are combined to generate private key sk through KGC;

5) $params$ and x are combined to generate public key pk through KGC;

6) Data M which needs encryption is encrypted using $params$, sender ID, sk and receiver ID and pk, and it is transmitted to the platform of the receiver through the secure channel of mobile network;

7) After receiving the encrypted M, the receiver platform makes authentication with $params$, sender ID, sk, receiver ID and pk and decrypts it to obtain plaintext.

In the above algorithm steps of certificateless public key cryptography, Steps 1-5 are about generating encryption parameters and public and private keys about KGC, and Steps 6 and 7 are about encrypting and decrypting the plaintext information by using the encryption parameters and public and private keys. Compared with the traditional public key cryptography described above, certificateless public key cryptography avoids the management problem of public key certificate and the hosting problem of private key as the secrete key generated by KGC is only a part and will be combined with x randomly selected by user when using and the private key is stored by user.

The flow of mobile payment based on certificateless public key cryptography is shown in Figure 2. After the customer places an order on the mobile terminal, the merchant generates payment information according to the order and transmits it to the customer's mobile terminal through the secure channel of the mobile network [14].

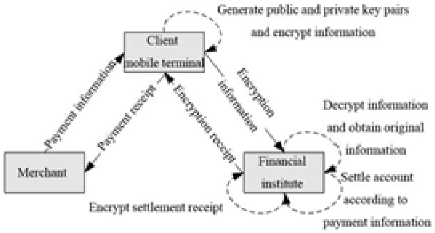


Figure 2: The mobile payment flow based on certificateless public key cryptography

Then, the public key pair is generated in the server of the mobile terminal and the payment information is encrypted.

The encrypted payment information is transmitted to the customer through the secure channel. Financial institutions decrypt the encrypted information after passing the authentication, so as to obtain the payment information, then settle the user's account according to the payment information, and generate the settlement receipt. Financial institutions also encrypt the settlement receipt by using the certificateless public key cryptography technology and transmit the encrypted receipt to the customer's mobile terminal through the secure channel. After receiving the encrypted receipt, the mobile terminal decrypts it in its server to obtain the payment receipt information and then transmits the payment receipt information to the merchant through the secure channel. After receiving the payment receipt, the merchant confirms that the payment is successful, and the whole payment process ends.

4 Simulation Experiment

4.1 Experimental Environment

In this experiment, the cloud platform was built using OpenSack [4]. The computer, mobile phone and cloud platform in the laboratory were all in the wireless LAN of the laboratory. The computer was configured with 6G memory, core i5 processor and 32-bit Windows 7 operating system; the mobile phone was configured with Android operating system, 4G memory and six-core processor; the maximum transmission speed of wireless LAN was 100 MB/s.

4.2 Experiment Setup

1) Security analysis of mobile payment based on certificateless public key cryptography.
   The experimental method was to publish the payment information including user name, order information, payment amount, *etc.*, by taking computer as the merchant, then send the payment information to the mobile phone, encrypt the payment information by the certificateless public key cryptography technology and send it to the cloud platform (the cloud platform in this experiment as a third-party financial institution) to simulate the process of mobile payment. In order to verify the security of the mobile payment system in the big data environment, 10 100 pieces of payment information were processed in the WLAN at the same time, and the processing method was the same as experiment Steps 1 and 2 above. The regular payment process was used to interact 10-100 pieces of payment information in the LAN at the same time, and the irregular third-party attacker was applied for pretending to be the platform and users in LAN. In the regular payment process experiment, the number of successful payment was counted; for the irregular payment experiment, the decryption degree of the attacker to the payment information was counted. This experiment was compared with mobile payment systems based on public key cryptography and security authentication.

2) Efficiency analysis of mobile payment based on certificateless public key cryptography.
   In this study, regular mobile payment was performed in the mobile payment system through mobile phone, and the whole mobile payment process was divided into five processes:

   a. The phase when mobile phones received payment information from merchants;
   b. The phase when mobile phones received information and sent it to the cloud platform after encryption;
   c. The phase when the cloud platform receives information, decrypts it, and sends the information to the mobile phone according to the information encryption payment receipt;
   d. The phase when the mobile phone receives the payment receipt and decrypts it and sends it to the merchant;
   e. The phase when the merchant receives the payment receipt.

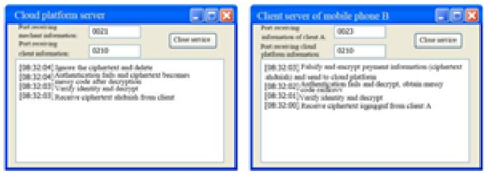
In this study, the time point of information transmission and reception was determined by the time stamp of data transmission [8], so as to calculate the time consumption of each phase. Moreover, in order to verify the efficiency of the mobile payment system proposed in this study, it was compared with two mobile payment systems based on public key cryptography and security authentication system. The total number of payment information transmitted in the experiment was 100, and the average value was taken as the final result.

4.3 Experimental Results

There is no severe problem in the regular payment; therefore considering the limited length of paper, only the background logs of the cloud platform and attacker in the irregular payment process are displayed. It was seen from

Figure 3 that mobile phone B, as an attacker, intercepted the payment information ciphertext sent by mobile phone A at 08:32:00. At that time, mobile phone B disguised itself as a cloud platform to receive the payment ciphertext and then authenticated and decrypted the ciphertext. However, as mobile phone B was not registered in the mobile system and did not master part of the private key of mobile phone A, the authentication failed, and only messy code was obtained after decryption.

As the real payment information cannot be obtained, mobile phone B attempted to forge the payment information, encrypted the forged payment information with public parameters and forged private keys, and sent it to the cloud platform. The above process lasted about 3 s according to the records. The cloud platform received the ciphertext at 08:32:03, and the cloud platform did not know whether the ciphertext was from user A at that moment and then it verified the identity of the ciphertext sender according to the registration data stored in the database and decrypted it with part of the private key and public parameters. The final identity authentication failed, and the only messy code was obtained after decryption. The cloud platform determined the payment information as invalid and deleted it.



Port receiving merchant information: 0021
Port receiving client information: 0210

```
[08:32:04] Ignore the ciphertext and delete
[08:32:04] Authentication fails and ciphertext becomes
           messy code after decryption
[08:32:03] Verify identity and decrypt
[08:32:03] Receive ciphertext [illegible] from client
```

Port receiving information of client A: 0023
Port receiving cloud platform information: 0210

```
[08:32:03] Falsify and encrypt payment information (ciphertext
[illegible]) and send to cloud platform
[08:32:02] Authentication fails and decrypt, obtain messy
           code [illegible]
[08:32:01] Verify identity and decrypt
[08:32:00] Receive ciphertext [illegible] from client A
```

Figure 3: Background logs of the cloud platform and attacker client in the regular mobile payment process

One of the characteristics of big data environment in mobile network is the huge amount of data transferred. Therefore, in order to verify the security of this mobile payment system in big data environment, mobile payment information transferred at the same time was gradually added in wireless LAN, and the system was compared with the payment system under the other two cryptography technologies. The comparison results are shown in Figure 4.

In the regular payment process, the payment system proposed in this study could effectively handle the increase of the amount of payment information that needed to be processed in the network, without payment failure; the payment system based on public key infrastructure (PKI) and the payment system based on wireless public key infrastructure (WPKI) did not show payment failure when processing 10-30 pieces of payment information, but when processing 40 or more pieces of payment information, both payment systems had payment failure, and the WPKI based payment system failed more times.

In the irregular payment process, the decryption degree of the third party attacker to the payment ciphertext of the payment system kept at about 1% with the increase of the amount of payment information, which was regarded as the decryption failure; the decryption degree of the third party attacker to the payment ciphertext of the payment system under the other two cryptography technologies increased with the increase of the amount of payment information, in which the increase of the PKI based payment system was faster.

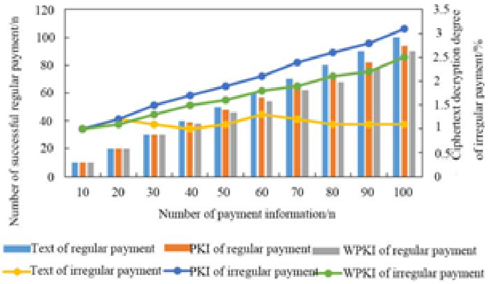


Figure 4: Security comparison of three cryptography technologies in big data environment

For mobile payment, its greatest convenience is that it can initiate transactions anytime and anywhere within the network coverage. In the existing big data environment, the amount of data transmitted in the network is very large, and the communication channel resources of the mobile network are limited, so the efficiency of mobile payment will directly affect the user's experience. The faster the payment efficiency, the lower the delay, the less the occupied channel resources, the more the mobile payment users supported. In order to verify the efficiency of the mobile payment proposed in this study, it was compared with the other two mobile payment systems, and the results are shown in Figure 5. PKI represents mobile payment based on public key cryptography, and WPKI represents mobile payment based on security authentication system. It was seen intuitively from Figure 5 that no matter what kind of mobile payment was used, the time consumed was the shortest in Steps 1 and 5, and the time consumed in Step 3 was the longest. The reason for the above phenomenon was that Steps 1 and 5 were only about the transfer of payment information and receipt information, and Step 3 not only involves encryption, but also involves decryption.

As to the comparison between the three mobile payment means at the same phase, the difference between them atSteps 1 and 5 was not large, and the reason has been described above; in Steps 2, 3, and 4, the mobile payment proposed in this study consumed the shortest time and the WPKI based mobile payment consumed the longest time. The reason for the above phenomenon was that Hash function which was used for encryption and decryption consumed more time in the computation of finite field compared to point multiplication, and the mobile payment proposed in this study used less Hash function computation in the encryption and decryption phases, and the WPKI based mobile payment needed safety certificate certification in the certificate management center in addition to Hash function computation. Finally, the average total time consumed by the mobile payment system proposed in this study was 49.28 ms, the average total time consumed by the mobile payment based on PKI was 50.72 ms, and the average total time consumed by the mobile payment based on WPKI was 51.95 ms.

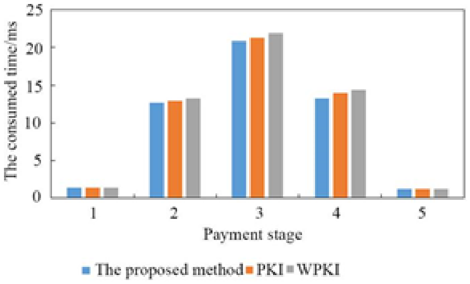


Figure 5: Comparison of mobile payment efficiency under three kinds of cryptography

5 Conclusion

This paper introduced the mobile payment and certificateless public key cryptography, applied certificateless public key cryptography to the mobile payment system, and carried out the simulation experiment on the security and efficiency of the mobile payment system in the wireless LAN built in the laboratory. The experimental results are as follows:

1) No matter another mobile terminal with the same configuration pretended to be the cloud platform to receive information or pretended to be the regular user to send information when attacking the mobile payment, it failed to pass authentication and decryption;

2) With the increase of payment information in the network, the payment system proposed in this study could ensure the success of payment in the process of regular payment and maintained a very low degree of decryption under the attack of the third party; times of failure of the other two payment systems increased with the increase of payment information to be processed, and the degree of decryption under attack also increased;

3) The average total time consumed by the mobile payment system proposed in this study was 49.28 ms, the average total time consumed by the mobile payment based on PKI was 50.72 ms, and the average total time consumed by the mobile payment based on WPKI was 51.95 ms; the phase of encryption and decryption consumed the longest time in the whole payment process.

Acknowledgment

The study is supported by Changchun Finance College "Research on Security Problems and Countermeasures of the Environment for Mobile Payments" (JZSJPT2019004).

References

[1] S. Abughazalah, K. Markantonakis, and K. Mayes, "Secure mobile payment on NFC-enabled mobile phones formally analysed using casperFDR," in *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 2014.

[2] T. Dahlberg, J. Guo, and J. Ondrus, "A critical review of mobile payment research," *Electronic Commerce Research and Applications*, vol. 14, no. 5, pp. 265-284, 2015.

[3] S. K. H. Islam, and A. Singh, "Provably secure one-round certificateless authenticated group key agreement protocol for secure communications," *Wireless Personal Communications*, vol. 85, no. 3, pp. 879-898, 2015.

[4] B. Klugah-Brown, J. B. A. K. Ansuura, and Q. Xia, "A Signcryption Scheme from Certificateless to Identity-based Environment for WSNs into IoT," *International Journal of Computer Applications*, vol. 120, no. 9, pp. 16-23, 2015.

[5] Y. Lu, and J. G. Li, "Provably secure certificateless proxy signature scheme in the Standard Model," *Theoretical Computer Science*, vol. 639, pp. 42-59, 2016.

[6] M. M. Ma, D. B. He, and N. Kumar, "Certificateless searchable public key encryption scheme for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 759-767, 2017.

[7] N. E. Madhoun, and G. Pujolle, "Security enhancements in EMV protocol for NFC mobile payment," in *IEEE Trustcom/BigDataSE/ISPA*, 2016.

[8] S. Mathi, R. Nivetha, B. Priyadharshini, and S. Padma, "A certificateless public key encryption based return routability protocol for next-generation IP mobility to enhance signalling security and reduce latency," *Sadhana*, vol. 42, no. 12, pp. 1987-1996, 2017.

[9] T. Oliveira, M. Thomas, G. Baptista, and F. Campos, "Mobile payment," *Computers in Human Behavior*, vol. 61(C), pp. 404-414, 2016.

[10] J. Ondrus, A. Gannamaneni, and K. Lyytinen, "The impact of openness on the market potential of multi-sided platforms: A case study of mobile payment platforms," *Journal of Information Technology*, vol. 30, no. 3, pp. 260-275, 2015.

[11] C. Phonthanukitithaworn, C. Sellitto, and M. W. L. Fong, "An investigation of mobile payment (m-payment) services in Thailand," *Asia-Pacific Journal*

of Business Administration, vol. 8, no. 1, pp. 37-54, 2016.

[12] E. Taylor, “Mobile payment technologies in retail: a review of potential benefits and risks,” *International Journal of Retail & Distribution Management*, vol. 44, no. 2, pp. 159-177, 2016.

[13] C. Thammarat, W. Kurutach, and S. Phoomvuthisarn, “A secure lightweight and fair exchange protocol for NFC mobile payment based on limited-use of session keys,” in *17th International Symposium on Communications and Information Technologies (ISCIT'17)*, 2017.

[14] T. Tsai, Y. Tseng, and S. Huang, “Efficient revocable certificateless public key encryption with a delegated revocation authority,” *Security and Communication Networks*, vol. 8, no. 18, pp. 3713-3725, 2016.

[15] M. H. Zhong, and H. Wu, “Research on the development of mobile payment industry chain in China,” *Journal of Computational and Theoretical Nanoscience*, vol. 14, no. 1, pp. 221-224, 2017.

Biography

Tianhong Yang, born in 1989, has gained the master's degree. She is now a lecturer in Changchun Finance College. She is interested in electronic business.