IEEE IMCEC(ISSN:2693-2776)

2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) | 978-1-6654-7968-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/IMCEC55388.2022.10020036

A Secure and Efficient Hybrid Encryption Scheme for Power Regulation and Control Business

Yunfei Guo[1,2*], Peng Wu[1,2], Wei Huang[3], Yong Zhang[4], Jian Meng[5]
1. State Grid Smart Grid Research Institute Co. Ltd, Nanjing, China
2. State Grid Laboratory of Electric Power Communication Network Technology, Beijing, China
3. Electric Power Research Institute of State Grid Jiangsu Electric Power Co. Ltd, Nanjing, China
4. State Grid Shandong Electric Power Company Power Dispatching Control Center, Jinan, China
5. State Grid Qingdao Power Supply Company, Qingdao, China
guoyunfei@geiri.sgcc.com.cn, wupeng@geiri.sgcc.com.cn, h_w@js.sgcc.com.cn, zhangyong@sd.sgcc.com.cn, mengjianwww@163.com

Abstract—**The power communication network based on 5G network slicing is an important foundation to support smart grid, and the bearing of small granularity power regulation and control class services depends on the slicing soft isolation technology, and the data isolation between each soft isolation channel is crucial. In this paper, we propose a new symmetric cryptographic algorithm based on random coding, and establish a hybrid encryption method based on this symmetric algorithm, combined with SM2 and SM3 algorithms, which is suitable for encrypting the data of power regulation and control services. It is also verified through simulation that the proposed hybrid encryption method has high encryption efficiency while ensuring security.**

Keywords—power regulation service; network slicing; hybrid encryption; SM2；SM3

I. Introduction

With the continuous development of Chinese power system, the power business based on 5G bearer presents new features. For the power regulation and control business typically represented by distributed energy regulation, precise load control, distribution network area protection and distribution network automation, more stringent millisecond-level low latency transmission and ultra-high reliability higher than 99.99% are required.

However, there are still many important issues in carrying power regulation and control business through 5G virtual private network slicing. In terms of its communication performance, the communication needs to ensure regulation and control services are realized based on slicing isolation technology. However, since the current power virtual private network supports a large slice granularity (more than 1G), while the business data granularity of power regulation business is small, it is necessary to divide multiple soft slices within a hard slice for economic requirements. The implementation of soft slicing scheme under the existing network mechanism is based on the mapping of virtual local area network (VLAN) tag and network slice identification, but the sliced data under this method cannot achieve data isolation at hardware and time slot level. Therefore, more secure safeguards need to be studied to ensure the security of soft slicing. The most common way to achieve data isolation between soft slices is through encryption of service data.

In terms of data isolation between soft slices, various data encryption methods are widely used to achieve the economy of soft isolation and the cryptographic security of communication. In general, cryptographic algorithms are divided into symmetric cryptographic algorithms and asymmetric cryptographic algorithms [1]. Symmetric algorithms include AES, DES, 3DES, SM4, etc., and asymmetric algorithms include SM2, RSA, ECC, etc. Compared with the asymmetric algorithms, symmetric algorithms have high encryption efficiency [2]. However, the receiving parties need to share the secret key, and there is the problem of secret key leakage during the secret key transmission. Asymmetric algorithm uses public key for encryption and the receiver's own private key for decryption, which avoids the process of secret key transmission and has higher security, but also brings higher complexity [3]. In order to avoid the possible vulnerability of a single cryptographic algorithm, the industry often uses hybrid encryption to encrypt transmitted data. An effective hybrid approach is to make use of a symmetric cryptographic algorithm with low complexity to encrypt the relatively large volume of regulation business data, while using an asymmetric cryptographic algorithm with relatively complex implementation to encrypt the secret key of a symmetric algorithm with small volume to avoid the possible leakage of the symmetric algorithm secret key during transmission [3].

In literature [4], the hybrid use of AES and ECC cryptographic algorithms solves the problems of poor security and performance of traditional cryptographic algorithms in the cloud data storage of power bidding system. Where AES is used to encrypt large file blocks and ECC is used to encrypt small file blocks and the secret key of AES. In literature [5], a combination of AES encryption algorithm, RSA encryption algorithm and SHA256 encryption algorithm is used for the information transmission of the Zhejiang power market big data analysis system, and SHA256 is used to test the integrity of the transmitted message. However, their algorithms are entirely based on international cryptographic algorithms, which have certain risks. For the data of power regulation and control business, which is crucial to social production, certain domestic commercial cryptographic algorithms need to be used. In literature [6, 7], the SM4-ECC and SM4-SM2 algorithm combinations are chosen to build their encryption schemes. SM2 and SM4 are domestic commercial cryptographic algorithms with high enough security, and they prove that the proposed hybrid encryption system is higher than the single system algorithm in terms of security and diffusivity factor at the software level. However, the encryption and decryption efficiency of all the above hybrid cryptographic algorithms still needs to be improved in order to meet the increasingly stringent low latency requirements of power regulation and control operations. Since the main computational effort and complexity of the hybrid encryption approach comes from the symmetric cryptographic algorithm. However, in view of the actual demand for low latency and high reliability in power regulation and control business, the computational complexity of the currently popular AES, DES, SM4 and other algorithms is large, so there is a need to propose more secure and efficient symmetric cryptographic algorithms to achieve higher security and higher effectiveness than the classical symmetric algorithms.

The contribution of this paper is as follows.

(1) An efficient symmetric cryptographic algorithm based on random coding is proposed.

(2) A secure and efficient hybrid encryption scheme based on symmetric cryptographic algorithm, asymmetric cryptographic algorithm SM2, and cryptographic hash algorithm SM3 is proposed.

(3) Through simulation experiments, the proposed hybrid encryption algorithm is verified to have high encryption efficiency.

II. MATERIALS AND METHODS

To fully protect the security of power business data, realize the localization of encryption algorithms, and adapt to the increasingly strict low latency requirements of power regulation and control business, this paper proposes a secure and efficient hybrid cryptographic algorithm combining with a symmetric cryptographic algorithm and domestic commercial cryptographic algorithms SM2 and SM3. Among them, a new symmetric cryptography based on random coding (SCRC) is proposed to replace the traditional AES, DES and other symmetric cipher algorithms with high complexity.

A. SM2 asymmetric cryptographic algorithm

SM2 domestic commercial cryptographic algorithm is a public-key cryptographic algorithm whose security and complexity are equivalent to or slightly better than some international elliptic curve public-key cryptographic algorithms [8]. SM2 is essentially based on elliptic curves in the pseudo-Mason prime field GF(p): $E: y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0 \bmod p$, and $a, b \in \mathrm{GF(p)}$. In fact, in the National Cryptography Standard, the recommended parameters for the SM2 elliptic curve system defined on the 256-bit prime field are published.

B. SM3 password hash algorithm

The SM3 algorithm is a promiscuous algorithm whose input can be data of arbitrary length and whose output is a summary value of length 256 bits [9] . Since only the exact same data input will have the same output, SM3 is often used to compare two data to see if they are the same. The principle is as Fig. 1. It consists of two main steps: padding grouping and iterative compression.

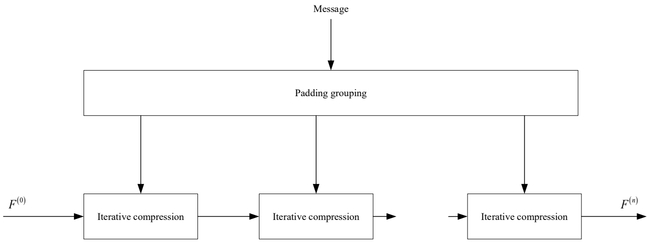


Fig. 1. SM3 algorithm flow chart.

Padding grouping: The length of the input data (bit) is padded to a multiple of 512 by padding 1s and 0s. The specific filling method is: add "1" at the end of the input data, then add several zeros and 64 bits of file information to make the total data length a multiple of 512, and group it in 512bit units.

$$F^{(i+1)} = CF\left(F^{(i)}, U^{(i)}\right), i = 0,1,2,\ldots,n-1 \quad (1)$$

Where, n is the number of groups; CF is the compression function, $F^{(0)}$ is the initial 256bit value, $U^{(\mathrm{i})}$ is the data grouping, and $F^{(n)}$ is the final hash result.

C. Symmetric cryptography based on random coding

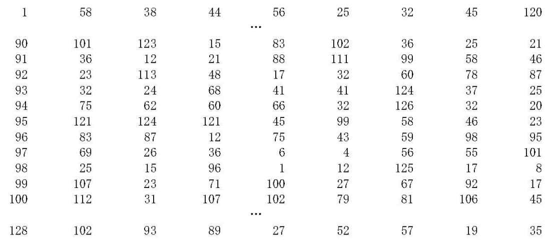
The proposed symmetric cryptographic method based on random coding mainly utilizes near-random coding techniques to achieve encryption, and the process is easy to implement in software and integrated circuit without mathematical operations such as bilinear mapping. And its encryption process is divided into four steps: generating random numbers, generating encoding tables, plaintext randomization and data encoding.

First, generate 4 random numbers. This includes an eight-digit random number V , where each digit takes values from 1 to 8, but each number can only be taken once, for example 36457128 and 45126873; a random number M that takes values between 1 and 128!; a random number L that takes values in the range 1 to 1000 and a random number N that values between 2 and 9.

Then a coding table is generated based on the values of M and L . Based on the random number M , the first M arrangement of the sequence $[1,2,\cdots,128]$ is generated by a factorial system and is denoted M_0 . The new number $M1$ is obtained by dividing M by L and rounding up to the nearest integer. Using M_0 as the base, generate the $M1$th arrangement of M_0 based on the factorial system, which is M_1 . Using M_1 as the basic arrangement, generate the $M1$th arrangement of M_1 based on the factorial system as M_2 . Using M_2 as the basic arrangement, generate the $M1$th arrangement of M_2 according to the factorial system, which is M_3 . And so on, we get M_4, M_5, M_6, M_7, M_8 , which is not repeated here. According to the above steps, the arrangement of $M_i\left(1 \le i \le 8\right)$ is used to generate the coding table. The coding table has 128 rows and 9 columns, the first column value is $1,2,\cdots,128$ and the first $j(2 \le j \le 9)$ column value is M_{j-1} .

The plaintext is then mixed and washed, i.e., the input business data is encoded for the first time. The random encoding-based symmetric cipher method described encodes 128 characters at a time, so the first 128 characters of the input data are taken and the plaintext is encoded according to the first column of the generated encoding table at N . Suppose $N = 7$, the plaintext message is "abcd". In the Fig. 2, the value of the 7th column of the encoding table is $[56,125,67,81]$, then "a" is encoded as the 56th symbol of ASCII code, i.e. "8"; "b" is encoded as the 125th symbol of ASCII code. Therefore, the result of the above plaintext message is "8}CQ" after plaintext randomization. Due to the limitation of the encoding table, this step can only operate 128 characters at a time, and it is only necessary to repeat this step for the subsequent business data. Note that if the data size is not a multiple of 128, you need to make up the zeros on the last segment of the data and write the number of zeros in the first part of the data to enable the receiver to decrypt it correctly.

The generation process of the encoding table uses a factorial system for generating the first M arrangement of a certain set of 128 characters, which works as follows. First, a basic arrangement A is determined, and the coefficient data $[a_{127}, a_{126}, \dots, a_0]$ is obtained by decomposing M into the form of $a_{127}127! + a_{126}126! + \cdots + a_0 0!$ according to the random number $M \in [1,128!]$.



1	58	38	44	56	25	32	45	120
				...				
90	101	123	15	83	102	36	25	21
91	36	12	21	88	111	99	58	46
92	23	113	48	17	32	60	78	87
93	32	24	68	41	41	124	37	25
94	75	62	60	66	32	126	32	20
95	121	124	121	45	99	58	46	23
96	83	87	12	75	43	59	98	95
97	69	26	36	6	4	56	55	101
98	25	15	96	1	12	125	17	8
99	107	23	71	100	27	67	92	17
100	112	31	107	102	79	81	106	45
				...				
128	102	93	89	27	52	57	19	35

Fig. 2. A table of possible codes.

Then select the a_{127}th character of A (starting from 0) as the 0th character of B . For the remaining 127 characters of A , the first a_{126} character is selected as the first character of B . And so on, a new arrangement of 128 characters from A is obtained at B , B is the output of the said factorial system, also called the M arrangement of the base arrangement A .

To illustrate more clearly how the factorial system works, let's take a simple example of a 5-bit character arrangement: suppose the initial arrangement of 5 symbols is [5 3 2 4 1], which has 5!=120 arrangements. If we want to get its arrangement, then the first thing we need to do is to convert it into the form of a cumulative sum of factorials of natural numbers, i.e. 0*4!+2*3!+ 2*2!+1*1!+0!, whose coefficient matrix is [0 2 2 1 0]. The original data are then ranked according to the specific values of the coefficient matrix. Since the 0th value of the coefficient matrix is 0, the 0th value of the system output is the 0th value of the original data [5 3 2 4 1], which is "5". After the "5" is extracted, the original data remains [3 2 4 1]. Since the 1st value of the coefficient matrix is 2, the 1st output of the system is the 2nd value of the remaining original data, i.e. "4". Now [3 2 1] is left, and since the 2nd value of the coefficient matrix is 2, the 2nd output of the system is the 2nd value of [3 2 1], i.e. "1". And so on, the output of the said system can be obtained as [5 3 2 4 1], which is also the $M = 17$ arrangement of the original input.

For the decryption of the proposed symmetric algorithm, the receiver needs to know the random number used by the sender: V, M, L, N . The decryption process of the proposed symmetric cryptographic method based on random encoding is the inverse process of the encryption method, and when the key is received, the receiver can easily generate the encoding table by the same method as the sender. The receiver can then easily and quickly decrypt the data by reverse substitution with the help of the encoding table and the random number V .

For the decryption of the proposed symmetric algorithm, the receiver needs to know the random number used by the sender: V, M, L, N . The decryption process of the proposed random encoding-based symmetric cryptography method is the inverse process of the encryption method, where the receiver can perform the same steps as the sender to obtain the corresponding encoding table based on the random number provided by the sender, and then replace the original data based on the encoding table, the random number V, N and the inverse operation.

After receiving the symmetric secret key, the receiver generates the same encoding table again according to the principle of encryption process to generate the encoding table. Then the reverse substitution is done based on the encoding table. For example, the encoding table shown in Figure 2 is 46357128, and the ciphertext is "SQ<c", the standard ACCII value of "S" (83) is found in column 5 of the encoding table (the 0th value of the random number 46357128 is 4). In Fig. 2, the value of 83 in column 5 is the element of the 90th ("Z") row, so we need to replace "S" with "Z". And so on, we can get the inverse replacement of "SQ<c" as "Zd^_".

According to the value of N in the secret key, the inverse plaintext randomization operation is performed to get the standard ASCII value corresponding to the original data and thus the plaintext data. The only difference is that the decoding process uses a different coding table each time, and the form of coding table transformation has been explained in the encryption process, so we will not repeat it here.

D. The proposed hybrid encryption method

This paper proposes a hybrid cryptographic algorithm that takes into account data security and encryption and decryption speed, and its flow chart is shown in Fig. 3. The role of the symmetric algorithm is to encrypt and decrypt the large volume of power regulation business data, the role of the asymmetric algorithm is to encrypt and decrypt the small volume of the symmetric algorithm secret key, and the promiscuous algorithm is used to calculate and compare the data summary of the business data between the receiving parties to ensure the integrity of the received data.

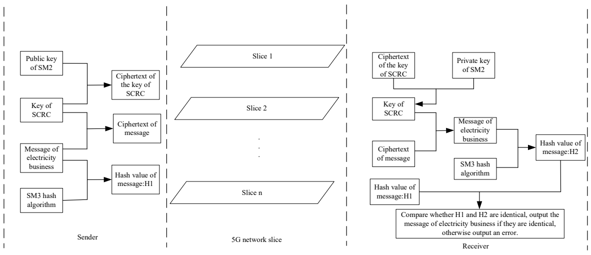


Fig. 3. Flow chart of hybrid cryptographic algorithm.

For data encryption: in the first place, a symmetric cryptographic algorithm based on random coding is used to encrypt the plaintext message of the electricity business data to form an encrypted ciphertext. Then the secret key of the above SCRC is encrypted using the SM2 public key to form the SCRC secret key ciphertext. Then the SM3 cryptographic hash algorithm is used to calculate the plaintext digest H1 for the plaintext message.

For data decryption: after the 5G network slicing transmission, the receiver receives the encrypted ciphertext, SCRC secret key ciphertext and plaintext digest, and then decrypts the SCRC secret key ciphertext with the SM2 private key to get the SCRC secret key. Then the SCRC secret key is applied to decrypt the encrypted ciphertext to get the plaintext message. Finally, compare the new plaintext digest H2 with the received plaintext digest H1, and output the plaintext message if they agree, otherwise, an error will be reported.

III. RESULTS & DISCUSSION

A. Security Analysis

The proposed hybrid encryption algorithm encrypts power data by SCRC symmetric cryptographic algorithm, which ensures the security of power business data. The connection between plaintext and ciphertext is effectively hidden by the two steps of plaintext mixing and data encoding, which makes it difficult for an attacker to link ciphertext and plaintext even if he also obtains them. For encrypted ciphertexts, the highly randomized encryption process greatly reduces the correlation between the ciphertext data and the original data. For example, even if the most frequent character "a" appears in the ciphertext, it is not considered to be the most frequent character in the original data because the encoding table changes after every 8 characters are encrypted.

The SCRC symmetric algorithm guarantees security against brute force attacks. For a single arrangement M, there are 128! possible arrangements, and the exhaustive number of times to find the correct arrangement by brute force attack is about $128!/2 = 1.92 \times 10^{215}$, which is much larger than the internationally popular 256-bit AES symmetric algorithm (2^{256}). Therefore, the security strength of the proposed algorithm is much stronger than the international classical algorithm. In fact, the proposed algorithm uses not only the random numbers M, but also L and N, which in turn significantly improves the security of the algorithm.

In order to make the secret key of the symmetric algorithm needs to be securely transmitted to the receiver, the SM2 public key cryptographic algorithm is used to encrypt the secret key of the symmetric cryptographic algorithm. the encryption of the SM2 algorithm is performed through the public key, but its decryption needs to use the private key provided by the secret key management center for the receiver, so even if the secret key of the pair of algorithms is captured by the attacker, the real secret key cannot be deciphered without the private key.

In addition, the SM3 promiscuous algorithm is used to compare the business data of both receiving parties, which ensures the integrity of the business data. Any loss or tampering of data during data transmission will change the output value of SM3 algorithm, making the data integrity and authenticity fully guaranteed.

B. Performance Analysis

It has been shown that using symmetric cryptographic algorithms to encrypt large blocks of data and asymmetric cryptographic algorithms to encrypt small blocks of symmetric secret keys is an efficient hybrid encryption method [3]. In this paper, we propose a more efficient SCRC symmetric cipher algorithm to replace the traditional symmetric cipher algorithm. Studies have shown that the encryption efficiency of symmetric encryption algorithm is much higher than the asymmetric cipher algorithm, and the AES algorithm is the most efficient one among the symmetric cipher algorithms[10, 11]. The AES algorithm is the most efficient among the symmetric cryptographic algorithms and outperforms other algorithms in terms of throughput and encryption and decryption time.

In this paper, we use different sizes of text data(in English) to compare the AES algorithm with a secret key length of 128 bits to verify the high performance of the proposed SCRC symmetric algorithm. The simulation is performed on a Windows 11 (64-bit) computer with Intel Core i7 3.2GHz CPU and 16GB RAM, and the programming language used is Java 1.8.0_25. For each data block, the encryption and decryption computations are repeated ten times, and then the average value is taken as the final result.

Table I. and Table II. show the comparison results of encryption time and decryption time of the proposed symmetric algorithm and AES algorithm, respectively. the data used for encryption and decryption are 5 sets of text data (in English) with sizes of 100kB, 1MB, 2MB, 5MB and 10MB, respectively. From the comparison results, we can see that the encryption and decryption efficiency of the proposed symmetric algorithm is better than that of AES algorithm. Defining the throughput as the average value of the total plaintext (k bytes) divided by the average encryption time, we can get the throughput of the proposed symmetric algorithm and AES as 14.8kB/ms and 13.7kB/ms, respectively, and the throughput of the proposed symmetric algorithm is better than that of AES.

The literature [4] proposes an efficient hybrid encryption method which uses AES symmetric encryption principle is to encrypt the data in chunks, with large file chunks encrypted using the AES algorithm, thus improving the total encryption efficiency, and small file chunks and the secret key of AES encrypted by ESS, thus improving the security. To verify the effectiveness of the hybrid encryption algorithm proposed in this paper that integrates SCRC symmetric algorithm, SM2 and SM3 algorithms, the simulation of this paper is implemented to compare with the hybrid encryption method proposed in literature [4], and the imitation parameter setting is consistent with the comparison of the previous symmetric algorithm, and the block ratio of AES+ECC method is set to 0.01. Fig. 4 shows the encryption time comparison of different hybrid cryptographic algorithms, and it can be seen from the figure that the encryption efficiency of the SCRC+ SM2+SM3 method proposed in this paper is significantly better than that of the AES+ECC hybrid encryption method proposed in [4], except in the case of text data larger than 100kB, which is more suitable for power regulation and control services with stricter requirements for low latency.

TABLE I. COMPARISON OF ENCRYPTION TIME OF SYMMETRIC ALGORITHMS (UNIT: MS)

Flie	*AES*	*Proposed method*
100kB	11.5	11.3
1MB	96.3	89.8
2MB	150.8	140.7
5MB	392.3	378.5
10MB	667.7	599.8

TABLE II. COMPARISON OF DECRYPTION TIME OF SYMMETRIC ALGORITHMS (UNIT: MS)

Flie	*AES*	*Proposed method*
100kB	12.9	11.7
1MB	126.3	88.9
2MB	188.6	145.8
5MB	512.8	377.5
10MB	796.7	580.1

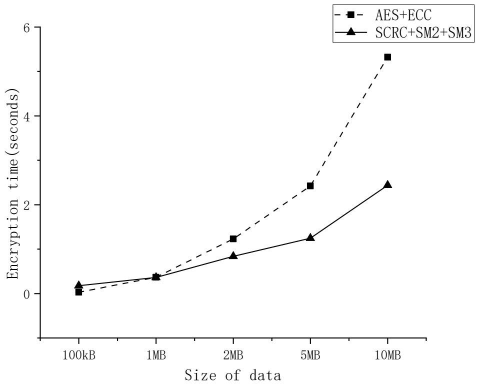


Fig. 4. Comparison of total encryption time of different hybrid cryptographic algorithms.

IV. CONCLUSIONS

In this paper, in terms of data isolation of soft slicing, a hybrid form of cryptographic algorithm is used to ensure the security of business data and symmetric secret keys while greatly improving the effectiveness of data encryption and decryption and saving the time of encryption and decryption. The proposed hybrid encryption method combined with soft slice isolation technology can effectively reduce the network rental cost and ensure the real-time and security requirements of power regulation and control services, which is of great significance to the safe bearing of power regulation and control services under 5G network.

ACKNOWLEDGMENT

This work was supported by State Grid Corp Science and Technology, China (NO.5700-202118444A-0-0-00).

REFERENCES

[1] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," International Journal of Scientific and Research Publications, vol. 8, no. 7, pp. 495-516, 2018.

[2] C. Yang, Y. Ling, and X. Li, "Information encryption algorithm in power network communication security model," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 750, no. 1: IOP Publishing, p. 012161.

[3] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," in 2021 2nd International Conference on Computing and Data Science (CDS), 2021, pp. 616-622.

[4] M. J. Ding, K. Cao, Z. X. Wang, and L. P. Zhu, "Design of a Cloud Storage Security Encryption Algorithm for Power Bidding System," in 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2020.

[5] L. Jin, J. He, W. Zhao, J. Pang, J. Lv, and L. Cheng, "Design of Electricity Market Big Data Analysis System Based on Hybrid Encryption and Secure Transmission," in 2021 IEEE 4th International Electrical and Energy Conference (CIEEC), 2021: IEEE, pp. 1-6.

[6] Bian Jianxiu, Li Yuanjiang, and Wang Jianhua, " STUDY ON SM4 AND ECC-BASED HYB R ID ENC R YPTION ALGO R ITHM," Computer Applications and Software, vol. 33, no. 10, pp. 303-306, 2016.

[7] FANG Yi, CONG Linhu, and DENG Jianqiu, " A Hybrid Encryption Scheme of Weapons and Equipment Data Based on National Security Algorithm," Journal of Detection & Control,, vol. 42, no. 1, p. 6, 2020.

[8] Wang Zhaohui and Zhang Zhenfeng, " Overview on Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves," Journal of Information Security Research, vol. 2, no. 11, pp. 972-982, 2016.

[9] L. B. Martinkauppi, Q. He, and D. Ilie, "On the design and performance of Chinese OSCCA-approved cryptographic algorithms," in 2020 13th International Conference on Communications (COMM), 2020: IEEE, pp. 119-124.

[10] M. Panda, "Performance analysis of encryption algorithms for security," in 2016 International conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016.

[11] N. A. Advani and A. M. Gonsai, "Performance analysis of symmetric encryption algorithms for their encryption and decryption time," in 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019: IEEE, pp. 359-362..