Journal of Computers Vol. 33 No. 1, February 2022, pp. 189-198
doi: 10.53106/199115992022023301017

Based on SM - 9 Cloud Edge System Information Security Transmission

Cai-Sen Chen[1], Yang-Xia Xiang[2*], Jia-Xing Du[2],
Song Chen[2], Cong Lin[3]

[1] Military Exercise and Training Center, Army Academy of Armored Forces, Beijing, 100072, China
caisenchen@163.com
[2] Information and Communication Department, Army Academy of Armored Forces, Beijing, 100072, China
elephant_187@163.com, dhtl2004@163.com
[3] Logistic Support Center, Army Academy of Armored Forces, Beijing, 100072, China
479994143@qq.com

Received 1 December 2021; Revised 2 January 2022; Accepted 2 February 2022

Abstract. In the past few years, cloud edge system from conception to gradually improve, develop to today has become a mature side of cloud model. Compared with simple cloud computing, cloud edge system has lower network latency and is suitable for application scenarios with higher real-time requirements. Although it can make up for some shortcomings of cloud computing, it also faces many problems in practical application, how to realize the safe transmission of information in the open network environment is one of the difficulties. Since the data transmission process between the edge and the cloud exists in the form of plaintext transmission, this allows attackers to easily disrupt normal data interactions. It is an important research point to ensure the stable operation of the cloud edge system while maximizing the security of communication. To this end, the following work has been done in the direction of secure data transmission in this paper:

1. Analyzed the potential risks of the cloud edge system communication network from the perspective of data source security and data transmission security.

2. Summarizes the requirements and limitations of secure communication, introduces a lightweight SM9 encryption algorithm with low implementation cost and low resource consumption. And compared with other encryption algorithms.

3. Provide algorithmic foundation for establish a framework for secure transmission of lightweight data and achieve data confidentiality protection

Provides a viable reference for secure data transmission in the cloud edge system

Keywords: SM9, encryption algorithm, cloud edge system, information security transmission

1 Introduction

1.1 Background and Significance of the Study

With the continuous development of the cloud computing industry, more and more cloud applications are used in practice, and more and more companies are constantly inclined to the research and development and use of cloud computing products. As more and more data are stored in the cloud, the security problem of cloud data transmission is gradually exposed. According to the report, in 2018, the user data of a number of large enterprises was leaked, so the data security issue must be taken seriously. When user-generated data or large data are transmitted in the cloud edge system, how to guarantee the security of the data has become our focus, and encryption technology to encrypt the data is the most appropriate method to meet the security of data transmission.

In the middle of the 20th century, message encryption processing technology has become increasingly complex and systematic, and has gradually become a key technology for data security at the social, commercial and even national levels. Symmetric encryption is the fastest and simplest form of encryption, and the same key is used for encryption and decryption. There are many kinds of symmetric encryption algorithms, and because of its high efficiency, it is widely used in the core of many encryption protocols. But since both parties use the same key, security is not guaranteed. The disadvantage of symmetric encryption is that before the data can be transmitted, the sender and receiver must agree on the secret key, and then both parties can keep the secret key. Asymmetrically encrypted into data encryption and decryption provides a very secure method that uses a pair of keys: a public

* Corresponding Author

key and a private key. The private key can only be kept safe by a party, can't leaked out, while the public key can be sent to anyone who requests it. Asymmetric encryption uses one of these keys to encrypt, while decryption requires the other key. Unlike symmetric encryption, there is no need to send the private key across the network, so security is greatly improved. At present, the most widely used in the field of cryptography RSA cryptography algorithm and elliptic curve cryptography algorithms are public key cryptography algorithms. RSA cipher algorithm is characterized by its simple principle and easy implementation. RSA can only maintain its security by extending the key bit width. However, the increase of key bit width not only makes the hardware implementation more difficult, but also reduces the efficiency of encryption and decryption, so RSA has some limitations in security. The security of elliptic curve cryptography (Elliptic Curve Discrete Logarithm Problem，ECDLP) mainly comes from the difficulty of elliptic curve discrete logarithm problem. Compared with RSA, ECC encryption performance is higher and the required key length is shorter, currently ECC has the highest security strength of a single bit key. Identification cipher algorithm (IBC) is an encrypted scheme in which the user's unique identity (or identity is simply calculated) is used as the public key, the private key is calculated from the user ID and system parameters. In the identity cryptography system, the public key derived from the identity can effectively avoid the complicated certificate exchange process in the traditional public key cryptography system, and improve the throughput of wireless network. The SM9 identity cryptography algorithm is the first identity-based cryptography algorithm standard released by the State Secret Administration of China in 2016. The standard stipulates the specific implementation algorithms of digital signature, secret key exchange, and public key encryption and decryption. SM9 identity password algorithm has both the advantages of ECC and IBC, its biggest advantage is easy to carry on key management, the system users don't need to apply for digital certificate, don't need online query and verification certificate, greatly simplifies the link of secure communication, especially suitable for the realization of mass user environment identity authentication and data encryption. This paper first introduces the principle of several main encryption calculation and its.

1.2 Cloud Edge System Security Issues

In order to more targeted deployment of the cloud edge system security protection system, design and implementation of effective security protection measures, it is important to first understand the current security risks and the threats and challenges faced in the cloud edge system. There are several shortcomings in the current cloud edge system:

(1) System data security: No security level identification and classification of system data.

(2) System architecture: lack of effective control network layering.

(3) Communication networks: lack of control of data flow, backup of configuration information and key management; lack of protection and access control of hardware devices; lack of delineation of system security boundaries.

1.3 Attacks Against Communication Networks

(1) Denial of service attack: The attacker finds a way to make the target machine stop providing services, and is one of the common attacks used by hackers. It forces the server's buffer to be full and not to receive new requests; secondly, it uses IP spoofing to force the server to reset the connection of illegal users and affect the connection of legitimate users.

(2) Integrity attacks, which are operations that tamper with data.

(3) Data injection attack: After fully grasping the principle of the communication protocol, the attacker misleads the operator or controls the operation of the component by sending wrong control status or information.

(4) Replay attack: A replay attack is when an attacker intercepts data transmitted over the network, records data information over a period of time, and then replays these packets.

2 Related Work

Scholars have designed a series of lightweight cryptographic algorithms based on the basics of number theory, algebra, classical hard problems with low computational resources and moderate real-time and security. Or the original cryptographic algorithm can be lightened by reducing the key length and the number of rounds, and then applied to the cloud edge system. Msahoney [1] et al. proposed a block encryption algorithm based on Quasigroup. First, a random 256bit key is generated by constructing a proposed group of size 256*256 and dividing it evenly into individual byte blocks as the round key for each round. Then the original plaintext data is divided into 128 bit blocks, and processed. Premnath [2] uses NTRU to implement authentication and data integrity protection within the system and compares NTRU execution time with ECC and RSA on the ARMV6 platform [4]. The results show that the execution speed is 2 to 2.5 times faster than the latter. The above authors secure the control system by introducing lightweight cryptographic algorithms. However, the impact of algorithms on performance is mainly considered from the perspective of device power consumption and hardware implementation cost, and the analysis of algorithm running time and its impact on control system performance is lacking. In this paper, we analyze the SM9 encryption algorithm in terms of its running time and its security, compare it with its encryption algorithm, and finally show the feasibility of the SM9 lightweight encryption algorithm.

3 Lightweight secure transport Algorithm

3.1 Algorithm Overview

3.1.1 SM4 symmetric encryption algorithm:

SM4 is a symmetric cryptography algorithm, which is the standard of block encryption algorithm published by China in 2012. The message block length and key length of SM4 block encryption algorithm are both 128 bits. The main operation process can be divided into the following steps:

In the process of encryption and decryption, both the unencrypted and encrypted messages are treated as the same number of bit words by the SM4 algorithm, in this case, as four 32-bit words, the four bytes of (X_0,X_1,X_2,X_3) represent the input plaintext data. After 32 rounds of key operation, the encrypted information can be obtained, that is, the encrypted ciphertext can be output: (Y_1,Y_2,Y_3,Y_4) means the output ciphertext. The encryption process is as follows:

$$X_{i+4}=\mathrm{F}(X_i,X_{i+1}, X_{i+2}, X_{i+3},rk_i)=X_i \oplus \mathrm{T}(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i). \quad \textbf{(1)}$$

$$(Y_0,Y_1, Y_2, Y_3)= (X_{35}, X_{34}, X_{33}, X_{32}). \quad \textbf{(2)}$$

The SM4 algorithm encryption and decryption keys are the same. The difference is that the encryption and decryption round keys are used in the reverse order. When encrypting, its round keys are used in the order (rk0, rk1, rk2, …, rk31), in the process of decryption, its round key is used in the order (*rk31,rk30,rk29…rk0*). SM4 encrypted symmetric encryption algorithm in detail in Fig. 1 work-flow:

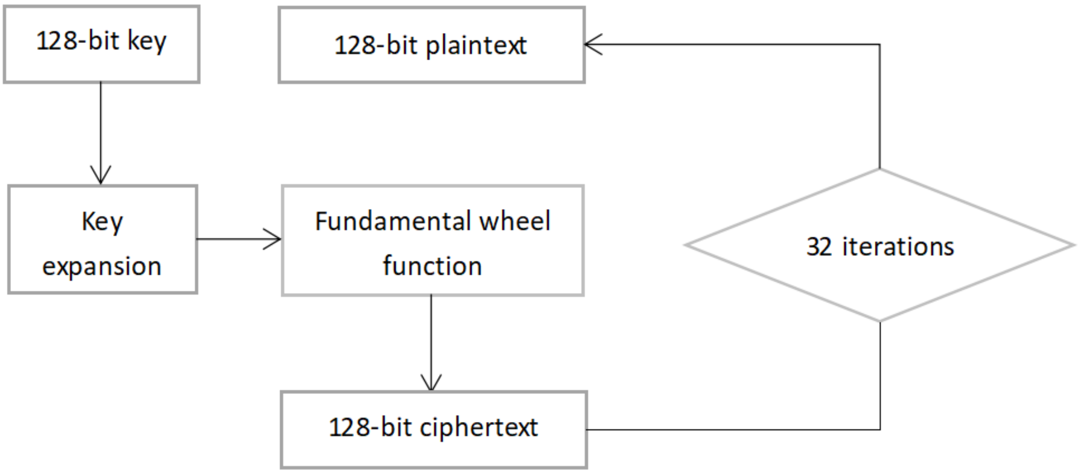

Fig. 1. SM4 algorithm encryption process

3.1.2 SM9 asymmetric encryption algorithm:

(1) Digital signature and verification algorithm:

Most of the time, people often need to perform identity authentication, integrity verification and anti-repudiation of the received information [3]. Identity verification helps us confirm the source of the message. Data integrity verification ensures that the message has not been tampered with. Anti-denial can prevent the publisher of the message from denying the message. Digital signature, also known as public key digital signature, is realized through public key cryptography, which has high security. Digital signature generally includes two relative processes, namely digital signature and signature verification, in order to realize the functions of identity authentication in digital space, document integrity verification and anti-repudiation.

In the process of digital signature, the sender uses the private key to sign the information, and the receiver uses the corresponding public key to verify the signature [5]. For the traditional public key cryptosystem, the signer first calculates its corresponding public key through its own private key, and then applies for a certificate from CA, which contains the user's identity information, public key and signature of CA, and then sends the certificate to the verifier through the open channel. The verifier determines the source of the public key by verifying the CA's signature, and then uses the public key to verify the signature. Under the traditional cryptography system, the acquisition of public key involves the exchange of certificates, which increases the redundancy of data transmission. In the wireless network, this will certainly affect the network performance and reduce the throughput. Different from the traditional public key cryptosystem, SM9 identity cryptosystem calculates the public key through the user identity, which avoids the complicated certificate exchange process and greatly improves the efficiency of information transmission. It adopts bilinear mapping to implement the identification integration, which makes the signature algorithm more efficient and secure. Fig. 2 shows how the SM9 digital signature system works.

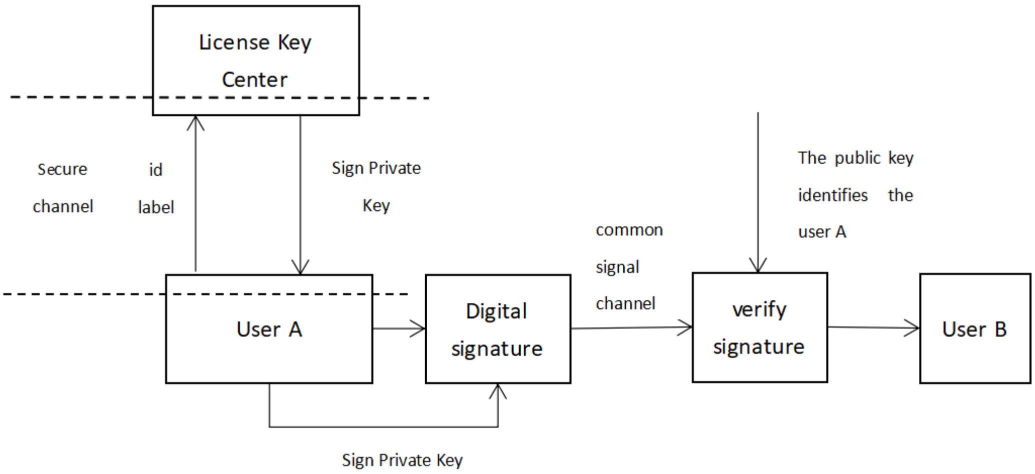

Fig. 2. Digital signature algorithm flow

(2) Public key encryption and decryption algorithm

Data encryption and decryption is also an important part of the cryptosystem, which is an important guarantee for the safe transmission of information on the public channel [6]. In the ID based encryption and decryption algorithm, the public key needed for encryption can also be calculated according to the user ID. Fig. 3 shows the working principle of SM9 public key encryption and decryption system.

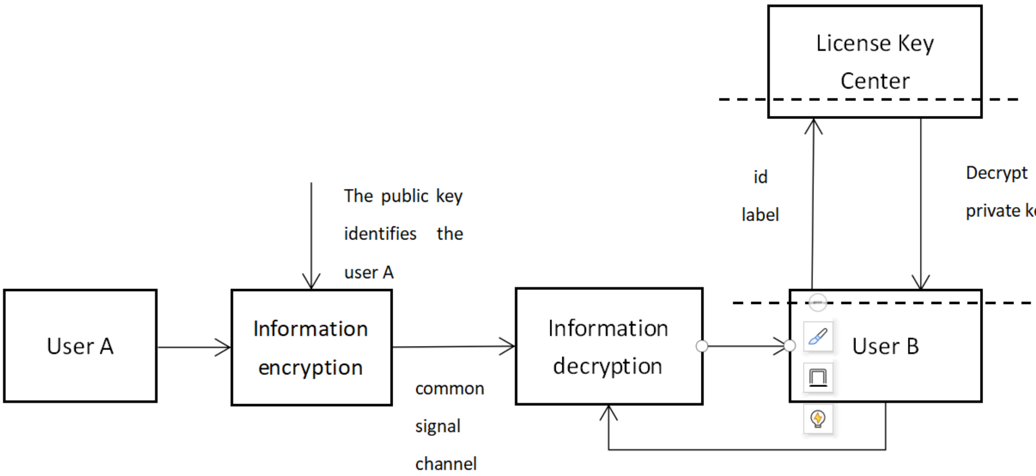

Fig. 3. Principle of SM9 public key encryption and decryption system

User A needs to send encrypted information to User B. Firstly, User A encrypts the information by using the calculated identity of User B as the public key, and then sends the ciphertext information to User B through the open channel. After receiving the ciphertext information, User B decrypts it by using the decryption private key. The private key of User B is distributed by the key generation center. When the system is initialized, the key generation center authenticates the identity of User B, then calculates the decryption private key with its identity and system parameters, and sends it to User B through the secure channel for storage. Encryption and Decryption Algorithm of Elliptic Curve Cryptography This encryption method will be less secure, but the speed will be greatly improved. In the SM9 identification password algorithm, the data encryption algorithm adopts the hybrid encryption method [7]. In other words, the key used for data encryption is encoded on a point of the elliptic curve, and then the symmetric encryption key is calculated by the key derived function KDF, and then the key is used to encrypt the data. Fig. 4 shows the SM9 public key encryption algorithm flow.

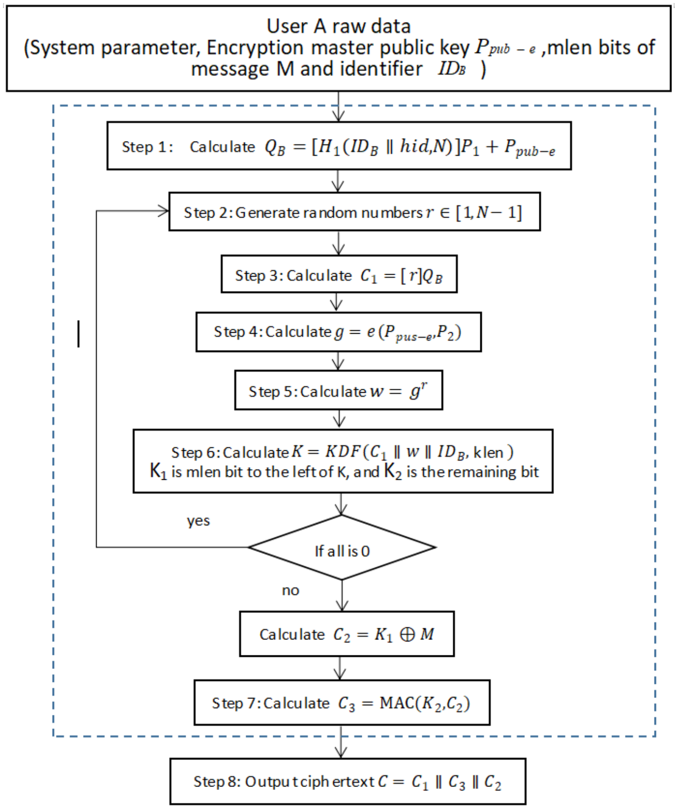
User A raw data
(System parameter, Encryption master public key P_{pub-e} ,mlen bits of message M and identifier ID_B)
Step 1: Calculate $Q_B = [H_1(ID_B \parallel hid, N)]P_1 + P_{pub-e}$
Step 2: Generate random numbers $r \in [1, N-1]$
Step 3: Calculate $C_1 = [r]Q_B$
Step 4: Calculate $g = e(P_{pus-e}, P_2)$
Step 5: Calculate $w = g^r$
Step 6: Calculate $K = KDF(C_1 \parallel w \parallel ID_B$, klen)
K_1 is mlen bit to the left of K, and K_2 is the remaining bit
yes
If all is 0
no
Calculate $C_2 = K_1 \oplus M$
Step 7: Calculate $C_3 = \mathrm{MAC}(K_2, C_2)$
Step 8: Output ciphertext $C = C_1 \parallel C_3 \parallel C_2$

Fig. 4. Encryption algorithm flow chart

Bit string M is the plaintext message to be encrypted, mlen is the bit length of the plaintext message, K_2_len is the bit length of key K_2 in function MAC (K_2, Z). The public key used for encryption is calculated through User B's identity, and User A can use this public key to encrypt plaintext M. The specific encryption steps are as follows:

(1) Calculate element $Q_B = [H_1(ID_B \parallel hid, N)]P_1 + P_{pub-e}$of group G1. **(3)**

(2) Generates a random number $r \in [1, N-1]$. **(4)**

(3) Calculate the element $C_1 = [r]Q_B$ in group G1 and convert the data type of G1 to a bit string. **(5)**

(4) Calculate the element $g = e(P_{pus-e}, P_2)$ of group G_T. **(6)**

(5) Calculate the element $w = g^r$ of group G_T. **(7)**
convert the data type of w to a bit string.

(6) Calculate klen $= mlen + K_2$_len. **(8)**
then calculate $K = KDF(C_1 \parallel w \parallel ID_B, klen)$, let K_1 be the leftmost mlen bit of k, if K_1 is a string of zero bits, then return A_2;

(7) Calculate $C_2 = K_1 \oplus M$ and $C_3 = \mathrm{MAC}(K_2, C_2)$, output ciphertext$C = C_1 \parallel C_3 \parallel C_2$. **(9)**

When User B receives the ciphertext message, it needs to decrypt the ciphertext and take out the plaintext information. Fig. 5 shows the flow of the public key decryption algorithm. Where *mlen* is the bit length of C_2 in ciphertext $C=C_1||C_3||C_2$, K_2_ *len* is the bit length of key K_2 in function MAC (K_2, *Z*), User B uses the decryption private key to decrypt the ciphertext. The decryption algorithm is as follows:

(1) Take the bit string C_1 from the bit string *C* and convert C_1 into the form of a point on an elliptic curve to judge whether it is true or not. If it is not true, an error message will be returned;

(2) Calculate the element $w = e(C_1, de_B)$ **(10)**
of group $G_T G_T$, convert the data type of ww to a bit string;

(3) Calculate klen $= mlen + K_2\_len$. **(11)**
then calculate $K = KDF(C_1 \parallel w \parallel ID_B, klen)$. **(12)**
let K_1 be the leftmost *mlen* bit of *k*, if K_1 is a string of zero bits, an error message will be returned;

(4) Calculate $M = C_2 \oplus K_1$, output plaintext M. **(13)**

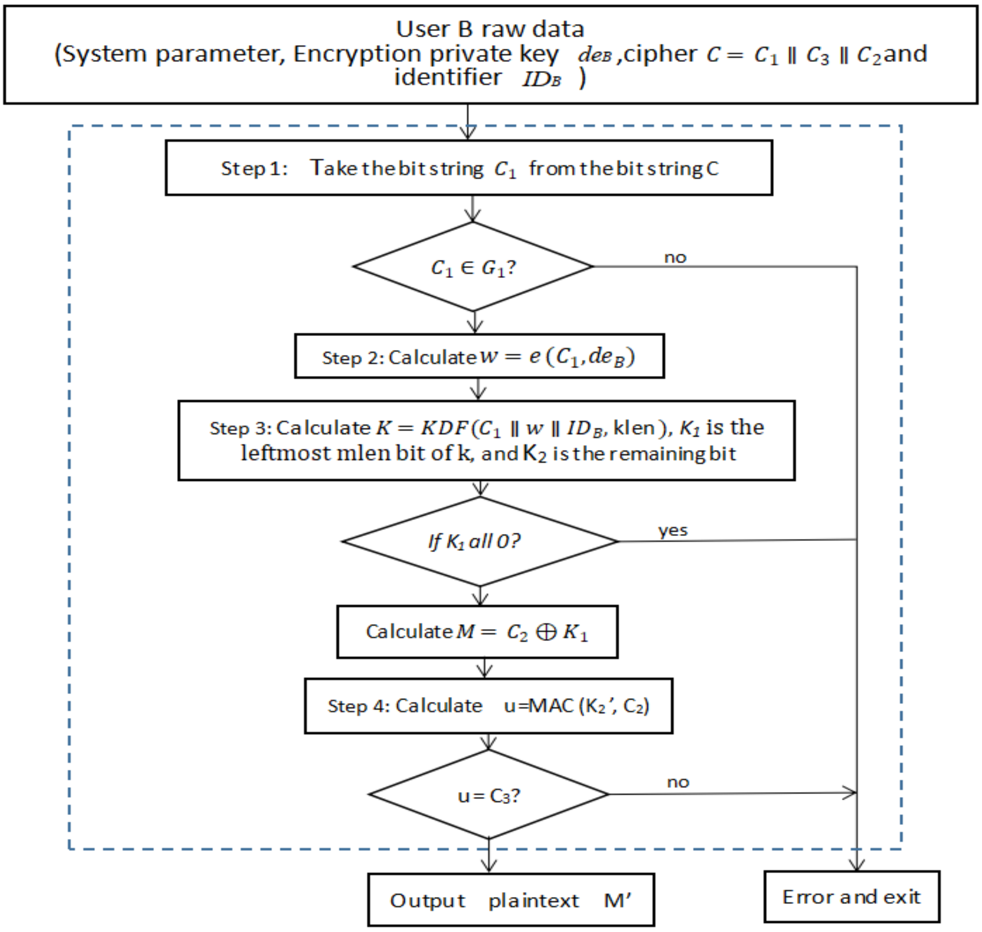
User B raw data
(System parameter, Encryption private key de_B ,cipher $C = C_1 \parallel C_3 \parallel C_2$ and identifier ID_B)
Step 1: Take the bit string C_1 from the bit string C
$C_1 \in G_1$?
no
Step 2: Calculate $w = e(C_1, de_B)$
Step 3: Calculate $K = KDF(C_1 \parallel w \parallel ID_B, \text{klen})$, K_1 is the leftmost mlen bit of k, and K_2 is the remaining bit
If K_1 all 0?
yes
Calculate $M = C_2 \oplus K_1$
Step 4: Calculate u=MAC (K_2', C_2)
u= C_3?
no
Output plaintext M'
Error and exit

Fig. 5. Decryption algorithm flow chart

3.2 Algorithm Analysis

Scheme of the design to the algorithm considering several aspects, such as the algorithm computational complexity, complexity, and so on. The SM9 identity cryptography algorithm is relatively complex, which not only includes the basic operations of modular addition and subtraction, modular multiplication and modular inverse in the finite field, but also includes complex algorithms such as elliptic curve group operation, HASH algorithm and bilinear mapping, as shown in Fig. 6.

Application layer	Digital signature, signature verification, data encryption, data decryption
Functional algorithm layer	Dot multiplication operation, HASH algorithm, bilinear mapping, modular power operation
Group computing layer	Point plus operation, double point operation
Domain operation layer	Modular addition and subtraction, modulo multiplication, modulo inverse

Fig. 6. Structure diagram of SM9 identity cipher algorithm

In the whole SM9 identity cryptosystem, digital signature and verification algorithm and public key encryption and decryption algorithm are in the application layer of SM9 cryptosystem [8]. Through the combination of point multiplication operation, extended domain modular exponentiation operation, cryptographic auxiliary function and bilinear pairing calculation, the corresponding functions are realized. The dot product operation, power operation of the twelfth extended domain module, HASH algorithm and bilinear pair calculation are in the functional algorithm layer. The dot product operation is implemented by scheduling point addition operation and multiple point operation on elliptic curve. The twelfth expansion modular power operation is based on the finite field operation. Hash algorithm adopts the SM3 HASH algorithm, which is mainly used to implement cryptographic auxiliary functions, including message authentication code function MAC and key derivation function KDF. The calculation of bilinear pairings includes not only the operation of point addition and doubling on elliptic curve, but also the power operation of extended domain module. The elliptic curve point-addition operation and point-doubling operation are located in the point operation layer of the cryptosystem, which schedule the operations in finite domain according to the group operation method. The bottom layer is the finite domain operation, including prime domain modular addition and subtraction, modular multiplication, modular inverse operation and extended domain modular addition and subtraction, modular multiplication, modular inverse operation. It can be concluded that finite-field operation is the basic unit of SM9 identification cipher algorithm, and its optimization is the key to improve the performance of cryptographic system.

4 The algorithm performance assessment and comparison

SM4 is the use of block password, symmetric encryption algorithm, and SM9 identification password algorithm is asymmetric encryption algorithm, DES algorithm is commonly used in the international symmetric encryption algorithm, the algorithm performance assessment and comparison of these algorithms. Based on the principle of each algorithm, the SM4 algorithm, DES algorithm and SM9 identity encryption algorithm written by Java language are implemented at first, and the algorithm speed, CPU occupation of several aspects of the experiment. When testing the algorithm speed, run the algorithm program several times and record the average running time of the program to test the algorithm running speed. Test CPU occupancy using the Windows System Performance Monitor to get the situation of the occupancy.

(1) Running speed of the algorithm

In the algorithm speed experiment, each algorithm program is allowed to run 50 times on the English string encrypted with less than 100 words, and the average running time of each algorithm program is shown in Table 1:

Table 1. Time used to encrypt and decrypt English characters

Algorithm	SM9 encryption algorithm	SM4 encryption algorithm	DES algorithm
Encryption time-consuming	528.85ms	279.64ms	335.72ms
Decryption time-consuming	17.34ms	4.35ms	4.90ms

Through the experimental results of the algorithm speed test can be seen, in the English string within 100 words for encryption and decryption, the speed of various algorithms have a big difference, among which SM4 algorithm encryption and decryption speed is the fastest, followed by DES algorithm, and SM9 encryption algorithm encryption and decryption time is the longest.

(2) CPU occupancy

According to the experimental results of CPU utilization of the algorithm, it can be seen that SM9 algorithm has the highest CPU utilization, followed by DES algorithm and last is SM4 encryption algorithm. CPU usage of each algorithm is shown in Table 2.

Table 2. CPU usage of each algorithm

Algorithm	SM9 encryption algorithm	SM4 encryption algorithm	DES algorithm
CPU occupancy	14%	8%	12%

(3) Comparison of safety strength of algorithms

Algorithm breaking is called cryptanalysis. In view of these encryption algorithms, the most effective cryptanalysis methods of these encryption algorithms are selected to carry out cryptanalysis respectively.The cryptographic security strength of the two algorithms can be judged by the time and space taken to decipher the algorithms. SM9 identity encryption algorithm uses different keys for encryption and decryption, so the key exhaustive search method is adopted. In a network of 3000 computers, the calculation of exhaustive key search can be carried out. Using the rough time estimation principle, it can be concluded that it takes several hours to several days to crack it. For SM4 algorithm, algebraic analysis is used to attack it. Algebraic analysis is to construct the calculation process of a cryptographic algorithm into a set of algebraic equations, and obtain the key information in the cryptographic algorithm by solving the unknown elements in the equations. In the algebraic analysis of the SM4 algorithm, the required space can be provided by a single personal computer, and the time cost is several days, which is mainly used to solve the equations. This is shown in the following Table 3.

Table 3. Comparison of algorithm security strength

Algorithm	Deciphering method	Time required	Space required
SM9 encryption algorithm	Key exhaustion search	Hours to days	Computer system
SM4 encryption algorithm	Algebraic analysis	Hours to days	Personal computer

Although the rough estimation time principle is used to measure the deciphering time, it does not prevent the analysis of the security strength of these two algorithms. SM9 encryption algorithm and SM4 encryption algorithm in exchange for a similar cost of time, but in the space required to decipher, the former is much larger than the latter. In other words, the security of SM9 encryption algorithm is better than SM4 encryption algorithm.

5 Summarization

Cloud edge collaboration can better match the needs of various application scenarios, maximize the value of edge computing and applications, and jointly help industrial enterprises achieve digital transformation. However, as large amounts of data are transmitted through the system, security issues arise. In this paper, we analyze the possible network attacks and their risks with regard to the secure transmission of data. After analyzing the SM9 lightweight algorithm and comparing it with the currently available algorithms for encryption, we conclude that it is suitable for application in data transmission encryption in terms of security and efficiency, and is going to apply it to the framework of data lightweight secure transmission. It provides a reference basis for secure data transmission.

6 Future Work

From the previous algorithm analysis and comparison, SM9 encryption algorithm consumes more time when processing large amounts of data encryption and decryption. But the encryption and decryption keys are inconsistent, the security is high and it is not easy to be cracked. SM4 symmetric encryption algorithm is very suitable for large amount of data encryption and decryption, but its safety is relatively low, to ensure the security of data transmission, we can use SM4 symmetric encryption algorithm for encryption and decryption, and SM9 algorithm for key management, at the same time, the SM3 hash algorithm is used to verify the integrity of data transmission to improve the security and efficiency of data transmission, this will be the future research direction of this article.

Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments. This research was supported by the National Natural Science Foundation of China under Grant No. U1836101, and Fund projects in the technical field of the basic strengthening plan of the science and Technology Commission of the Military Commission under Grant No. 2019-JCJQ-JJ-031.

References

[1] A. P. Premnath, Application of NTRU Cryptographic Algorithm for securing SCADA communication, 2013.
[2] W. Mahoney, A. Parakh, M. Battey, Hardare Implementation of Quasigroup Encryption for SCADA Networks, in: Proc. of

IEEE 13th International Symposium on Network Computing and Applications (NCA), 2014.

[3] W.W. Zhang, Research on data transmission and storage security scheme for cloud computing users, [Master's thesis] Beijing: Beijing University of Posts and Telecommunications, 2011.

[4] N. Wang, K.K. Yu, K. Li, M.J. Li, X. Wei, X.Q. Yu, Plant-Inspired Multifunctional Fluorescent Hydrogel: A Highly Stretchable and Recoverable Self-Healing Platform with Water-Controlled Adhesiveness for Highly Effective Antibacterial Application and Data Encryption-Decryption, ACS applied materials & interfaces 12(52)(2020).

[5] W. Qiang, Application of Data Encryption Technology in Computer Network Communication Security, International Journal of Social Sciences in Universities 3(4)(2020).

[6] R. K. Kumar, K. Subodh, K. Sunil, A data encryption model based on intertwining logistic map, Journal of Information Security and Applications 55(2020).

[7] Y.J. Liu, Application research of computer security protection technology based on cryptography, Information and Computer (Theoretical Edition) 32(22)(2020) 204-205.

[8] Y. Mao, J. Zhang, K.B. Letaief, Dynamic computation offloading for mobile-edge computing with energy harvesting devices, IEEE Journal on Selected Areas in Communications 34(12)(2016) 3590-3605.