TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 09/10 pp610–620
DOI: 10.26599/TST.2018.9010031
Volume 23, Number 5, October 2018

Secure Authentication Protocol for Mobile Payment

Kai Fan*, Hui Li, Wei Jiang, Chengsheng Xiao, and Yintang Yang

Abstract: With the increasing popularity of fintech, i.e., financial technology, the e-commerce market has grown rapidly in the past decade, such that mobile devices enjoy unprecedented popularity and are playing an ever-increasing role in e-commerce. This is especially true of mobile payments, which are attracting increasing attention. However, the occurrence of many traditional financial mishaps has exposed the challenges inherent in online authentication technology that is based on traditional modes of realizing the healthy and stable development of mobile payment. In addition, this technology ensures user account security and privacy. In this paper, we propose a Secure Mutual Authentication Protocol (SMAP) based on the Universal 2nd Factor (U2F) protocol for mobile payment. To guarantee reliable service, we use an asymmetric cryptosystem for achieving mutual authentication between the server and client, which can resist fake servers and forged terminals. Compared to the modes currently used, the proposed protocol strengthens the security of user account information as well as individual privacy throughout the mobile-payment transaction process. Practical application has proven the security and convenience of the proposed protocol.

Key words: mutual authentication; security; privacy; Universal 2nd Factor (U2F); mobile payment

1 Introduction

The Internet has dramatically changed the face of the world. In this era, the Internet provides a variety of convenient services for individuals anywhere and anytime[1], having completely changed our daily lives, our ways of thinking, and the way we understand the world. With the development of mobile communication technology over time, many mobile Internet applications have become popular, thereby making us more informed and our activities more portable. In the mobile Internet field, the mobile phone has an indispensable role, and has become an inseparable life accessory for most individuals. Mobile phones maintain personal information and are used for both traditional communication as well as to interact in new ways with people and things[2]. In addition, commerce is a necessary element of social stability and constitutes an inevitable part of our daily lives. The combination of smart phones and mobile Internet technology has effectively upgraded traditional offline transactions into networked, mobile, and more efficient exchanges. Statistics reported by China's central bank show that in 2016, Japan's GDP was about 4.37 trillion dollars, whereas in China, mobile payments soared from 85.82 trillion yuan to 99.27 trillion yuan (about 14.1 trillion dollars). This indicates that mobile payment is becoming a mainstream payment method that is profoundly affecting the way we live.

China skipped over the era of credit card payment to directly enter the mobile-payment era, and is the

• Kai Fan, Hui Li, and Wei Jiang are with State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China. E-mail: kfan@mail.xidian.edu.cn; lihui@mail.xidian.edu.cn; 2450855261@qq.com.
• Chengsheng Xiao is with Shanghai Haijiye High Tech Co. Ltd, Shanghai 200000, China. E-mail: robot@haijiye.com.
• Yintang Yang is with Key Lab. of the Ministry of Education for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi'an 710071, China. E-mail: ytyang@xidian.edu.cn.
∗ To whom correspondence should be addressed.
Manuscript received: 2017-11-01; accepted: 2017-11-21

world leader in the mobile-payment field. In China, as well as in some other countries where financial technology (fintech) applications are well developed, there are many mobile payment scenarios occurring as routine aspect of daily life. People can pay for water and electricity, public trips, online shopping, and many other things by mobile-payment methods. In addition to more typical application scenarios, mobile Internet financial transactions are more numerous in China than elsewhere. Other popular scenarios include the sharing of bicycles and giving electronic red envelopes (i.e., monetary gifts). Science and technology are important driving forces of social progress. Compared with traditional payment methods, mobile payment has the following features:

(1) Digital transmission. Mobile payment uses advanced technology to digitally transmit financial transaction information, whereas the traditional payment method requires payment via the transfer of cash, notes, or bank statement.

(2) Open payment environment. The mobile-payment environment operates from an open system platform, whereas the traditional payment system operates in a relatively closed system.

(3) Advanced means of communication. In mobile payment, the demands on hardware and software resources are high, but traditional payment uses traditional communication media, which are less demanding.

(4) Other economic advantages. Mobile payment is convenient, fast, and efficient. Users simply use a networked tablet computer or mobile phone, thereby enjoying fewer geographical restrictions and the ability to complete the entire payment process in a very short period of time. Traditional payments, in contrast, involve cumbersome procedures and can be time-consuming.

Some organizations in China and other countries have defined mobile payment as follows: a transaction payment process whereby the payer uses mobile communication technology and mobile devices to initialize, authorize, or complete payment[3]. Compared with that of the past, the number of mobile phone users has skyrocketed, as has the number of accounts. Mobile payment, as a new kind of network financial service, is attracting increasing attention from researchers[4]. Moreover, with the emergence of mobile applications like Alipay and WeChat in China, mobile payment has entered a period of rapid development, and is greatly facilitating the activities of daily life, as well as spawning new Internet financial enterprises. In the United States, companies like Facebook have also begun to get involved in this field. With the gradual implementation of this concept over time, mobile payments will spread to more areas and be used by many more people. While mobile payment is popular because of its many advantages, unfortunately, it also faces many threats and security challenges. Mobile transactions face a range of security issues, such as the reliability of the transactions, the confidentiality of the data, the non-repudiation of transactions, and data integrity[5]. In many parts of the world today, no standardized programs have been established for mobile payments. To ensure payment reliability, the trading environment must be reliable and the transaction object must be true. Confidentiality of data refers to the protection of the privacy of transaction information. In addition, the transaction itself must be undeniable, which means that the participants are also undeniable, whereas data integrity refers to the prevention of malicious changes being made to the data during the transmission process.

A number of fraud problems have occasionally arisen with mobile payments in recent years, which seriously undermine the user experience. To a certain extent, fraud will also work against the popularity of the technology. More importantly, some security issues may provide opportunities for theft, thereby making the user vulnerable to huge financial losses due to mobile-payment security issues. The occurrence of such events also increases the burden on society. It is clear that security in the payment system is a major problem that must be solved. Our work in this study mainly focuses on the security of mobile-payment systems. To ensure the security of the online trading environment, we propose a Secure Mutual Authentication Protocol (SMAP) that plays an important role in the payment process. We note that traditional physical authentication devices such as USB keys[6], or similar devices produced by different organizations and which provide no unified interface standard, result in individuals carrying a variety of authentication devices, which is not only inconvenient but also full of risk. Our proposed protocol is based on the Universal 2nd Factor (U2F), which is an open standard that supports all certification services that meet these standards. In fact, a growing

number of Internet services are beginning to support the two-step certification standard, which can identify and reject forged servers and counterfeit users.

The rest of this paper is organized as follows: In Section 2, we review related work on mobile payment and its security issues. In Section 3, we propose the SMAP architecture based on U2F. We present our security analysis and performance simulation results for the protocol in Section 4. Finally, we draw our conclusions in Section 5.

2 Related Work

Mobile payment has been a growing trend in recent decades with the booming development of communication technologies like 4G. Users can purchase almost anything they desire online via their mobile phones, such that mobile payments have become incorporated into many aspects of daily life. Today, in Hangzhou, China, commuters can travel by bus or subway using only their phones[7]. Customers can buy anything they wish in supermarkets like Wal-Mart via QR code payment[8]. In addition, people can also use their phones to perform many of their daily activities, such as buying a film ticket, purchasing a cup of coffee online, or paying an automobile court fine[9]. As such, the mobile-payment process has become a very important part of e-commerce, and has developed into a convenient and relatively reliable technology.

In fact, to some extent, mobile payment has improved everyone's lives in most every sphere of activity. Several years ago, USB key technology became mainstream in the network transaction field, and people began using it for online shopping. In 2011, Yu[10] proposed a solution using the USB key for the network authentication process. On this basis, in 2012, Wang[6] proposed another online identification approach for payment that improved efficiency and feasibility. However, the authentication phase remains risky, as Trojans can be implanted into the USB key, which lead to differences in the transaction information between the computer and USB device. This means that the Trojans have falsified the transaction information, since the USB device is only responsible for providing a signature for the transaction data, never for distinguishing this information. In addition, different kinds of USB devices have provided various interfaces with no uniform standard, and the standards for USB devices vary between banks. Moreover, it is troublesome to carry USB devices, which are easily lost. Today, due to its lack of security and portability, USB devices are slowly withdrawing from the technology development stage.

As noted above, China skipped over the credit card payment phase and went directly to mobile payments. However, credit cards remain a widespread way for individuals to pay in developed and developing countries. In the United States, for instance, credit cards continue to be the main payment tool. However, the credit card involves substantial risk, being vulnerable to untrustworthy credit card readers or a skimming devices[11]. Recently, there have been many credit card attacks. For instance, as reported by the New York Times in October 2012, attackers stole customers' credit card information at 63 Barnes & Noble book stores by hacking the credit card readers[12]. As a traditional payment method, credit card payments lack security, and, to a certain extent, are not consistent with the trend of scientific and technological progress in digitization or even social development.

Nowadays, mobile payment methods are becoming more popular due to their convenience, time saving, and personalization. For example, Near-Field Communication (NFC) technology, a wireless proximity technology operating at 13.56 MHz[13], is convenient for booking travel tickets. NFC technology offers several features for mobile handsets, such as hand-free charging and fast matching[7]. With the booming development of mobile payment, NFC is now widely used in public traffic systems and supermarkets in Hangzhou, China. In addition, with the success and popularity of the O2O mode, QR code payment now has a wide range of applications. QR code requires the use of equipment for scanning. The most common method is for a mobile device with a fixed camera or scanner to read the QR code, after which the user can complete the payment via the device[14]. Today, many applications support the recognition of a QR code, including Alipay, WeChat, UC Browser, OFO, and Mobike, shown in Fig. 1.

However, mobile payment can be a double-edged sword[15]. For example, in the interaction process with NFC, the radio-frequency signal is easily hijacked. If a phone with an NFC function happens to be located close to a bank card, it can read the card number, some of the identifying information,

Fig. 1 Architecture of mobike.

and even some transaction records without inputting any authentication information. For consumers, NFC payment is convenient and fast, but brings with a security risk, in that it can lead to the disclosure of information contained in consumers' bank cards. In addition, QR code payment also has some weaknesses, such as its vulnerability to dirt and damage. If stained or tarnished, mobile devices cannot read the QR code. Also, currently, some QR code reading tools cannot recognize malicious websites or intercept risky URLs, which leads to the proliferation of mobile phone viruses and the potential for huge financial loss to the consumer.

Since mobile phones have been embedded with the Universal Identification Module (USIM) card, they have become the most widespread mobile device ever used. Global telecom operators, without exception, are engaged in mobile-payment services for an increasing number of electronic payment markets. In this paper, we propose a protocol, SMAP, for use in mobile payments, which embeds a secure working environment in the USIM card that enhances the privacy and security of users.

3 SMAP

3.1 Fast IDentity Online (FIDO)

3.1.1 Introduction of FIDO

Biometric identification technologies, including fingerprint, face, and iris recognition, are becoming increasingly mature, whereas mobile identity authentication technologies are tending to diversify. At the same time, mobile devices are fragmented, as are their interfaces, because there is no unified authentication protocol that is compatible with the range of authentication methods. Problems like compatibility are becoming more and more difficult to address. The FIDO standard represents the best innovative mobile identity authentication practice in the industry, and can provide a good solution to the above problems, by "separating the authentication mode and authentication protocol, and taking advantage of hardware equipment capabilities that can be embedded with security modules, they can ensure the same level of support for the different authentication methods utilized by various devices and applications"[16]. In July 2012, the FIDO Union was nominally established, with six initial companies involved: PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon, and Agnitio. Today, more than two hundred companies or enterprises have membership, including Alibaba, Google, and RSA. In December 2014, FIDO launched its technical specification version 1.0, which includes a Universal Authentication Framework (UAF) standard that uses no password, and a U2F standard that provides a "two-factor experience" (passwords and specific devices), as shown in Fig. 2. In addition to solving a range of identity authentication problems, FIDO also addresses problems with the traditional mobile authentication method being too centralized and inconvenient to input, with respect to the password or SMS authentication code.

3.1.2 Passwordless UX

The passwordless FIDO experience is supported by the UAF protocol, in which users register their devices with the online service by selecting a local authentication

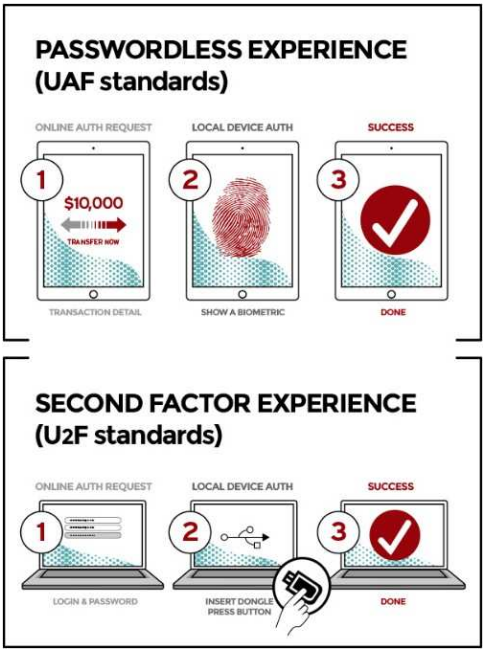

Fig. 2 UAF and U2F standards.

mechanism, e.g., swiping a finger, looking at the camera, speaking into the microphone, or entering a PIN. The UAF protocol allows the service to select which mechanisms are offered to the user. Once registered, users simply repeat the local authentication action whenever they need to authenticate a transaction for the service. This dispenses with the need to enter a password when authenticating a transaction from that device. The UAF also allows the combination of multiple authentication mechanisms, such as a fingerprint + PIN.

3.1.3 U2F protocol

The second-factor FIDO experience is supported by the U2F protocol, which allows online services to augment the security of their existing password infrastructure by adding a strong second factor to the user login process. With U2F, the user logs in with a username and password as before, and the service can also prompt the user to present a second-factor identification at any time. The strong second factor allows the service to simplify its passwords (e.g., 4-digit PIN) without compromising security. During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. Users can use their FIDO U2F devices for all online services that support the protocol to leverage the built-in support in web browsers, and websites can simplify the required password when a user carries a U2F device with built-in support in the web browser.

3.2 Proposed SMAP

In mobile payments, online certification plays a vital role in ensuring a safe payment environment for users. In this section, to address the security and convenience issues of mobile payments, we present a SMAP that is based on the theory of the U2F mechanism to achieve secure authentication between the user and website. Figure 3 shows the overall workflow of the proposed protocol architecture. The precondition for the smooth operation of this protocol is that the U2F device has built-in support in web browsers. We use an asymmetric cryptosystem in this SMAP during the mutual authentication between mobile terminals (e.g., a mobile phone) and the website. The protocol is divided into two phases—online registration and online certification. During registration with an online service, the user's client device (mobile phone) creates a new key pair. A private key is retained in the device locally and a public key is registered in the website with

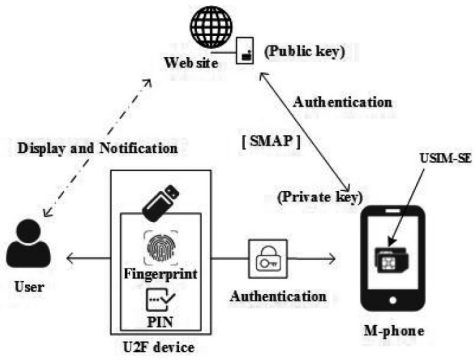

Fig. 3 Proposed protocol architecture.

the online service. Authentication is performed by the client device—it proves to the service that it possesses the private key by signing a challenge sent from the website. The client's private key can be used only after it is unlocked locally on the device by the user. That is, only a valid user can access the private key, which is guaranteed via the successful authentication exchange between the user and the device. The local unlock is accomplished by a user-friendly and secure action such as swiping a finger, entering a PIN, inserting a second-factor device, or pressing a button.

As illustrated in Fig. 3, the authentication process in this system is mutual. In the mobile-payment environment, this intact protocol has two steps: registration and authentication. The first can be regarded as an initialization step, which provides a channel for both the server and user to store some cryptographic information for use in the next phase. Cryptography is used in the authentication process to ensure the reliability of both the server and client, thereby guaranteeing security[17]. In addition, a Secure Element (SE) is embedded in the USIM card, which is responsible for identification and computation.

3.2.1 Notation

Before introducing the details of the workflow, we first explain the notations used, as shown in Table 1.

3.2.2 Registration phase

In this phase, the user must choose an available U2F authenticator that is compatible with the online service's acceptance policy. Then, the user unlocks the U2F authenticator to reach a mobile client using a fingerprint reader, a button on a second-factor device, a securely entered PIN, or other similar method. An asymmetric cryptosystem is used, as noted above, for the user's device to create a new public/private key pair that is unique to the local device, the online server,

Table 1 The summary of the notations used in the scheme.

Notation	Description
Fingerprint	Fingerprint identification
PIN	PIN code
K_1	Private key
K_2	Public key
K_d	Key handle used for searching K_2
RN	A random number generated by the device
M0	Transaction information
M1	Payment data
M2	Transaction result
C_s	Challenge value generated by the server
S_m	Signature value operated by the device
XOR	Bitwise xor operation
$H()$	Hash operation

and the user's account. The public key is sent to the online service (website) and is associated with the user's account. The private key and any information regarding the local authentication method (such as biometric measurements) will always remain in the device. The integrated registration procedure, as shown in Fig. 4, involves the following interactive steps:

(1) User mobile phone: Establishes an identification between the user and the mobile device with a fingerprint, PIN, or other similar method.

(2) Mobile phone: The USIM card with the embedded SE module in the mobile device generates a pair of keys (K_1, K_2) for the local device and the online server. And then the SE module creates the K_d. A hash value of $h_1 = H(K_2, K_d)$ is locally computed.

(3) Mobile phone server: The mobile phone stores the private key in the local device and sends the public key, the key handle, and their hash values to the server.

(4) Server: At this end, the K_2 and K_d are stored, then the server computes the hash value $h_2 = H(K_2, K_d)$, and conducts an XOR operation using h_1. If the result is not zero, this indicates that the information sent from the mobile device to the server has been changed, so the registration fails. Otherwise, the registration is successful and the server sends an acknowledgment (ACK) response to the mobile device.

(5) User mobile phone: Upon viewing the ACK response, the user unlocks the device using one of the methods listed above.

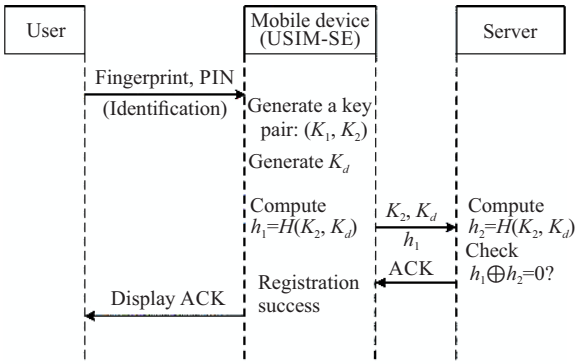

Fig. 4 Registration phase.

In this registration phase, as shown in Fig. 4, we can see that all the preparatory work is completed and ready for the next phase. The first step guarantees that the user can access the mobile device by the way of fingerprint or PIN code. The public key K_2, which is sent to the server and pertains to the user's account K_d, is used for searching K_2 based on the private key K_1. At the server end, the binary XOR operation between the calculated hash value h_2 and the received hash value h_1 ensures that the data sent from the mobile device to the server is secure. If the result of the XOR operation is zero, this means that the values h_1 and h_2 are equal, which indicates that the registration keys have not been falsified. If ok, the ACK response is sent to the mobile device and is displayed to the user. At this point, the registration has been completed smoothly.

3.2.3 Authentication phase

If the user wants to utilize an online payment service for the first time, the registration phase is an indispensable first step. Some relevant information will be sent to the user's own account during this procedure. In addition, if the user wants to be assured of a good online shopping experience, the certification process is necessary and will play an important role. This process involves the use of the asymmetric cryptosystem mechanism to perform information exchange, as well as a mutual authentication process, in which user-initiated transaction information and the online payment service information are strictly compared. When their consistency is confirmed, only then will payment occur. If the information is inconsistent, this indicates that the transaction has been tampered with, and the user can directly end the transaction. This certification process is effective for helping users to avoid phishing sites. As shown in Fig. 5, the authentication process is divided into six steps.

When registration is complete, the private key is stored in the SE module in the mobile device, whereas the public key and key handle are stored in the online server. When a user performs an online mobile

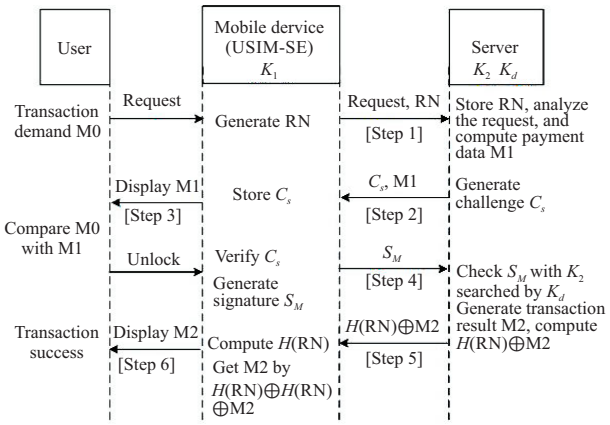

Fig. 5 Authentication phase.

payment, the entire transaction also comprises six steps, the details of which are as follows:

Step 1 The user initiates an online transaction by sending a request to the mobile device. Based on this request, the mobile device (USIM-SE) generates a Random Number (RN) locally, and then sends both the request and the RN to the server.

Step 2 After receiving and storing the RN, the server analyzes the transaction request, transforms it into payment data, and computes it correctly, which is denoted as M1. Next, the server generates a challenge C_s based on the public key K_1 that had been stored earlier during registration. Then, the server sends the challenge C_s and the M1 to the mobile device.

Step 3 C_s is stored in mobile device (USIM-SE). The payment data M1 is displayed to the user via a popup or other similar method on the screen. Based on the M1, the user can compare the payment data with the previous transaction information M0 created by the user's own demand. If they do not match, this indicates that the transaction request has been falsified, so the user can stop the transaction to avoid any financial loss from a wrong payment. However, if M1 matches M0, this confirms that the transaction data is unchanged and the transaction payment data is correct, so the user can unlock the SE by fingerprint, simplified PIN code, or other similar method.

Step 4 After being unlocked by a valid user, the SE will verify the challenge C_s previously stored locally. Then, the SE generates a signature S_M with the local private key K_1 to respond to the challenge C_s and the S_M will be sent to the server.

Step 5 The server searches the public key K_2 based on the key handle K_d, and uses it to verify the signature S_M. If successful, the server will generate the transaction result, denoted by M2, then compute the value H(RN) ⊕ M2 and send it to the mobile device (USIM-SE).

Step 6 Compute H(RN) with the local RN in SE, and obtain the M2 by H(RN) ⊕ H(RN) ⊕ M2. Then, the mobile device displays the M2 transaction result to the user. The authentication process is then complete and the whole transaction has been smoothly executed.

From the steps described above, we know that the private key K_1 is stored in the SE module and the public key K_2 in the server. These keys are never transferred to the other ends in any form, plaintext or ciphertext. In Step 3, the user compares M1 with M0 to determine whether the transaction information has been falsified. Verification is conducted several times by the user, mobile device, and server, which ensures that no transaction information has been falsified. In addition, the validity of the user is confirmed in Step 3 by the unique biological fingerprint or simplified PIN code. This ensures that only the user can unlock the SE. The security of the communication channel between the server and mobile device is safeguarded through the mechanism of the asymmetric cryptosystem. Therefore, this system architecture works well in defending against phishing sites.

4 Security Analysis and Practical Evaluation

In this section, we analyze and evaluate the proposed protocol. To our knowledge, there have as yet been no similar payment U2F-based architectures reported with respect to mobile payment. Therefore, in lieu of conducting a comparative analysis of the performance of our proposed protocol with that of others, we evaluate the performance of the proposed protocol architecture itself with our simulation experiment results.

4.1 Security analysis

Of the various payment modes available, mobile payment is becoming increasingly popular and accepted, especially in China. Due to its superior convenience and ongoing advances, mobile payment is expected to be the main payment method throughout the world in the future. From Fig. 3, we can see that many advanced technologies will utilized in the field of mobile payment, including biotechnologies, such as the existing fingerprint, iris, and face identifications. Mobile payment is a developing megatrend. With

respect to our proposed protocol, to ensure that the user is the valid owner of the mobile device, as shown in Fig. 3, we can see that the SE module embedded in the USIM card in the mobile phone is locked by default, and the user unlocks the mobile phone with a fingerprint, PIN code, or other similar method. In this protocol, we developed the SE module into a Trusted Execution Environment (TEE), which is responsible for the cryptography computation.

During the registration phase, the user unlocks the SE, and the SE generates a new key pair (K_1, K_2) and a key handle for searching the server. The private key K_1 is stored locally in the SE module and the public key K_2 is kept in the server. These keys are never transferred out, even in the authentication phase, which means that intruders cannot obtain the key pair by any method. In this procedure, the server checks h_2 with h_1 to ensure that received K_2 as well as K_d is right, and that the communication channel between the mobile device and server has not been invaded. The whole transaction process takes place without inputting any username or password to the server, so the user's account information cannot be revealed. Therefore, the proposed protocol performs well with respect to privacy protection and the security of the key pair and user account.

In the authentication phase shown in Fig. 5, when a user launches a transaction request, an RN is generated in the SE, which is used in Steps 1 and 5. This RN must be regenerated when the next round of the online transaction is conducted, so even if this random number is obtained illegally, it cannot be used in the future transaction for verifying the transaction information in Step 5. Therefore, to some extent, this proposed protocol is capable of anti-replay[18].

Another popular mobile-payment approach is based on the fact that many QR code readers cannot recognize malicious URLs[19] when using QR payment, which puts the financial security of users at great risk. However, we use an asymmetric cryptosystem in this payment architecture, which can ensure the authenticity of the entities (i.e., user, mobile device, and server) throughout the transaction. By verifying the challenge sent from the server to the SE end, and checking the signature generated by the SE at the server end, the reliabilities of the server and user are guaranteed. If the verifications and comparison by the mobile device regarding the challenge fail, this shows that the server is fake, so the user can abandon the transaction and the payment by the mobile phone will be stopped. In the opposite case, by authenticating the signature from the mobile phone, the server can also guarantee the validity of the user because only the valid user can unlock the SE and have the SE generate a signature. As such, the mutual authentication protocol is anti-counterfeit, and can ensure the security of the user's account.

In Fig. 5, we can see that the user makes a transaction request when a need arises. When the payment data is displayed on the mobile device after three steps, the user can check that it matches the initial request. When they are verified as consistent, only then will the transaction be executed. The purpose of the comparison is to ascertain whether the communication data has been intentionally falsified. In the opposite case, if they are different, this means that the data have been changed and the user can then refuse the transaction to avoid any wrongful payment. In this way, this protocol solves the problem of forged and altered information.

4.2 Practical evaluation

As discussed earlier, recognition may fail to occur when a QR code has been tarnished or stained, and contactless cognition technology also places a high demand on the system's software and hardware. In contrast, in the proposed mutual authentication protocol, the SE embedded in the USIM card functions as a TEE that is responsible for cryptography computation. This TEE exists only in the mobile phone, which no one can take away or destroy. In addition, almost all the operations are online, so no external physical damage will affect it.

Not only does the proposed protocol perform well with respect to security, it also exhibits good operating performance. In light of the lack of research studies based on U2F in the mobile payment field, we performed a simulation analysis on the basis of our experimental results, rather than any comparative analysis. Throughout the authentication procedure, the experiment data regarding time consumption, which mainly focused on the asymmetric cryptosystem, shows the protocol performance to be good.

In Step 4 in Fig. 5, we can see that the server generates a challenge C_s using the public key K_2, as shown in Fig. 6.

The SE module is a trusted execution environment. After receiving the challenge C_s, the SE module addresses it and generates a signature in response. In our experiment, we conducted this partial procedure more than 60 times. The time consumed by this phase

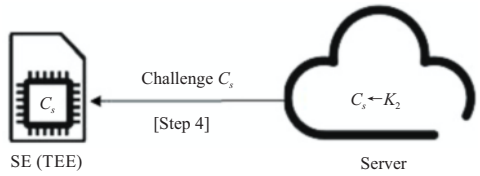

Fig. 6 Challenge operation.

each time was random to a certain degree, as shown in Fig. 7, with the scattergrams being decentralized over a range from 1.05 s to 1.15 s. Despite this result, the time consumption in Fig. 7 shows that most scattergrams float up and down in 1.1 s. Compared to the sequence of our experiments, the Matlab simulation result showed an average time consumption for generating a signature in the SE module of about 1.11 s, as indicated by the black solid line in the graph. This means that the time cost for the SE to verify the challenge and generate a signature is about 1.11 s, which represents a time savings, relatively speaking.

Next, we simulated and analyzed the time consumed in Step 4. In Fig. 5, we can see that, in Step 4, the server verifies the signature S_M using the stored public key K_2 searched by the key handle K_d, as illustrated in Fig. 8. We performed this part of the procedure more than 9000 times, the results of which are shown in Fig. 9. From these results, we can see that with increased authentication times, the time consumption increases almost linearly overall.

In Fig. 9, the black line indicates the practical experiment simulation results, and the red line the simulation average, most of which overlap. According to these experiment data, the slope of the red line is 0.003, which means that the time cost of the server

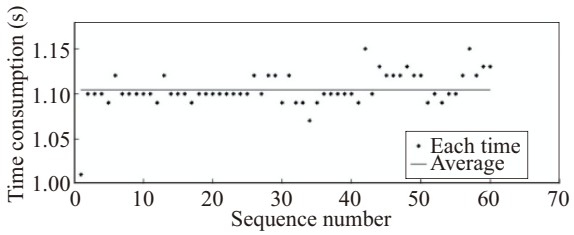

Fig. 7 Time consumption of generating signature in SE.

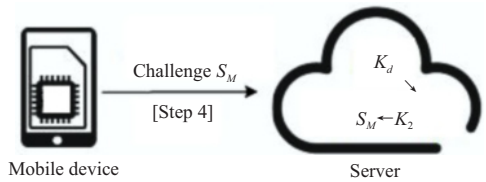

Fig. 8 Signature verification in server.

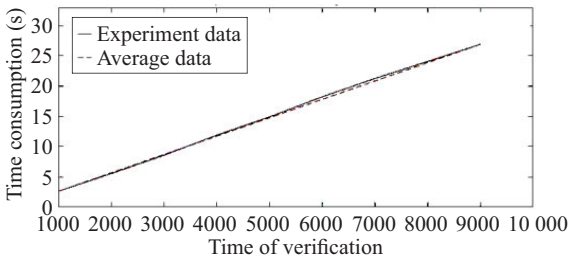

Fig. 9 Time cost of verifying the signature in server.

authentication of the signature using the stored public key is calculated in about 3 milliseconds. In general, we can conclude that the mutual authentication process occurs fast, which makes for a successful mobile-payment experience. More importantly, it is also much safer. In today's world, time is a valuable resource and security plays a vital role in a pleasant payment experience. The proposed protocol we have presented in this article performs well with respect to both time cost and security. In addition, with the further rapid development of mobile fintech, the relationship between mobile devices and users is becoming closer, especially in this age of artificial intelligence. As a vital accessory, the mobile device is very portable and has become an unconscious addition to our everyday lives. As it becomes even more convenient and safe to use mobile devices in mobile fintech, the use of mobile payments will continue to flourish.

5 Conclusion

With the rapid evolution of mobile-payment technology, modes for making mobile payments will be increasingly popular. As noted above, mobile payment can be a double-edged sword. On one hand, it provides convenience in almost every respect to its users, such as for traveling, shopping, and paying fees. On the other hand, hostile attacks can harm the user account and result in great financial loss. In this paper, we found the proposed SMAP to work well in protecting the security of the user's account and improving the payment experience with low time consumption. In addition, this protocol architecture is based on U2F, which provides a unified payment model, with no need for the use of various payment tools, which will greatly contribute to the development of payment technology.

Acknowledgment

This work was supported by the National Key R&D

Program of China (No. 2017YFB0802600), the National Natural Science Foundation of China (Nos. 61772403 and U1401251), the Natural Science Basic Research Plan in Shaanxi Province of China (No. 2017JM6004), and National 111 Program of China (Nos. B16037 and B08038).

References

[1] J. C. Liou and S. Bhashyam, A feasible and cost effective two-factor authentication for online transactions, in *Proc. 2nd Int. Software Engineering and Data Mining Conf.*, Chengdu, China, 2010, pp. 47–51.

[2] S. Nseir, N. Hirzallah, and M. Aqel, A secure mobile payment system using QR code, in *Proc. 5th Int. Computer Science and Information Technology Conf.*, Amman, Jordan, 2013, pp. 111–114.

[3] Z. Sahnoune, E. Aïmeur, G. E. Haddad, and R. Sokoudjou, Watch your mobile payment: An empirical study of privacy disclosure, in *Proc. 2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 934–941.

[4] M. Shao, J. Fan, and Y. Li, An empirical study on consumer acceptance of mobile payment based on the perceived risk and trust, in *Proc. 2014 Int. Cyber-Enabled Distributed Computing and Knowledge Discovery Conf.*, Shanghai, China, 2014, pp. 312–317.

[5] H. Jiang, Study on mobile e-commerce security payment system, in *Proc. 2008 Int. Electronic Commerce and Security Symposium*, Guangzhou, China, 2008, pp. 754–757.

[6] C. Wang, The solution design using USB key for network security authentication, in *Proc. 4th Int. Computational Intelligence and Communication Networks Conf.*, Mathura, India, 2012, pp. 766–769.

[7] I. Turk and A. Cosar, An open, NFC enabler independent Mobile payment and identification method: NFC feature box, in *Proc. 17th Int. A World of Wireless, Mobile and Multimedia Networks (WoWMoM) Symposium*, Coimbra, Portugal, 2016, pp. 1–3.

[8] Z. Čović, Ü. Viktor, J. Simon, D. Dobrilović, and Ž. Stojanov, Usage of QR codes in web based system for the electronic market research, in *Proc. 14th Int. Intelligent Systems and Informatics Symposium*, Subotica, Portugal, 2016, pp. 187–192.

[9] K. Fan, N. Ge, Y. Gong, H. Li, R. Su, and Y. Yang, An ultra-lightweight RFID authentication scheme for mobile commerce, *Peer-to-Peer Netw. Appl.,* vol. 10, no. 2, pp. 368–376, 2017.

[10] J. Yu, The program design for the network security authentication based on the USB Key technology, in *Proc. 2011 Int. Electronic & Mechanical Engineering and Information Technology Conf.*, Harbin, China, 2011, pp. 2215–2218.

[11] Y. Cao, X. Pan, and Y. Chen, SafePay: Protecting against credit card forgery with existing magnetic card readers, in *Proc. 2015 Int. Communications and Network Security (CNS) Conf.*, Florence, Italy, 2015, pp. 164–172.

[12] M. Schmidt and N. Perlroth, Credit card data breach at barnes & noble stores, http://www.nytimes.com/2012/10/24/business/hackersget-credit-data-at-barnes-noble.html?r=1&adxnnl=1&adxnnlx=1363194210-ff1jKgh5cV-LKuz8egxYwCmw, 2012.

[13] N. E. Madhoun, F. Guenane, and G. Pujolle, An online security protocol for NFC payment: Formally analyzed by the scyther tool, in *Proc. 2016 Int. Mobile and Secure Services (MobiSecServ) Conf.*, Gainesville, FL, USA, 2016, pp. 1–7.

[14] A. Choche and H. R. Arabnia, A methodology to conceal QR codes for security applications, in *Proc. Int. Information and Knowledge Engineering Conf.*, Las Vegas, NV, USA, 2011, pp. 151–160.

[15] A. M. Alshahrani and S. Walker, NFC performance in mobile payment service compared with an SMS—based solution, in *Proc. 2013 Int. Green Computing, Communication and Conservation of Energy (ICGCE) Conf.*, Chennai, India, 2013, pp. 282–286.

[16] V. E. Von Bokern, P. Goel, S. Schrecker, and N. M. Smith, Hardware-based device authentication, US Patent 8955075, February 10, 2015.

[17] Y. S. Lee, H. J. Lee, and E. Alasaarela, Mutual authentication in wireless body sensor networks (WBSN) based on Physical Unclonable Function (PUF), in *Proc. 9th Int. Wireless Communications and Mobile Computing Conference (IWCMC) Conf.*, Sardinia, Italy, 2013, pp. 1314–1318.

[18] C. Zhang, W. Zhang, and H. Mu, A mutual authentication security RFID protocol based on time stamp, in *Proc. 1st Int. Computational Intelligence Theory, Systems and Applications (CCITSA) Conf.*, Yilan, China, 2015, pp. 166–170.

[19] T. Marktscheffel, W. Gottschlich, W. Popp, P. Werli, S. D. Fink, A. Bilzhause, and H. Meer, QR code based mutual authentication protocol for Internet of Things, in *Proc. 17th Int. A World of Wireless, Mobile and Multimedia Networks (WoWMoM) Symposium*, Coimbra, Portugal, 2016, pp. 1–6.

Kai Fan received the BS, MS, and PhD degrees from Xidian University, China, in 2002, 2005, and 2007, respectively. He is working as an associate professor in State Key Laboratory of Integrated Service Networks at Xidian University. He has published over 40 papers in journals and conferences. He received 3 Chinese patents. He has managed 5 national research projects. His research interests include cloud computing security, IoT security, and information security.

Hui Li received the BS degree from Fudan University in 1990. He received the MS degree and PhD degree in telecommunications and information system from Xidian University in 1993 and 1998, respectively. He is now a professor of Xidian University. His research interests include network and information security.

Wei Jiang received the BS degree from Xidian University in 2015. He is studying as a master student in State Key Laboratory of Integrated Service Networks at Xidian University. His research interest is RFID security.

Chengsheng Xiao received the BS degree from Xidian University in 1993. He is now the technical director of Shanghai Haijiye High Tech Co. Ltd. His research interests include information security and analysis.

Yintang Yang received the BS degree from Fudan University in 1990, and the MS degree and PhD degree in telecommunications and information system from Xidian University in 1993 and 1998, respectively. He is now a professor of Xidian University. His research interests include network and information security.