IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 12, 2021, accepted August 22, 2021, date of publication August 26, 2021, date of current version September 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3108189

Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance

YUKUN ZHOU[1], BAIDONG HU[2], YITAO ZHANG[3,4], AND WEIMING CAI[3]

[1]Applied Engineering College, Zhejiang Business College, Hangzhou 310053, China
[2]Hangzhou Sunyard Technology Company Ltd., Hangzhou 310053, China
[3]School of Information Science and Engineering, NingboTech University, Ningbo 315100, China
[4]College of Control Science and Engineering, Zhejiang University, Hangzhou 310058, China

Corresponding author: Weiming Cai (caiwm@nit.zju.edu.cn)

This work was supported in part by Zhejiang Basic Public Welfare Research Program Project of China under Grant LGF20F010002, in part by the Scientific Research Project of Zhejiang Provincial Department of Education under Grant Y202045049, in part by the Visiting Engineer of Zhejiang Province "School-Enterprise Cooperation Project" under Grant FG2020113, in part by the Technical Commissioner Team of Ningbo City under Grant 2018-65, and in part by the Major Special Projects of Ningbo City under Grant 2019B10079.

ABSTRACT QR code payment plays an indispensable role in the mobile payment market, and the security of scanning codes has always been a problem in the field of information security. Static QR codes are easily copied and replaced, and there are huge security loopholes. The QR code payment in a closed system still faces security challenges. In order to solve the security problem of QR code payment, we have studied dynamic QR code payment system that supports SM2, SM3, and SM4 cryptographic algorithms, which can realize QR code scanning and scanned transactions, UnionPay cloud QuickPass transactions, etc., and generate dynamic QR code information in real time during the transaction process, one order and one code. Through dynamic algorithm distribution, the randomness and uniqueness of QR code generation are guaranteed, and it is suitable for multi-scene application transactions. The algorithm correctness test result shows that the system has achieved the expected effect. The performance test results show that the hardware of the security module implements the algorithm flow and improves the payment performance. Compared with some other algorithms, the processing time is shorter, the running speed is faster, and the system is more secure.

INDEX TERMS Cryptographic protocols, product codes, software algorithms, data security, embedded software.

I. INTRODUCTION

QR code payment is currently the most commonly used mobile payment method. Juniper Research shows QR code payment users to reach 2.2 billion globally by 2025. Although there are many advantages, but scanning code security is still a big problem. A large number of static QR codes in the form of stickers or cards have been used in the market for a long time to collect or transfer funds. Criminals have seized this feature to tamper, replace or cover the QR codes, and steal business income of merchants and users' personal information with highly concealed means. The ≪Barcode Payment Business Specification (Trial)≫ issued by the People's Bank of China requires that QR code payment be determined according to the strength of the transaction verification method and how much the limit is [1]. The cumulative transaction amount of the same customer's single bank account or all payment accounts in a single day using static scan code payment shall not exceed 500 yuan. The Alipay and WeChat static QR codes commonly used by small and micro enterprise operators are restricted to extremely low daily cumulative amounts due to their low-risk prevention capabilities.

Static barcodes are low in security, easy to be tampered with or implanted with Trojan horses and other security issues that need to be solved urgently, data or file encryption protection during the payment process is often subject to various attacks. The data encryption system adopts general

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

algorithms and software pseudo-random numbers, etc., which cannot guarantee transmission security, often in a state of being attacked. The hash algorithm SHA-256 is described in [2] to generate dynamic payment keys. During the payment process, the dynamic QR code is generated every 60s, while the dynamic QR code of our system is automatically refreshed every 5s, which is more time-sensitive. The SM3 encryption algorithm is an improved algorithm based on SHA-256, it mainly produces data message digests for the system, the algorithm design is complex. At present, there are fewer attacks on it and the security is relatively high. Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code is discussed in [3]. The prospects security anti-counterfeit application and the background anti-counterfeit application are realized by the technology of visual secret sharing and QR code (VSSQR) scheme, which can greatly improve the security of QR code payment. The security of QR code payment is improved by software encryption program. But hardware encryption will be more secure and efficient in data application capacity processing, SM2, SM3 algorithm data encryption of the system is implemented by the security module hardware; SM4 algorithm data encryption is provided by the software algorithm library, it makes QR code payment more secure. In the process of data transmission, the data in near field communication (NFC) mobile payment is encrypted and decrypted by the advanced encryption standard (AES) algorithm, which is described in [4], that's OK for payment system with a small amount of data. But the key scheduling algorithm of AES algorithm is more complex, and decryption algorithm also needs to write additional code, the implementation is more complex. The algorithm of key scheduling and encryption of SM4 algorithm is basically the same, and the order of the keys is reversed when decrypting, which is simpler to realize. At present, the reference research mostly focuses on the realization of payment system security by software applications or a single algorithm. Our system is implemented by three algorithms encryption, and hardware encryption ensures data security, compared with the existing system, improve the security of payment.

Aiming at the security problems in the payment process, a dynamic QR code payment system based on cryptographic algorithm is proposed, the algorithm is published by State Cryptography Administration in China, SM2 is the elliptic curve public key cryptographic algorithm, SM3 is the cryptographic hash algorithm, SM4 is the block symmetric cryptographic algorithm. The dynamic QR code payment system can be used to pay small amounts of funds between two or more cardholders. For example, cardholder A uses the ''receiving'' service of the mobile banking client to show cardholder B a QR code containing the payment information, and B uses his mobile client to scan the QR code to obtain the payment information, and then complete payment to A [5]. In the choice of encryption algorithm, the system adopts the cryptographic algorithm with higher security, which makes the instant message transmission more secure. The system algorithm is implemented by the security encryption module hardware, which has higher security performance, and overcomes the disadvantages of the previous data encryption system using general algorithm and software pseudo-random number [6]. The security module has the function of encrypting the internal memory data of the chip and supports the operation of encryption. Storing in unreadable plaintext increases the security of the memory, which makes it impossible for external users to obtain sensitive data information by reading data directly. The system's hardware ''destroyed automatically after being taken apart'' function and software ''firmware encryption, self-test'' function makes sure that the terminal and transaction process are security. In the security environment, after clearing the attack state, the security key is regenerated and the master key is encrypted to make the data transmission more secure. The hardware part also supports a variety of attack detection functions, it has low power consumption and low cost for the system, which is easy to be applied in multiple scenes. Through password center detection, the performance and correctness of the algorithm are verified, the performance and rate of secure payment achieve the expected results.

II. PRINCIPLE AND METHODS

A. SYSTEM ARCHITECTURE AND HARDWARE DESIGN

The system can implement QR code main scan and scanned payment, as well as contactless card, NFC (Near Field Communication) small-amount password-free and visa-free payment, and generate dynamic QR code information in real time. It also has the function of scanning code recognition, supports connecting cash registers, electronic scales and other terminal devices by the serial port, and can independently access the payment background from the internet or wireless network to complete the acquiring business; supports remote downloads, remote online upgrades, etc. The system designs most modules on the hardware motherboard, including main control system modules, security chip modules, buttons, audio modules, WIFI modules, contactless modules, power modules, etc. The main control system consists of the main module, FLASH memory, clock, and power supply. The main control module is the core of the entire platform system, which completes the control, processing and storage of data signals. The main module provides external interfaces such as universal asynchronous receiver/transmitter (UART) port, universal serial bus (USB), serial peripheral interface (SPI), I2C, keyboard scan port, analog-to-digital converter (ADC), general input/output (IO), etc., and implements application functions by driving external functional modules. FLASH memory provides storage space for file system and user data. The system communication module uses ARM core processor, which is relatively mature and stable in hardware and software platform, with built-in scan code soft decoding and General packet radio service (GPRS) function. The security module selects a state secret chip

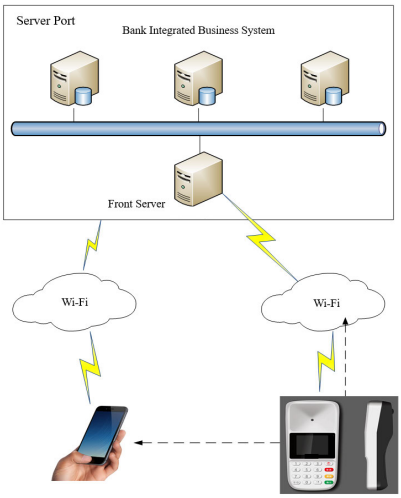


FIGURE 1. System topology diagram.

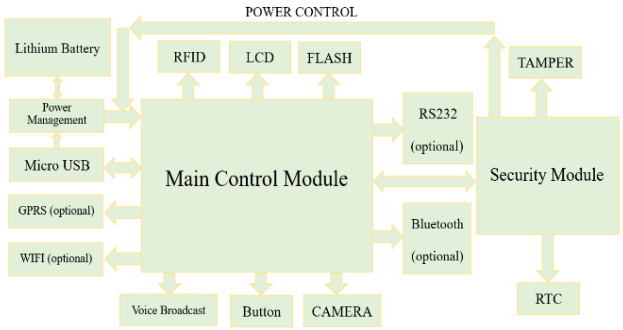


FIGURE 2. Hardware system architecture diagram.

with richer pin resources [7]–[9]. The system topology diagram and hardware system architecture diagram are shown in Figure 1 and Figure 2.

B. SOFTWARE DESIGN OF THE SYSTEM

1) SOFTWARE ARCHITECTURE

Software architecture of the system is shown in Figure 3; the main control module is an embedded real-time operating system, supporting priority preemption, no time slice, priority 0-255, priority range 100-255 can be created and modified by APP, USB communication protocol, TCP/IP protocol and serial communication protocol are supported. The main control module supports the local download and remote update of the application program, and has the function of system management and hardware testing program [10]–[12]. System structure from bottom to top is ISP and APP layer, API layer, SDK layer, application layer. The ISP is provided by the processor, the API is encapsulated by the driver layer, and the SDK is the middle layer encapsulation part between the driver and the application. The API interface is better for the application layer to use, the application layer implements the bank business functions based on the provided API interface and SDK interface.

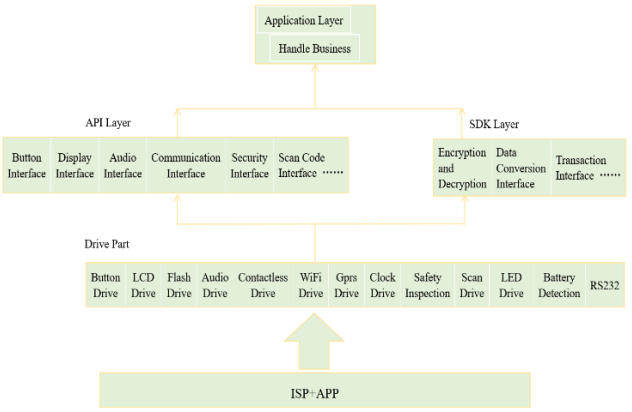


FIGURE 3. Software architecture of the system.

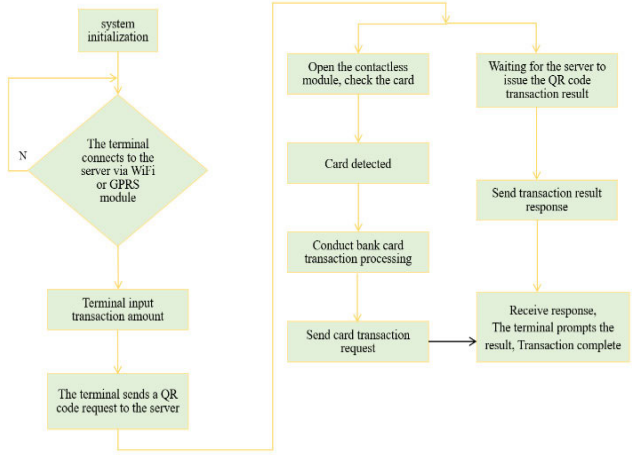


FIGURE 4. Application layer business design process.

2) APPLICATION

The application layer is the module layer that implements the specific requirements of the business in the actual project. The program code of the business layer is realized by calling the standard API of the unified API layer, the encapsulated library API of the common module layer and the standard C language. The business layer can be divided into multiple business modules according to actual business requirements, and the implementation of each business code is independent of each other, and modular development can be implemented. The business design process of the application layer is shown in Figure 4; the application program can view the parameters and set the parameters and download the key by the system administration interface.

C. QR CODE SCANNING AND SCANNED MODE OPERATION SCENES AND TRANSACTION STEPS

Depending on the applicable scene and the start way, QR codes can be divided into 'main scan mode' (main scanning mode of the payer) and 'scanned mode' (scanned mode of the payer). The scanning mode means that the payee displays the QR code and the payer scans the QR code; the

scanned mode means that the payer displays the QR code and the payee scans the QR code.

1) SCANNING MODE TRANSACTION STEPS

(1) The payee enters the amount in the registered store terminal and clicks on the collection service. The terminal system sends a transaction request message to the background based on the transaction information, and the back end generates a QR code serial number, and initiates transaction requests to the front platform by the ''collect payment'' port, the QR code serial number and other payment information are sent to the front end. At the same time, the client converts the QR code serial number into a QR code and displays it.

(2) The cardholder opens the payment bank's client APP to scan the terminal QR code and analyzes its content, completes the payment transaction according to the APP payment process, and synchronizes the APP to send the transaction information to the bank's background system.

(3) Because consumer transactions involve fund settlement, the front platform forwards the transaction result information of the UnionPay background to the terminal, and the terminal displays or gives voice prompts back to the merchant.

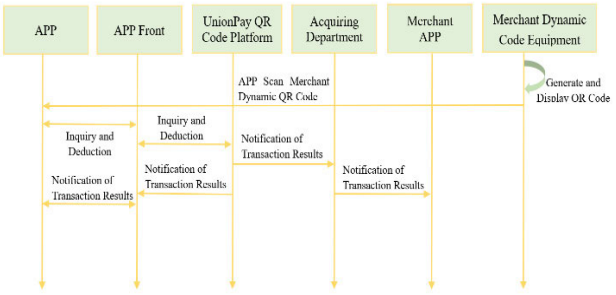


FIGURE 5. Scanning mode.

2) SCANNED MODE TRANSACTION STEPS

(1) The payer opens the payment bank client and clicks to pay. After the payment bank generates the QR code serial number, the client converts the serial number to QR code for display (if the barcode is formed synchronously, the barcode only reflects the QR code serial number itself).

(2) The payee uses the client end of the payee bank to scan the code, and the client prompts the payee to select the payment card and enter the payment amount to initiate the payment.

(3) Because consumer transactions involve fund settlement, the front platform forwards the transaction result information of the UnionPay background to the terminal, and the terminal displays or gives voice prompts back to the merchant.

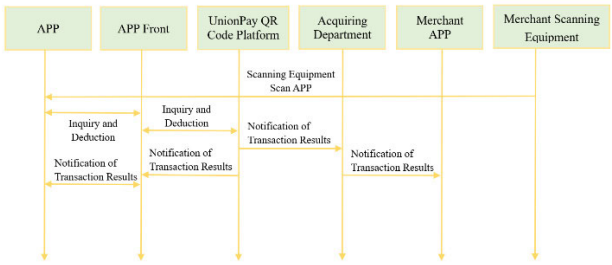


FIGURE 6. Scanned mode.

III. CRYPTOGRAPHIC ALGORITHMS AND PERFORMANCE TEST

The security of cryptographic algorithms is the core of information security, the security module of system integrates SM2, SM3, and SM4 cryptographic algorithms. SM2 algorithm is used for digital signature and verification, in the aspect of digital signature and key exchange, it is different from other algorithms, and adopts a more secure mechanism, which improves the amount of computation and complexity. It can provide higher security performance than RSA algorithm with less computing power, but the required key length is much lower than RSA algorithm. Its signature speed and key generation speed are faster than RSA. Compare with the RSA asymmetric encryption algorithm, SM2 algorithm has better performance of resisting attack, less CPU usage, less content use, low network consumption, fast encryption speed and so on [13]. In this system, the SM2 algorithm mainly provides signature and verification for identity authentication, completes data encryption and decryption, signature, and signature verification in the security module, and hardware encryption prevents attacks. The SM2 private key performs SM2 signature on the SM3 hash result. The private key cannot be read after being generated, and the RAM inside the chip can store sensitive data, which will be automatically destroyed after power failure. The SM2 public key performs SM2 verification on the SM3 hash and signature results. The public key is exported as a certificate to the receiver of the session key negotiation. The system uses SM3+SM2 signature calculation and verification to encrypt the firmware to ensure that the firmware is not tampered with and its integrity and authenticity are guaranteed. SM3 algorithm is used to generate data message digests and is an improved algorithm based on SHA-256. The Merkle-Damgard structure is adopted, the message packet length is 512 bits, and the digest length is 256 bits [14]. The compression function of SM3 algorithm has a similar structure to that of SHA-256, but the design of SM3 algorithm is more complicated. For example, each round of the compression function uses 2 message words, more secure than SHA-256 algorithm. The SM3 algorithm mainly completes the hash operation of transaction data and the pre-processing of SM2 signature in this system. When the password is used to verify the identity, SM3 is used to calculate the hash value and store it. After the user enters the password, the hash value is calculated, and

then compared with the stored hash value. If it is consistent, the verification is passed, otherwise the verification fails. The password used for authentication, its SM3 hash value is stored in the security data area of the state secret chip, and does not provide external output function. The correctness of the original password must be verified before changing the password to prevent unauthorized disclosure, modification and replacement of the password. SM4 block cipher algorithm is simpler to implement than AES algorithm and has higher security performance, it is used to encrypt and protect data in static storage and transmission channels. SM4 algorithm adds nonlinear transformations in the calculation process, which greatly improves the security of the algorithm [15]. In practical applications, it can resist all kinds of attacks against block cipher algorithm, including exhaustive search attack, differential attack, linear attack and so on. The hardware is easy to implement and the operation speed is fast. In this system, the SM4 algorithm mainly completes the encryption and decryption of the transaction data, and does the privacy protection; All external sensitive security parameters (SSP) input to the security module are encrypted by SM4 algorithm. Before executing all the sensitive operations provided by the state secret chip, a parallel task is synchronously started on the main CPU side and the SM4 encryption operation is executed cyclically. The initial key and initial data are generated randomly. The parallel task is stopped when the state secret chip completes the execution and returns. This protects against simple power analysis (SPA)/differential power analysis (DPA) attacks. While the program is running, the terminal state is constantly checked for attacks or abnormal states. When the terminal is attacked, it will lock and delete sensitive information in the key area.

A. KEY MANAGEMENT

The key management in the system adopts the layered mechanism, which is divided into three layers. The first layer is the local master key (LMK) which is used to encrypt and store the business master key; the second layer is the business master key; The third layer is the working key (one-time key, mainly used for data encryption and decryption) [16]. The key management module framework is shown in Figure 7.

The system key LMK is a set of key data automatically generated in the system. It has the function that the machine will automatically destroy after being taken apart. The security key is regenerated after the attack cleared in a secure environment, to encrypt the plaintext of the master key. The plaintext of the master key is encrypted with secure key to be stored after the master key issued.

The master key is issued by the customer (bank, etc.) to the secure storage area in the terminal through the key issuance system or the master program in a secure environment. It is stored in the form of ciphertext encrypted by the key. The master key is used to decrypt the work key.

The work key is a mandatory online check-in operation performed by the marketing system before the daily online business. When signing in, the work key will be issued by the

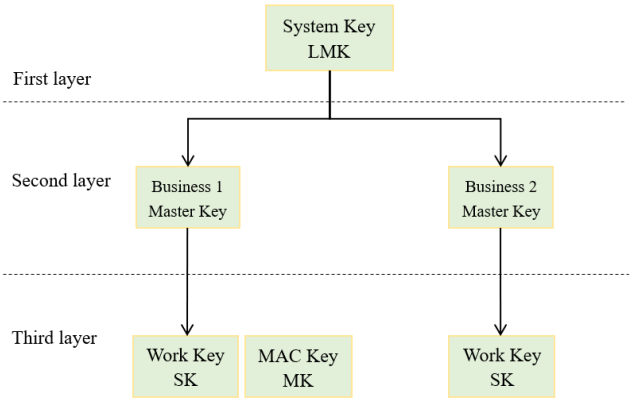


FIGURE 7. Key management module framework.

client background, and the work key will be stored in ciphertext form. The work key is divided into personal identification number (PIN) key, message authentication code (MAC) key, etc. The PIN key is used to encrypt the PIN, and the MAC key is used to calculate the MAC value of the transmitted data.

The MAC key is processed in the same way as the PIN working key. The terminal machine obtains it from the bank background when signing in to the bank. Since the sign-in transaction requires communication, the MAC key needs to be encrypted to be transmitted (the MAC key returned by the bank to the terminal when signing in is ciphertext). After receiving the message returned by the bank, the MAC key is decrypted by the terminal with the master key, and then stored in a dedicated key protection chip. This process is processed with the dedicated chip of the password keyboard. It also has the function that the machine will automatically destroy after being taken apart. and it is dedicated to calculating the MAC value (generating check data for data packets).

B. MAC VALUE CALCULATION PROCESS

In the algorithm test part, data analysis and verification are carried out in the secure channel, and the secure channel handshake protocol is established. After the processing center completes the authentication of the terminal, it decrypts to obtain the 48-byte shared master key. At this time, it is necessary to send a message to the terminal that the authentication has been completed by the processing center. In order to prevent this message from being forged, it is accomplished by calculating HMAC; that is, SM3 algorithm HMAC calculation process. The key is the first 16 bytes of the 48-byte shared master key, and the data is cipher text information. The processing center sends a handshake completion message to the terminal, that is, the HMAC value calculated by the processing center, and the terminal verifies the HMAC value after receiving it. Then, the HMAC ($P2 = 0 \times 00$) command is used to return the HMAC value generated by the completion of the terminal handshake to the processing center. The process of calculating the HMAC value by this command is the same as that generated by the processing center. After the processing center verifies the message that the terminal

handshake is completed, the session key is generated and the process of shaking hands is over. Finally, both the terminal and the processing center own a 48-byte shared master key and a 20-byte session key, with the first 16 bytes of the 20-byte session key serving as the encryption key and the last 16 bytes serving as the key to compute the MAC.

After a successful handshake, the two parties can transfer data over the established secure channel. The integrity of the application data exchanged by both parties is protected by the message authentication code MAC, the calculation method of MAC is described as follows: SM4 algorithm calculates MAC process. After receiving the data, the terminal or processing center first verifies the correctness of MAC, and then processes it if it is correct. Otherwise, send an error message and end the current link.

1) SM3 ALGORITHM

SM3 algorithm generates data message digest, verifies the message authentication code, and meets the security requirements of multi-password application. The algorithm is as follows [17]–[18]:

a: DEFINE VECTOR IV AND CONSTANT T_j AND INITIALIZE

$$IV = 7380166f\ 4914b2b9\ 172442d7\ da8a0600\ a96f30bc\ 163138aa\ e38dee4d\ b0fb0e4e$$

$$T_j = \begin{cases} 79cc4519 & 0 \le j \le 15 \\ 7a879d8a & 16 \le j \le 63 \end{cases} \quad (1)$$

Define Boolean function;

$$FF_j(X, Y, Z) = \begin{cases} X \oplus Y \oplus Z & 0 \le j \le 15 \\ (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z) & 16 \le j \le 63 \end{cases} \quad (2)$$

$$GG_j(X, Y, Z) = \begin{cases} X \oplus Y \oplus Z & 0 \le j \le 15 \\ (X \wedge Y) \vee (\neg X \wedge Z) & 16 \le j \le 63 \end{cases} \quad (3)$$

Define replacement function P_0, P_1;

$$P_0(X) = X \oplus (X <<< 9) \oplus (X <<< 17) \quad (4)$$

$$P_1(X) = X \oplus (X <<< 15) \oplus (X <<< 23) \quad (5)$$

b: ITERATIVE COMPRESSION PROCESS

The filled message is expanded group to generate 132 words $W_0 \sim W_{67}, W'_0 \sim W'_{63}$ for the compression function:

(1) Divide the message group into 16 words $W_0 \sim W_{15}$;

(2) For $16 \le j \le 67$

$$W_j \leftarrow P_1\left(W_{j-16} \oplus W_{j-9} \oplus \left(W_{j-3} \ll 15\right)\right) \oplus \left(W_{j-13} \ll 7\right) \oplus W_{j-6} \quad (6)$$

(3) For $0 \le j \le 63$

$$W_j' = W_j \oplus W_{j+4} \quad (7)$$

c: DEFINE THE COMPRESSION FUNCTION

Let A, B, C, D, E, F, G, and H be word registers, SS1, SS2, TT1, TT2 are intermediate variables, and the compression function calculation process is as follows:

$ABCDEFGH \leftarrow V^{(i)}$

For $0 \le j \le 63$

$$V^{(i+1)} \leftarrow ABCDEFGH \oplus V^{(i)}$$

$$ABCDEFGH \leftarrow V^{(n)}$$

The 256-bit hash numerical value ABCDEFGH is output.

2) SM3 ALGORITHM HMAC CALCULATION PROCESS

In this paper, after the completion of the authentication of the terminal, when sending the message that the authentication is completed by the processing center, in order to prevent the message from being forged, it is completed by calculating HMAC [19]. The MAC value of the input data text is calculated as follows:

MAC (text)t = HMAC (K, text) t = Hash (($K_0 \oplus$opad) || Hash (($K_0 \oplus$ipad) || text))

The detailed description process is shown in Figure 8:

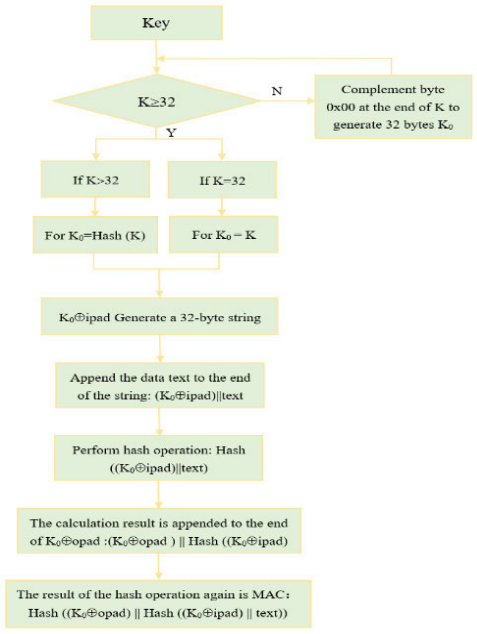


FIGURE 8. HMAC calculation description.

3) SM4 ENCRYPTION AND DECRYPTION ALGORITHM

In this paper, after the successful handshake between the processing center and the terminal on the secure channel, the integrity of the interactive application data between the two sides is protected by the message authentication code MAC, and the SM4 algorithm is used to calculate MAC. SM4 encryption algorithm and key expansion algorithm both adopt 32 rounds of nonlinear iteration structure, and the encryption operation is performed in units of words (32 bits). Each iteration operation is a round of transformation function

F. The encryption and decryption algorithms have the same structure, while the round key is opposite. The decryption round key is the reverse order of the encrypted round key.

Synthesize permutation T by nonlinear transformation and linear transformation, the overall encryption function of the round function is: $i = 0,1,\ldots,31$

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \end{aligned} \tag{8}$$

The linear transformation is as follows, where B is the character obtained by the nonlinear transformation

$$\begin{aligned} C = L(B) = B \oplus (B <<< 2) \oplus (B <<< 10) \\ \oplus (B <<< 18) \oplus (B <<< 24) \end{aligned} \tag{9}$$

Encryption key $MK = (MK_0, MK_1, MK_2, MK_3)$;
system parameters $FK = (FK_0, FK_1, FK_2, FK_3)$;
fixed parameter $CK = (CK_0, CK_1, \ldots..,CK_{31})$; rk_i is the round key, which is generated by the encryption key.

$$(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3) \tag{10}$$

$$\begin{aligned} rk_i &= K_{i+4} \\ &= K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i) \\ & i = 0, 1, \ldots, 31 : \end{aligned} \tag{11}$$

The linear transformation is changed to:

$$L'(B) = B \oplus (B <<< 13) \oplus (B <<< 23) \tag{12}$$

Find the round key.

When encrypting the last round of transformation, the output is

$$\begin{aligned} (Y_0, Y_1, Y_2, Y_3) &= R(X_{32}, X_{33}, X_{34}, X_{35}) \\ &= (X_{35}, X_{34}, X_{33}, X_{32}) \end{aligned} \tag{13}$$

The final output is the reverse order of encryption, and only the reverse order of the round key is used for decryption.

4) SM4 ALGORITHM CALCULATES MAC

MAC algorithm based on SM4 refers to ISO/IEC 9797-1(Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher) specification, uses the symmetric encryption algorithm with the key length of 128 bits, and uses CBC mode to calculate the 16-byte MAC value for any length of the message [20].

Fill grouping:

Add 0×80 after the plaintext M, and then fill the minimum 0×00 at the right end, so that the length of the filled message $M = (M||80||00||00||\ldots||00)$ is an integer multiple of 16. Divide M into 16-byte blocks $M_1, M_2, \ldots, M_n$.

MAC calculation process:

Use SM4 algorithm, adopt CBC mode and use key K to encrypt packets $M_1, M_2, \ldots,$ Mn. Where the initial vector IV = (00||00||00||00||00||00||00||00||00||00||00||00||00||00||00||00).

FIGURE 9. Terminal decryption result.

FIGURE 10. Signature verification successful.

The CBC mode encryption process is as follows:

$$\begin{aligned} C_0 &= IV \\ C_i &= EKL(M_i \oplus C_{i-1}), \quad i = 1, 2, \ldots, n \end{aligned}$$

The left 8 bytes of the last piece of data calculation result is the message digest code MAC:

$$MAC = LEFT8(C_n) \tag{14}$$

C. CRYPTOGRAPHIC ALGORITHM CORRECTNESS TEST

Algorithm correctness test includes SM2 algorithm key pair generation, encryption, decryption, signature, and verification test; collect 5 sets of data. SM3 hash algorithm and SM4 symmetric grouping algorithm also generate 5 sets of data tests [21]−[22].

1) SM2 ALGORITHM CORRECTNESS TEST

a: MODE OF SM2 KEY PAIR GENERATED BY TERMINAL

SM2 key pair is generated by terminal, encrypted by the PC, and then decrypted and verified the correctness by terminal. When the communication is normal, click "Terminal generates SM2 key pair", the public key will be displayed in output, enter irregular data (maximum 32 bytes) in Input, and click "SM2 public key encryption" to generate PC end public key encryption data; click "SM2 private key decryption" to decrypt the terminal private key. The red mark in Figure 9 indicates that the decryption result is consistent with the terminal encrypted data. Enter random 32 bytes of data in Input to generate signature data and verify the correctness of the signature [23]–[24]. Figure 10 shows the verification is successful.

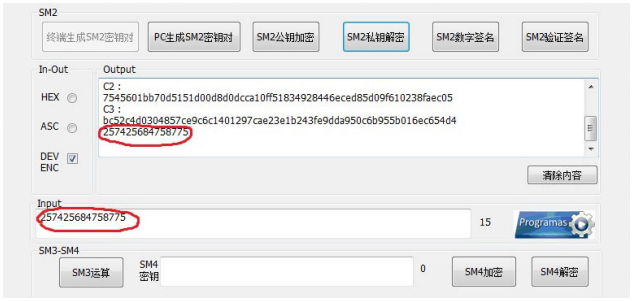


FIGURE 11. PC decryption result.

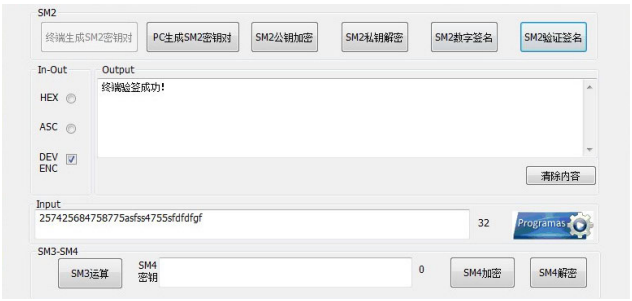


FIGURE 12. Terminal verification successful.

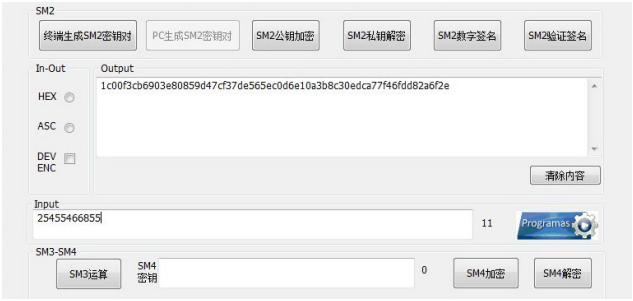


FIGURE 13. Hash operation result.

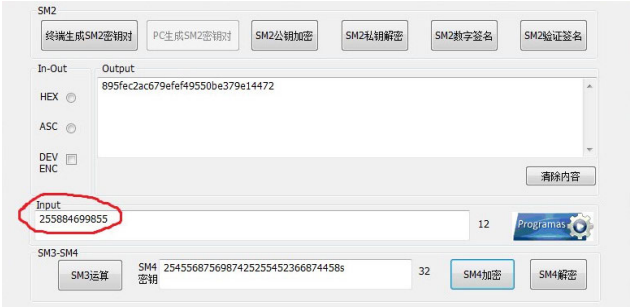


FIGURE 14. SM4 encrypted result.

b: MODE OF SM2 KEY PAIR GENERATED BY PC PORT

SM2 key pair is generated by PC port, encrypted by terminal, and then decrypted and verified the correctness by PC. In the case of normal communication, the PC generates the SM2 key pair and displays the public key in 'Output'. enter an irregular data (maximum 32 bytes) in 'Input', click ''SM2 public key encryption'' to generate encrypted data, click ''SM2 private key decryption'' to decrypt the private key for the PC port. The red mark in Figure 11 is the

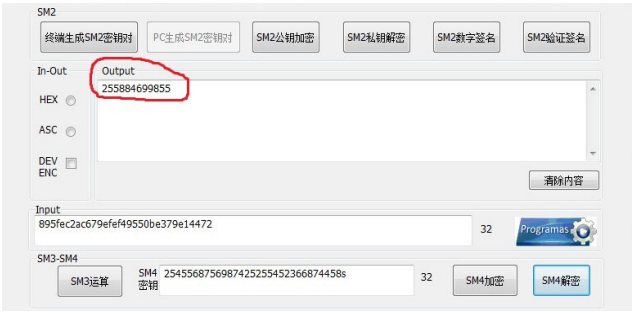


FIGURE 15. SM4 decrypted result.

decryption result. Enter random 32 bytes of data in 'Input' to generate signature data, and click ''SM2 Verification Signature'' to verify the correctness of the signature by the terminal, the terminal verification is successful as shown in Figure 12.

2) SM3 ALGORITHM CORRECTNESS TEST

Enter irregular data (maximum 1024 bytes) in 'Input', click ''SM3 operation'' to verify the operation, the hash operation result is shown in Figure 13.

3) SM4 ALGORITHM CORRECTNESS TEST

Enter irregular data (maximum 16 bytes) in 'Input', enter 32 irregular data in the SM4 key, and click ''SM4 encryption'' to perform SM4 encryption. The encryption result is shown in Figure 14. Copy the ciphertext encrypted in 'Output' in Figure 14 to 'Input' in Figure 15 and click ''SM4 decryption''. The decrypted result is consistent with the original text in Figure 14.

D. CRYPTOGRAPHIC ALGORITHM PERFORMANCE TEST

The performance test of cryptographic algorithm is divided into the overall test of the external interface. The PC software or terminal transmits data to the test terminal by serial port, LAN port, GPRS and other data ports. The test terminal encrypts and decrypts the data and returns the data. The time of this process is used as the overall performance index of the test terminal (except random numbers). In order to ensure that the quality of random numbers is not excessively affected by physical noise sources, the M sequence scrambling mechanism is used to reprocess the true random sequences in the security module. The M sequence is the most commonly used pseudo-random sequence. A shift register sequence with a period of 2^n is generated by an n-bit nonlinear feedback shift register. The M sequence is used to disrupt the input transmission code stream, the random number stream ''0'' and ''1'' after being disturbed have the same probability, although the original transmission code stream is changed, the disturbance is regular, so the original transmission data can be obtained after descrambling at the receiving end. M sequence has better characteristics of autocorrelation, equalization, run-length, shift and addition, which ensure the security of the random number transmission process. Even if the physical

FIGURE 16. Actual application effect.

noise source is affected, the random number results after the scrambling can still be maintained higher quality. In addition, the security module has high and low voltage, high and low frequency detection. When the input signal is out of range, the chip will stop working, avoiding the impact on physical noise source.

1) SM2 ALGORITHM PERFORMANCE TEST

Collect 1000 sets of 128K data to verify randomness. It is tested that the average execution time for generating 1000 sets of key pairs is 140 seconds, and the average operation rate is 7.143 pairs/sec. We used RSA-2048 algorithm to perform the same test on the interface key pair generation and private key operation. The RSA-2048 algorithm key pair generated 0.036 pairs/sec. The average private key operation rate is 0.133 times/sec, Comparing the SM2 calculation speed 7.143 pairs/sec and 1.352 times/sec, 1.489 times/sec, the calculation speed of SM2 algorithm is much higher than that of RSA-2048 algorithm. SM2 algorithm completes the functions of data encryption, decryption, signature and signature verification within the security chip. The private key is encrypted and stored in the secure area of the terminal, and can never be read out, and the public key can be output. In the two-way authentication process, a series of random numbers are generated to be used as transmission keys and encryption keys to ensure that the keys are transmitted in ciphertext during the transmission process. After the two-way authentication is passed, the key pair is deleted according to the specified index number, and the key pair is destroyed and cannot be restored. SM2 algorithm test results of system are shown in Tables 1, 2;

TABLE 1. SM2 algorithm encryption/decryption operation test results.

Encryption/ Decryption Data (KB)	Operation Time (Seconds)			Average Execution Time (Seconds)	Computing Average Rate (Kbps)
	First Time	Second Time	Third Time		
128	784.827	785.169	784.858	784.951	0.163 (Encryption)
128	781.472	783.852	781.532	782.285	0.164 (Decryption)

TABLE 2. SM2 algorithm signature/verification operation test results.

Number of signatures/verifications	Operation Time (Seconds)			Average Execution Time (Seconds)	Computing Average Rate (Times/sec)
	First Time	Second Time	Third Time		
320	228.277	228.227	228.467	228.324	1.489 (signature)
320	251.933	251.583	250.994	251.503	1.352 (verification)

TABLE 3. SM3 hash operation test results.

Operation Data (KB)	Operation Time (Seconds)			Average Execution Time (Seconds)	Computing Average Rate (Kbps)
	First Time	Second Time	Third Time		
128	163.991	163.933	163.934	163.953	0.781

2) SM3 ALGORITHM PERFORMANCE TEST

The SM3 algorithm is used to generate data message digest and is an improved algorithm based on SHA-256. The output does not depend on the input in a discernible way; a single bit change in any input string will cause about half of the bits in the output bit string to change. Based on the RSA-2048 algorithm, we conducted RSA+SHA algorithm test on the payment system. The test result is that SM2+SM3 operation rate is much higher than RSA +SHA algorithm. The SM3 algorithm test result is shown in Table 3;

3) SM4 ALGORITHM PERFORMANCE TEST

Reference [25] in the research on security of mobile payment, the efficiency of the hybrid algorithm is tested. The ECC+AES+RC4 algorithm requires 1.921s to encrypt 1Kb data. Compared with the execution time 0.267S of our system, the encryption time is shorter and the rate is higher. Similarly, the encryption rate of SM4 algorithm in system is much higher than that of 3DES algorithm, as described in [26]. The SM4 algorithm performance test is shown in Table 4;

The above three algorithms have passed the commercial password correctness and algorithm performance test, and passed the random number quality test and primality test, verifying the security and stability of the algorithm in the system.

TABLE 4. ECB mode encryption/decryption operation test results.

Encryption/ Decryption Data (KB)	Operation Time (Seconds)			Average Execution Time (Seconds)	Computing Average Rate (Kbps)
	First Time	Second Time	Third Time		
128	0.266	0.268	0.267	0.267	479 (Encryption)
128	0.270	0.268	0.269	0.269	476 (Decryption)

IV. TECHNOLOGICAL INNOVATION

The innovation point of the system is the adoption of a more secure state secret algorithm in the selection of encryption algorithm, which makes the system more secure in the instant message transmission, it can resist all kinds of attacks. secondly, the M sequence scrambling mechanism is used to reprocess the true random sequence in the security module. After reprocessing, even if the physical noise source is affected, the random number after scrambling can still maintain a high quality. It overcomes the shortcomings of various data encryption systems using general algorithms and software pseudo-random numbers in the past. Finally, the system key has the function that the machine will automatically destroy after being taken apart, and the security key is regenerated after the attack state cleared in a safe environment, and the plaintext of the master key is encrypted to make data transmission more secure. Password storage security implements multiple key containers and multiple keys for each key container. There is a dedicated circuit outside the cryptographic module for physical protection, which improves the security of algorithm operation.

V. CLIENT APPLICATION EFFECTS

As shown in Figure 16, the payment effect under the two modes of the payee displaying QR code, the payer scanning QR code and the payer displaying QR code and the payee scanning QR code was verified respectively.

VI. CONCLUSION

Compared with the traditional single encryption algorithm, the data encryption algorithm of the QR code payment system based on the state secret algorithm has higher security performance; It achieves the higher strength and better performance password operation, which ensures the payment process more secure and reliable. The test result shows that the system has achieved the expected effect in payment requirements, and it has a higher calculation speed than other algorithms. The dynamic QR code is only used for one-time payment, which solves the insecure technical problems such as the long time stay of the QR code; it is convenient to consume while ensuring the safety of the transaction environment. Payment can be made by two modes of QR code scanning and scanned, which is suitable for payment in more scene transaction. The system has been tried out in companies, meeting users' information security needs, and has good application prospects. The research in this paper will also provide a useful reference for the QR code payment security field.

REFERENCES

[1] *Security Specifications for UnionPay Payment Using Two-Dimensional Code*, document QCUP 067-2016, China UnionPay Co., Ltd., 2016.

[2] P. F. Cao, J. Li, and J. Yang, "Design and implementation of mobile cloud security payment system," *Comput. Appl. Softw.*, vol. 36, no. 4, pp. 296–301, Apr. 2019.

[3] S. Wan, G. Yang, L. Qi, L. Li, X. Yan, and Y. Lu, "Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code," *Math. Biosci. Eng.*, vol. 16, no. 6, pp. 6367–6385, 2019.

[4] M. F. Zhang, "Research on security technology and authentication scheme of NFC mobile payment," Harbin Inst. Technol., Harbin, China, Tech. Rep., Jun. 2019, pp. 21–24.

[5] *Interface Specifications of Cryptography Device Application*, document GM/T 0018-2012, National Cryptography Administration, 2012.

[6] J. Yao, "Domestic commercial cryptographic algorithm and its performance analysis," *Comput. Appl. Softw.*, vol. 36, no. 6, pp. 328–332, Jul. 2019.

[7] P. F. Cao, J. Li, and J. Yang, "Design and implementation of mobile cloud security payment system," *Comput. Appl. Softw.*, vol. 36, no. 4, pp. 296–300, Apr. 2019.

[8] Y. Q. Liu and X. Y. Li, "Mobile secure payment scheme using identity-based cryptographic algorithm + SMS verification code," *Comput. Sci.*, vol. 47, no. 1, pp. 294–300, Jan. 2020.

[9] J. T. Liu, K. Liang, J. Wang, X. W. Chen, H. C. Xu, and G. F. Li, "Cuttable structure design and hardware implementation of SM4 encryption algorithm," *Acta Scientiarum Naturalium Universitatis Nankaiensis*, vol. 52, no. 4, pp. 41–45, Aug. 2019.

[10] Y. Xu, Z. Ma, Z. Wang, X. Niu, and Y. Yang, "Survey of security for Android smart terminal," *J. Commun.*, vol. 37, no. 6, pp. 169–184, Jun. 2016.

[11] Y. Xi, Y. Huang, J. Su, and S. Wang, "Design and implementation of instant messaging encryption software system based on national secret algorithm," *Comput. Appl. Softw.*, vol. 37, no. 6, pp. 303–308, Jul. 2020.

[12] R. Huang, Q. Zhang, G. Li, and S. Huang, "Privacy information collection process encryption system based on national secret algorithm," *Autom. Instrum.*, vol. 9, no. 25, pp. 213–215, Sep. 2020.

[13] *Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves*, document GM/T 0003-2012, National Cryptography Administration, 2012.

[14] *SM3 Cryptographic Hash Algorithm*, document GM/T 0004-2012, National Cryptography Administration, 2012.

[15] *SM4 Block Cipher Algorithm*, document GM/T 0002-2012, National Cryptography Administration, 2012.

[16] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[17] *Information Security Technology-SM3 Cryptographic Hash Algorithm*, document GB/T 32905-2016, China Standards Press, Beijing, China, 2016.

[18] J. Zhao, X. W. Zeng, and Z. C. Guo, "Design and implementation of high speed PCIe cipher card supporting GM algorithms," *J. Electron. Inf. Technol.*, vol. 41, no. 10, pp. 2403–2407, Oct. 2019.

[19] *Information Technology—Security Techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms Using a Block Cipher*, Standard ISO/IEC 9797-1-2011, 2011.

[20] *Information Security Technology-SM4 Block Cipher Algorithm*, document GB/T 32907-2016, China Standards Press, Beijing, China, 2016.

[21] *Compulsory Product Certification Implementation Rules for Information Technology Equipment*, document CNCA-C09-01:2014, China National Certification and Accreditation Administration Commission, 2014.

[22] *Compulsory Product Certification Implementation Rules for Telecommunications Terminal Equipment*, document CNCA-C16-01:2014, China National Certification and Accreditation Administration Commission, 2014.

[23] *Information Security Technology-Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves*, document GB/T 32918.1-2016, China Standards Press, Beijing, China, 2017.

[24] X. P. Xu, "Design of device secure authentication system base on SM2," *Electron. Eng. Product World*, vol. 28, no. 3, pp. 36–37, Mar. 2021.

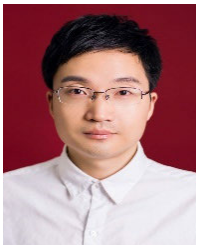
[25] X. M. Gao, "Research on security of mobile payment," Chang'an Univ., Xi'an, China, Tech. Rep., May 2017, pp. 59–60.

[26] D. D. Wang, "Design and implementation of secure encrypted instant messaging system," Shenyang Inst. Comput. Technol. Chin. Acad. Sci., Tech. Rep., Jun. 2020, pp. 64–66.

YUKUN ZHOU received the master's degree in measuring and testing technologies and instruments from Chongqing Institute of Technology. She has been working with the Applied Engineering College, Zhejiang Business College, since 2008. Her main research interests include technology of intelligent sensor, the Internet of Things application technology, embedded software and hardware development, and payment security related fields.

BAIDONG HU received the master's degree in measuring and testing technologies and instruments from Chongqing University of Technology. He has been working with the Terminal Research and Development Department, Hangzhou Sunyard Technology Company Ltd., as a Research and Development Manager, since 2009. He is currently a Senior Engineer, mainly engaged in research on embedded hardware and payment security related fields.

YITAO ZHANG received the bachelor's degree in automation from Hefei University of Technology, in 2019. He is currently pursuing the master's degree in engineering from Zhejiang University. He is also a postgraduate student at the College of Control Science and Engineering, Zhejiang University, majoring in control engineering. His research interest includes intelligent detection technology.



WEIMING CAI received the Ph.D. degree from Zhejiang University. From 2012 to 2013, he was studied with Oklahoma State University. He is currently an Associate Professor in electrical and electronic engineering and the Head of the Institute of Information and Electronic Technology, NingboTech University.