Scientific Research Publishing

Journal of Computer and Communications, 2022, 10, 42-56
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Research on a Secure Communication Protocol Based on National Secret SM2 Algorithm

Youhai Shao[1], Yong Wang[1], Yun Yang[1], Xiang Wang[2]

[1]College of Science, Shanghai University of Electric Power, Shanghai, China
[2]State Grid Shanghai Municipal Power Company, Shanghai, China

Email: 15279265616@163.com

How to cite this paper: Shao, Y.H., Wang, Y., Yang, Y. and Wang, X. (2022) Research on a Secure Communication Protocol Based on National Secret SM2 Algorithm. *Journal of Computer and Communications*, **10**, 42-56.
https://doi.org/10.4236/jcc.2022.101003

Received: April 20, 2021
Accepted: January 14, 2022
Published: January 17, 2022

Abstract

Most of the public key algorithms used in the exchange of information for power data transmission protocols are RSA. The core of the key part of this kind of algorithm system has not been announced. For the domestic sensitive information data field, there are threats such as preset backdoors and security vulnerabilities. In response to the above problems, the article introduces a secure communication protocol based on the optimized Secret SM2 algorithm, which uses socket programming to achieve two-way encrypted communication between clients and services, and is able to complete the security protection of data encryption transmission, authentication, data tampering, etc., and proves through experiments that the security protocol is more secure than traditional methods, can effectively identify each other, carry out stable and controllable data encryption transmission, and has good applicability.

Keywords

Secret Algorithm SM2, Communication Protocol, Hybrid Encryption, Security Protection

1. Introduction

In recent years, with the intensified construction of power grid informatization and the country's high requirements for the integration of urban intelligence, traditional electric energy meters are faced with energy that integrates key information from households and community users in addition to meeting the standard high-precision measurement of electric energy parameters. By building a power user information collection system with good performance and multi-functional feedback, it is of great importance not to be underestimated for the strategic layout of the macro-control of power prices and the guidance of reasonable power use to achieve high-efficiency use of power energy. The power information collection system generally uses public network (especially wireless) communication technology to exchange information. Therefore, the research and development and design of a high-performance and high-precision power information interaction system and the use of secure communication protocols for transmission are safe for power information data. Protection has unprecedented challenges [1] [2] [3].

So far, the transmission protocol for power information [4] has many standards, but most of them are in the stage of customization framework, and no specific solutions are clearly specified, and most of the cryptographic algorithms recommended to use are the ones frequently used by the international mainstream. Algorithms, this poses a greater security risk for sensitive data such as electricity related to our people's livelihood. Once the information infrastructure is not well protected, the consequences are unimaginable. It is even more necessary to adopt the algorithm system designed by my country's independent production for security protection to avoid risks such as backdoor events and vulnerabilities in the current mainstream public key algorithm RSA. The SM series of algorithms independently developed and designed by my country in the field of cryptography can effectively avoid this security hazard by participating in the formulation of standards throughout the entire process. At the same time, because the SM2 algorithm [5] is mathematically designed based on elliptic curves, it is very strong compared to previous algorithms such as RSA. The anti-interference ability, fast calculation speed, small calculation amount and performance has the advantages of greatly improving. Based on such a consideration, with the continuous and stable development of cryptographic algorithms in my country, it has become a hot spot to use this type of algorithm to replace the traditional encrypted transmission of power information data. Literature [6] Luo Zhao *et al.*, by optimizing the National Secret SM2 algorithm and in-depth study of its communication protocol interaction process, designed an information protection platform that satisfies the state's independent and controllable standards for the power information industry. This information security platform can ensure the accuracy of the identities of the communication parties. It is correct and protects the privacy of the authority of whether different users can access normally, and realizes the personalized management and control of different roles, but it is impossible to implement the layout of the park in a small area. Literature [7] Dong Weiwei *et al.* proposed the use of RSA-AES-HASH authentication scheme, using a hybrid cryptosystem to realize the identity authentication of the electric meter and the data center, which can integrate the advantages of convenience, security and speed of key management. However, this authentication method consumes a lot of time and is not conducive to real-time delivery. Literature [8] Chen Yalin and others used a symmetric broadcast protocol to calculate the key for the stable operation of the active distribution network, which improved the physical equipment's high requirements for time performance and the difficulty of broadcast authentication. At the same time, the secure communication protocol based on asymmetric keys passed Digital signatures effectively prevent malicious third-party attacks such as denial of service attacks. Due to the adoption of the public key system of the national secret SM2 algorithm, the security has been greatly improved. However, this method does not conduct an overall study on collection protection, and cannot avoid the possibility of man-in-the-middle attacks. Reference [9] Zuo Gao *et al.* aimed at the problem that power distribution automation terminal equipment needs to be powered off during the upgrade and transformation process, the national secret SM2 algorithm is used as the encryption module to authenticate the information integrity of the command message and the identity of the communicating parties. This method can meet Intelligent power distribution terminals have basic requirements for information security protection integrity and authentication, but the design of this encryption module does not introduce timestamps to improve the anti-attack of data signatures. It is prone to brute force cracking by illegal intrusions and has certain security risks exist.

In summary, this research method is based on such a background to study the security of the intelligent electricity information collection system in the perception layer, an important component of the "Power Internet of Things", through the embedded main control chip and The three-phase electric energy special collection chip builds a small user power information collection system, and transmits it to the display development platform of Alibaba Cloud server in real time through the MQTT protocol. The article is based on a real experimental environment to study the information collection technology and the key technology of active transmission for the security of power information. The article mainly studies the communication security protocol transmission data based on the optimization of the national secret algorithm SM2, mainly including the analysis of the SM2 algorithm, the network communication protocol, the realization of the simulated client server communication, and the experimental security analysis. Through the process of designing and implementing the protocol, the programming code design of network communication is carried out, and different system protection schemes are compared at the same time, and finally it is proved that the communication protocol is safe and efficient.

The article first discusses the digital signature algorithm, puts forward that the algorithm can be optimized and improved, and analyzes and proves its mathematical security logic, and then combines the commonly used protocol development basis to implement the design and development of the protocol process, and finally proposes the use of SM2. Security protection, mixed use of SM3/SM4 to strengthen the strict security of the communication protocol, the use of network programming to achieve the experimental process of the secure communication protocol proves the feasibility of the proposed scheme in this paper.

2. Digital Signature SM2 Algorithm Optimization and Improvement

Identity authentication SM2 algorithm [10] [11] [12] is that a signer generates a valid digital signature for the data that needs to be processed, and a verifier verifies the authenticity of the signature. Since the mechanism of SM2 is also based on an elliptic curve, the difference from ECDSA is that the selected curve equation is not the same. The specific curve used by the former is secp25k1, while SM2 uses the 256-bit element field GF(p). The elliptic curve sm2p256v1. This signature algorithm is different from ECDSA which directly processes the digest value of the message. Two preprocessing steps are required before signature verification: First, the message sender mixes the user ID and the public key of the message receiver into the elliptic curve parameters and passes through the cryptographic hash algorithm SM3 [13] obtains a result, and then uses the result and the message to be processed to further process the digest based on the hash function. Based on the traditional SM2 digital signature algorithm, on the one hand, the source of randomness numbers is the use of pseudo-random number generators (PRNGs), which are vulnerable to brute force attacks for their collision resistance, and time stamps can be introduced to prevent replay attacks; On the one hand, the reference calculation steps given by the National Secret Standard are relatively redundant. In order to increase the calculation speed, the calculation process can be processed in parallel at the same time to reduce communication costs and improve signature efficiency. In order to solve the above problems, this section optimizes the complete SM2 identity authentication algorithm through discussion and analysis. The specific operation flow of the optimized algorithm is discussed below. The flowchart of the SM2 algorithm signature calculation process after optimization is shown in **Figure 1**.

The optimized SM2 algorithm signature generation steps are described as follows:

Input: the public parameters on the elliptic curve, the private key d of the signing party and the message M to be processed;

Output: signature value (r, s);

Step 1: Let $M^* = Z \| M$, Z denote the output result obtained by the above preprocessing process;

Step 2: calculation $e = H_v\left(M^*\right)$;

Step 3: Introduce a random number generator algorithm with coordination time to generate random numbers $k \in [1, n-1]$ and calculate $k[*]G = (x_1, y_1)$;

Step 4: Calculate $r = (x_1 + e) \bmod n$, IF $r = 0$ or $r + k = n$, then return to step 3;

Step 5: Calculate $s = \left((1+d_A)^{-1} \cdot (k - rd_A)\right) \bmod n$, IF $s = 0$, then return to step 3;

The SM2 verification signature calculation process after optimization is shown in **Figure 2**.

The steps of the optimized SM2 signature verification algorithm are described as follows:

Input: system public parameters params, public key P, signature (r', s')

Output: true or false

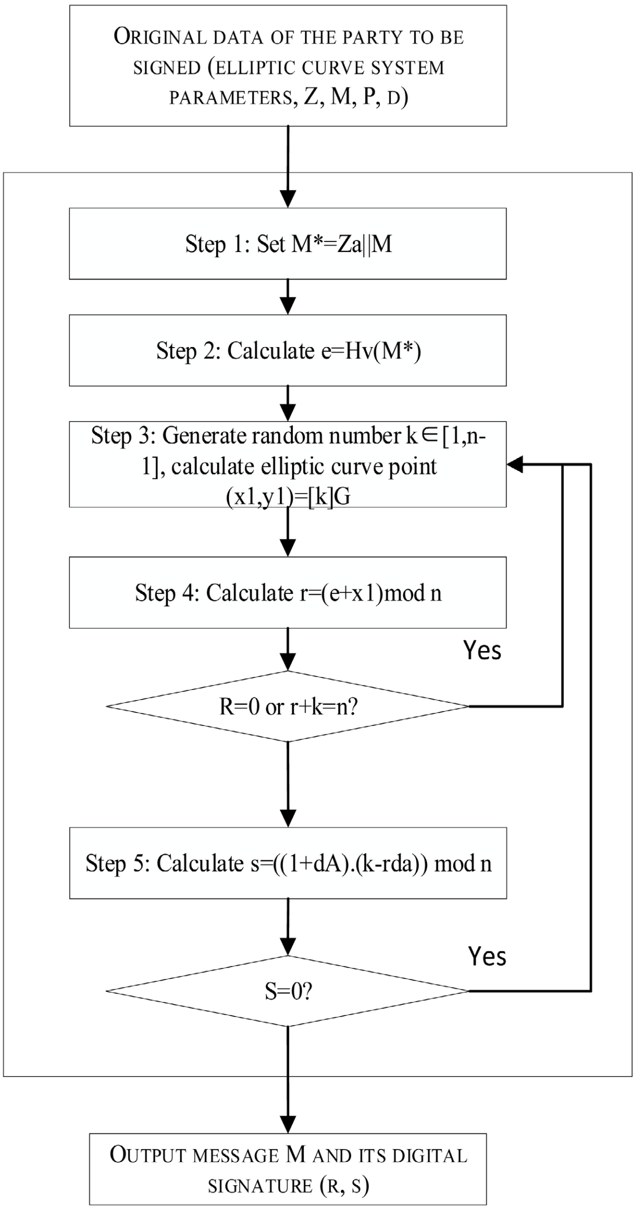

ORIGINAL DATA OF THE PARTY TO BE SIGNED (ELLIPTIC CURVE SYSTEM PARAMETERS, Z, M, P, D)
Step 1: Set M*=Za||M
Step 2: Calculate e=Hv(M*)
Step 3: Generate random number k∈[1,n-1], calculate elliptic curve point (x1,y1)=[k]G
Step 4: Calculate r=(e+x1)mod n
Yes
R=0 or r+k=n?
Step 5: Calculate s=((1+dA).(k-rda)) mod n
Yes
S=0?
OUTPUT MESSAGE M AND ITS DIGITAL SIGNATURE (R, S)

Figure 1. The signature calculation process after optimizing the SM2 algorithm.

Step 1: IF $r', s' \in [1, n-1]$, Then TRUE else FALSE;

Step 2: Set $M^* = Z_a \| M$, calculation $e' = \text{Hash}(M^*)$;

Step 3: IF $t = (r' + s') \bmod n \in 0$, Then FALSE else TRUE;

step 4: Calculation the point on the ECC point $(x_1, y_1) = [s]G + [t]P_A$;

Step 5: IF $R = (x_1' + e') \bmod n == r'$, Then TRUE else FALSE;

First, prove the correctness analysis of the optimized identity authentication process:

1) It is guaranteed $r \in [1, n-1]$ and $s \in [1, n-1]$ when signing and if there is an error in data tampering or loss during transmission, the signature will be verified $r' \in [1, n-1]$ and $s' \in [1, n-1]$, it can be found whether there is an error, so as to ensure its correctness;

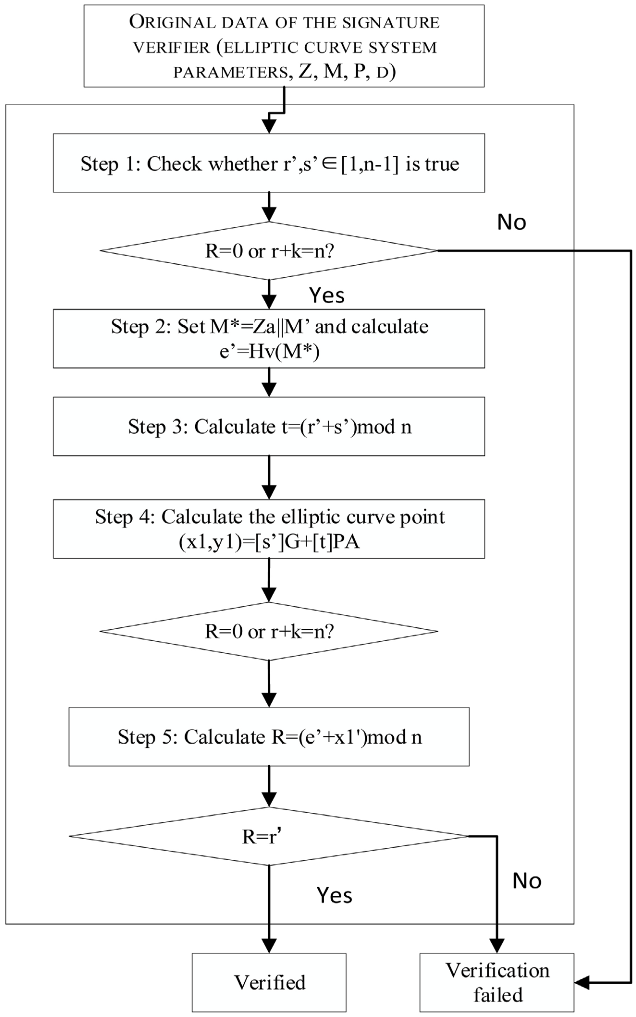

Original data of the signature verifier (elliptic curve system parameters, Z, M, P, d)
Step 1: Check whether r',s'∈[1,n-1] is true
R=0 or r+k=n?
No
Yes
Step 2: Set M*=Za||M' and calculate e'=Hv(M*)
Step 3: Calculate t=(r'+s')mod n
Step 4: Calculate the elliptic curve point (x1,y1)=[s']G+[t]PA
R=0 or r+k=n?
Step 5: Calculate R=(e'+x1')mod n
R=r'
Yes
No
Verified
Verification failed

Figure 2. Verify the signature calculation process after optimizing the SM2 algorithm.

2) It is also ensured $r \neq 0$ and $s \neq 0$ when signing, if $t = r + s = 0 \bmod n$ is an integer multiple of *n*, and when signing, it is ensured that $r + s$ it is not an integer multiple of *n*, $r + s = (1+d)^{-1} \cdot \left[r + (k - rd) \right] = (1+d)^{-1} \cdot (r + k)$, so $r + k$ it is not an integer multiple of n, otherwise because d is a positive integer, it will result in Integer multiples $(1+d)^{-1}(r+k)$ of *n*, creating contradictions;

3) On the one hand, $sG + tP_A = sG + (r+s)(dG) = (s + rd + sd)G$, on the other hand, $(s + rd + sd) = s(1+d) + rd = \left[(1+d)^{-1} \cdot (k - rd) \right](1+d) + rd$, so $sG + tP_A = kG = G_1(x_1 + y_1)$, and if x and e are correct, then there is $e' = e$, $x_1' = x'$, so the signature authentication is passed;

Secondly, the random number generation of the traditional digital signature authentication algorithm SM2 does not specify what standard to use. In previous studies, it is often only generated by a very common pseudo-random number generator, and the randomness of random number generation is not carried out. Research in this area. Generally speaking, the random number function should have ran domness, unpredictability, and non-reproducibility at the same time, and the relationship between them is strictly increasing. The definition of Coordinated Universal Time (UTC) refers to the number of seconds that have elapsed from the computer UNIX timestamp on January 1, 1970 to the current operation being executed. Obviously, this time is changing all the time and rising continuously. By introducing this time method, the randomness of the random number generator can be effectively in creased.

3. Communication Security Protocol Design

3.1. Communication Protocol Foundation

A series of steps that need to be operated in order to complete a specific goal belong to the category of algorithms, and agreements that are different from how specific steps are implemented are based on a set of mutual agreements that need to be followed. Although the development of information technology has brought new breakthroughs to all walks of life, network communication protocols are also facing various security problems, and the reliable data transmission of users on the channel has attracted many people's attention. Multiple communication protocols based on the TCP/IP protocol cluster complete the specified information exchange function, accelerating the construction of different application scenarios. The secure socket protocol [13] is the transition protocol between the protocol and the application layer. According to the model classification, it can be regarded as the recording layer and the handshake layer. Each layer will perform corresponding operations to complete the corresponding service. There is an interface for mutual exchange with the layer. Specifically, the record layer protocol provides basic functions such as encryption and compression, and the handshake layer completes identity authentication and is responsible for key distribution on this basis. The protocol uses digital certificates to determine whether the entities of both parties in communication are authentic, uses public key cryptographic algorithms for key negotiation, uses symmetric encryption algorithms to encrypt data before transmission to ensure data confidentiality, and calculates a digital digest to verify that the data is in Whether it has been tampered with or forged during the transmission process, it provides a safe mechanism for the transmission of sensitive data of the user's power information on the communication channel. This protocol can prevent such incidents from occurring. Although the communication protocol is diverse, the transformation and optimization of the security protocol is still a very worthy research direction. Next, the specific design and development process of the security protocol will be discussed.

3.2. Security Protocol Process

Regarding the data acquired by the power information collection system, the OpenSSL-based development environment [14] is an open cryptographic algorithm library. By optimizing the library, the security protocol design is not only good for portability, but also compatible with different development platforms. The integration level is very high, very suitable for expansion. The security protocol communication operation process based on this design and development of this program is shown in Figure 3.

The realization of the idea in the specific communication process can be carried out according to the following steps:

1) Negotiate the session communication protocol. Before starting the SSL session, select a protocol acceptable to both parties in this session. Such protocols must be compatible with each other, otherwise the normal communication connection cannot be established;

2) Prepare the content required for this session environment. After applying for this session environment, specify the verification method of the certificate in the handshake phase and load the public key certificate. At the same time, load the digital certificate of the message publisher, the certificate contains the public key used to encrypt the key to provide a verification method for identity confirmation, load the user's private key and verify whether the private key and the certificate are equal;

3) The SSL socket service is established normally, and the socket bound by the command is based on the ordinary TCP socket;

4) Completing the session handshake phase. During the handshake process, both parties in communication will negotiate to inquire about the certificate information of both parties in order to perform corresponding verification, and the certificate information can be obtained later;

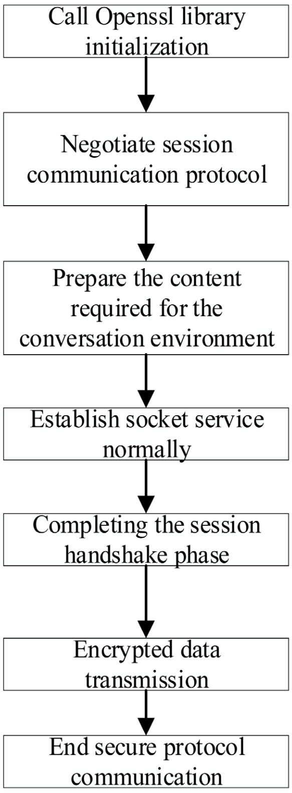

Call Openssl library initialization
Negotiate session communication protocol
Prepare the content required for the conversation environment
Establish socket service normally
Completing the session handshake phase
Encrypted data transmission
End secure protocol communication

Figure 3. Secure communication protocol communication.

5) Encrypted data transmission. After the above-mentioned handshake is completed, the data can be secured during the transmission process;

6) End the secure protocol communication. After the two parties complete the data secure communication, the SSL resources that have been applied for are released, and the entire secure communication process ends.

Finally, the above-mentioned security protocol communication process is summarized as the following points: First, A sends a request dialogue to B, and jointly negotiates the use of the transfer encryption algorithm SM4; then B sends a digital certificate issued by itself to determine its identity and contains the public key. A determines whether it needs to establish reliable communication with the other party by verifying the identity of B, avoiding information exchange with the wrong receiver, and ensuring that both parties in normal communication are accurate; further A will generate a random number as a temporary session key, Using the idea of hybrid encryption, the session key is encrypted with the public key in the certificate sent by B before transmission, which effectively solves the problem of key distribution; finally, B obtains the session key for this communication After that, the common key used by both parties for this communication will be obtained under the premise of their own private key, which ensures the security of the key. After the process of the above-mentioned security protocol, the data can be transmitted in a secure channel.

3.3. Communication Programming Design

Network communication programming [15] can be implemented through sockets. Different processes use port number binding to determine what service applications are used. Sockets are created to complete the mutual communication between different processes.

First, the server will take the initiative to create a socket, because each process identifier in the communication process will specify the allocated resources according to the IP address and port number, so the server can bind it. At this time, the server socket has not been opened, but Complete the initialization work for accepting applications from the client;

Secondly, the client also creates a socket and establishes a connection with the server through the provided IP address and port number. The connection status is divided into three handshake interactions, and finally the connection success status Establisted is sent to the server, and the server confirms the receipt through the accept method. After the two ends establish communication through the above operations, they can respectively receive/send data with each other, and the data can be switched back and forth through the buffer to the buffer area. After a series of communication and exchange of information, each one is closed one after another, and the entire complete communication process ends since then.

Based on the above-mentioned communication process, the main program interaction process of the designed safety communication protocol is shown in **Figure 4**.

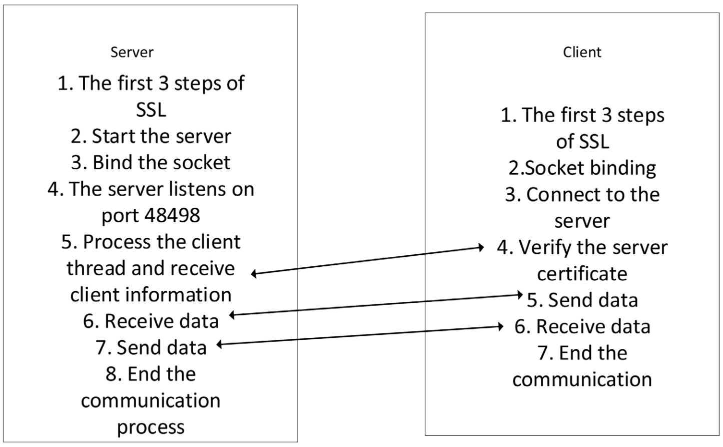

Server
1. The first 3 steps of SSL
2. Start the server
3. Bind the socket
4. The server listens on port 48498
5. Process the client thread and receive client information
6. Receive data
7. Send data
8. End the communication process
Client
1. The first 3 steps of SSL
2.Socket binding
3. Connect to the server
4. Verify the server certificate
5. Send data
6. Receive data
7. End the communication

Figure 4. Safety protocol communication main.

4. Experimental Verification and Analysis

The main part of the two-way communication simulation experiment built in this article will be carried out according to the following steps:

First create the EC parameters and optimize the SM2 algorithm to generate the private key file, and check the specific content of the private key file as shown in **Figure 5**.

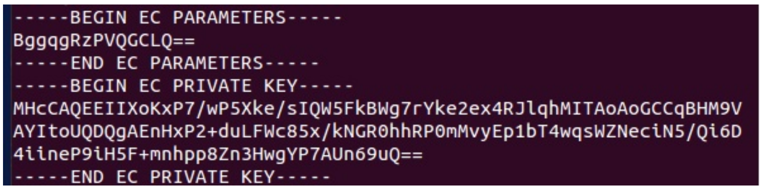
Then use the public key cryptosystem idea to use its private key to derive the corresponding SM2 public key file, and the file content is expanded as shown in **Figure 6**.

After the above preparation, the key pair of SM2 has been generated.

Due to the introduction of an asymmetric cryptographic algorithm in the digital signature algorithm, although it can prevent denial, the sender cannot determine whether the received public key is the only paired public key generated by the receiver's private key pair, so it is vulnerable to man-in-the-middle attacks. In order to prevent man-in-the-middle attacks, a self-signed certificate needs to be generated to determine the identity. This digital signature certificate has a five-year validity period. The result of the certificate generation is shown in **Figure 7**.

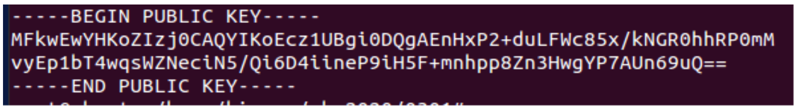
In order to further see the specific key information of the certificate, the above certificate is formatted to be able to visually see the content of the digital certificate. The certificate can be obtained mainly using the SM2 digital signature algorithm based on SM3, and the validity period of the certificate is 5 For the year, who is responsible for signing the issuance, the public key corresponding to the person responsible for the issuance is a 256-bit string, and the certificate generation result is shown in **Figure 8**.

After the above preparation process, the following safety protocol is used to simulate communication experiments. The communication process needs to open the client and server at the same time for communication connection. Open the server for port monitoring. The result of the communication operation are shown in **Figure 9**. At this time, you can see that the socket has been created, the binding



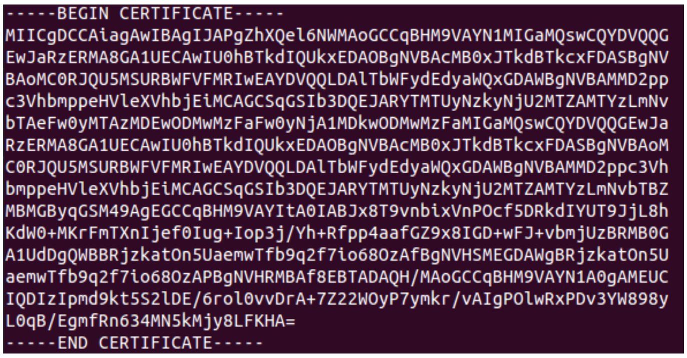
```
-----BEGIN EC PARAMETERS-----
BggqgRzPVQGCLQ==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIIXoKxP7/wP5Xke/sIQW5FkBWg7rYke2ex4RJlqhMITAoAoGCCqBHM9V
AYItoUQDQgAEnHxP2+duLFWc85x/kNGR0hhRP0mMvyEp1bT4wqsWZNeciN5/Qi6D
4iineP9iH5F+mnhpp8Zn3HwgYP7AUn69uQ==
-----END EC PRIVATE KEY-----
```

Figure 5. SM2 private key generation.



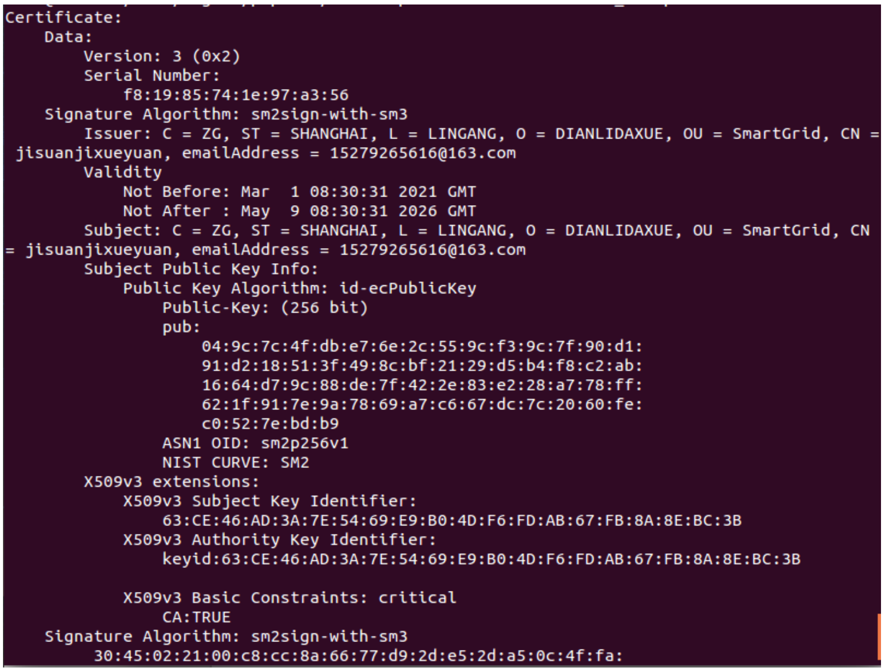
```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAEnHxP2+duLFWc85x/kNGR0hhRP0mM
vyEp1bT4wqsWZNeciN5/Qi6D4iineP9iH5F+mnhpp8Zn3HwgYP7AUn69uQ==
-----END PUBLIC KEY-----
```

Figure 6. SM2 public key generation.



```
-----BEGIN CERTIFICATE-----
MIICgDCCAiagAwIBAgIJAPgZhXQel6NWMAoGCCqBHM9VAYN1MIGaMQswCQYDVQQG
EwJaRzERMA8GA1UECAwIU0hBTkdIQUkxEDAOBgNVBAcMB0xJTkdBTkcxFDASBgNV
BAoMC0RJQU5MSURBWFVFMRIwEAYDVQQLDAlTbWFydEdyaWQxGDAWBgNVBAMMD2pp
c3VhbmppeHVleXVhbjEiMCAGCSqGSIb3DQEJARYTMTUyNzkyNjU2MTZAMTYzLmNv
bTAeFw0yMTAzMDEwODMwMzFaFw0yNjA1MDkwODMwMzFaMIGaMQswCQYDVQQGEwJa
RzERMA8GA1UECAwIU0hBTkdIQUkxEDAOBgNVBAcMB0xJTkdBTkcxFDASBgNVBAoM
C0RJQU5MSURBWFVFMRIwEAYDVQQLDAlTbWFydEdyaWQxGDAWBgNVBAMMD2ppc3Vh
bmppeHVleXVhbjEiMCAGCSqGSIb3DQEJARYTMTUyNzkyNjU2MTZAMTYzLmNvbTBZ
MBMGByqGSM49AgEGCCqBHM9VAYItA0IABJx8T9vnbixVnPOcf5DRkdIYUT9JjL8h
KdW0+MKrFmTXnIjef0Iug+Iop3j/Yh+Rfpp4aafGZ9x8IGD+wFJ+vbmjUzBRMB0G
A1UdDgQWBBRjzkatOn5UaemwTfb9q2f7io68OzAfBgNVHSMEGDAWgBRjzkatOn5U
aemwTfb9q2f7io68OzAPBgNVHRMBAf8EBTADAQH/MAoGCCqBHM9VAYN1A0gAMEUC
IQDIzIpmd9kt5S2lDE/6rol0vvDrA+7Z22WOyP7ymkr/vAIgPOlwRxPDv3YW898y
L0qB/EgmfRn634MN5kMjy8LFKHA=
-----END CERTIFICATE-----
```

Figure 7. Digital certificate content (PEM) format.

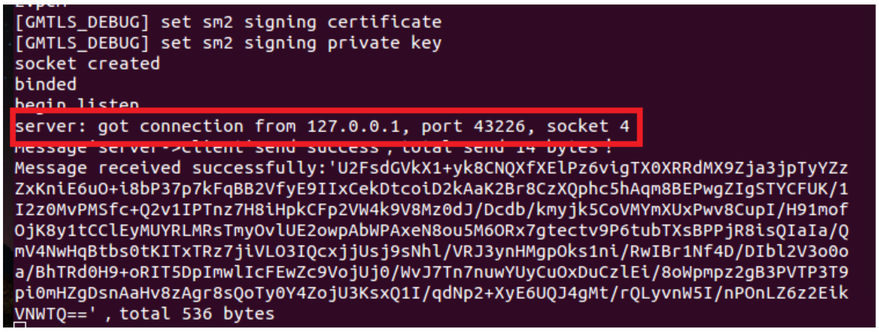


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f8:19:85:74:1e:97:a3:56
    Signature Algorithm: sm2sign-with-sm3
        Issuer: C = ZG, ST = SHANGHAI, L = LINGANG, O = DIANLIDAXUE, OU = SmartGrid, CN =
 jisuanjixueyuan, emailAddress = 15279265616@163.com
        Validity
            Not Before: Mar  1 08:30:31 2021 GMT
            Not After : May  9 08:30:31 2026 GMT
        Subject: C = ZG, ST = SHANGHAI, L = LINGANG, O = DIANLIDAXUE, OU = SmartGrid, CN
= jisuanjixueyuan, emailAddress = 15279265616@163.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:9c:7c:4f:db:e7:6e:2c:55:9c:f3:9c:7f:90:d1:
                    91:d2:18:51:3f:49:8c:bf:21:29:d5:b4:f8:c2:ab:
                    16:64:d7:9c:88:de:7f:42:2e:83:e2:28:a7:78:ff:
                    62:1f:91:7e:9a:78:69:a7:c6:67:dc:7c:20:60:fe:
                    c0:52:7e:bd:b9
                ASN1 OID: sm2p256v1
                NIST CURVE: SM2
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                63:CE:46:AD:3A:7E:54:69:E9:B0:4D:F6:FD:AB:67:FB:8A:8E:BC:3B
            X509v3 Authority Key Identifier:
                keyid:63:CE:46:AD:3A:7E:54:69:E9:B0:4D:F6:FD:AB:67:FB:8A:8E:BC:3B

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sm2sign-with-sm3
         30:45:02:21:00:c8:cc:8a:66:77:d9:2d:e5:2d:a5:0c:4f:fa:
```

Figure 8. Digital certificate.

is successful, and the monitoring starts. Waiting for the communication request with the client IP address of 127.0.0.1 and port number of 43,226 ceive the sent data and then read the communicated data.



```
[GMTLS_DEBUG] set sm2 signing certificate
[GMTLS_DEBUG] set sm2 signing private key
socket created
binded
begin listen
server: got connection from 127.0.0.1, port 43226, socket 4
message server->client send success , total send 14 bytes !
Message received successfully:'U2FsdGVkX1+yk8CNQXfXElPz6vigTX0XRRdMX9Zja3jpTyYZz
ZxKniE6uO+i8bP37p7kFqBB2VfyE9IIxCekDtcoiD2kAaK2Br8CzXQphc5hAqm8BEPwgZIgSTYCFUK/1
I2z0MvPMSfc+Q2v1IPTnz7H8iHpkCFp2VW4k9V8Mz0dJ/Dcdb/kmyjk5CoVMYmXUxPwv8CupI/H91mof
OjK8y1tCClEyMUYRLMRsTmyOvlUE2owpAbWPAxeN8ou5M6ORx7gtectv9P6tubTXsBPPjR8isQIaIa/Q
mV4NwHqBtbs0tKITxTRz7jiVLO3IQcxjjUsj9sNhl/VRJ3ynHMgpOks1ni/RwIBr1Nf4D/DIbl2V3o0o
a/BhTRd0H9+oRIT5DpImwlIcFEwZc9VojUj0/WvJ7Tn7nuwYUyCuOxDuCzlEi/8oWpmpz2gB3PVTP3T9
pi0mHZgDsnAaHv8zAgr8sQoTy0Y4ZojU3KsxQ1I/qdNp2+XyE6UQJ4gMt/rQLyvnW5I/nPOnLZ6z2Eik
VNWTQ==' , total 536 bytes
```

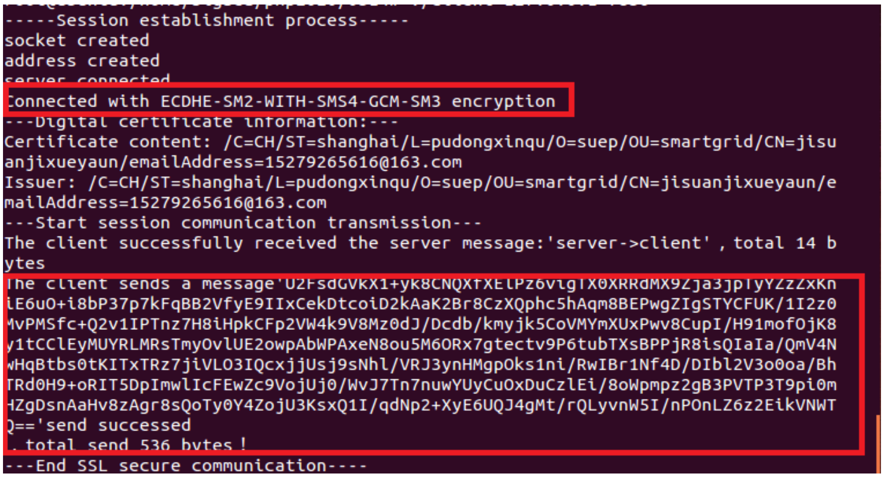
Figure 9. Server communication interface.

When the client is running, the communication interface is shown in Figure 10. During the information exchange process, the ECDHE-SM2-SM4-SM3 is used for information protection, the ECDHE generates the key selection materials, SM2 completes the digital signature and encryption key, and SM4 is used for the communication channel. The above data encryption process, SM3 is used for data integrity verification, through the above-mentioned colaborative work, it can complete the verification of the identity of the communicating parties, the key generation and exchange during the session, and the verification of whether the exchanged data is completely lost during the transmission process, thereby Perfectly guarantee confidentiality and integrity. During the communication process, the client first confirms the server-side certificate and prints out its information, and then starts the session communication. After completing the two-way data exchange, it releases resources and ends the SSL communication process.

Use wireshark software to capture data packets in the above-mentioned dual-terminal analog communication process, and the packet capture results are shown in Figure 11. The generated random number is 32 bytes in total. The 28 bytes that are actually generated by the random number generator algorithm and the random number of random numbers needed in the subsequent signing process to enhance the key generation and the subsequent signing process are mixed by adding the universal coordinated time as a parameter. It is through this method of introducing timestamps that it can effectively resist collision attacks.

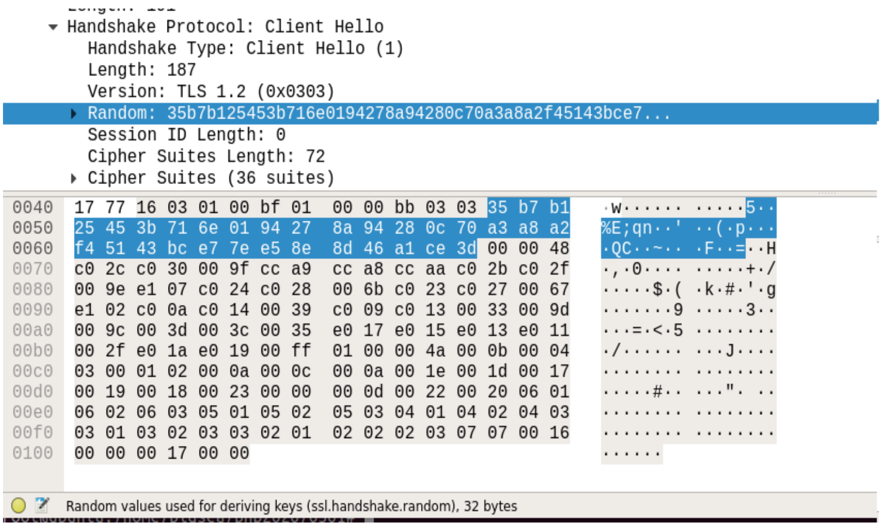
The entire communication interaction process is shown in Figure 12. First, the client sends an inquiry, and then the server responds and performs the corresponding key exchange. After the server responds, the client starts to prepare for key generation. After these communication sessions, the secure communication channel The establishment is successful, and then the communication data between the two ends are protected by security.

The time-consuming results of using the SM2-SM4-SM3 hybrid cryptographic system compared with other schemes are shown in Figure 13. It can be seen that the scheme in this paper is less time-consuming than the previous two, and the respective algorithms themselves are more secure, which proves the scheme Feasible and suitable for further related research. Since the transmission of power



```
-----Session establishment process-----
socket created
address created
server connected
Connected with ECDHE-SM2-WITH-SMS4-GCM-SM3 encryption
---Digital certificate information:---
Certificate content: /C=CH/ST=shanghai/L=pudongxinqu/O=suep/OU=smartgrid/CN=jisu
anjixueyaun/emailAddress=15279265616@163.com
Issuer: /C=CH/ST=shanghai/L=pudongxinqu/O=suep/OU=smartgrid/CN=jisuanjixueyaun/e
mailAddress=15279265616@163.com
---Start session communication transmission---
The client successfully received the server message:'server->client' , total 14 b
ytes
The client sends a message'U2FsdGVkX1+yk8CNQXfXElPz6vlgTX0XRRdMX9Zja3jpTyYZzZxKn
iE6uO+i8bP37p7kFqBB2VfyE9IIxCekDtcoiD2kAaK2Br8CzXQphc5hAqm8BEPwgZIgSTYCFUK/1I2z0
MvPMSfc+Q2v1IPTnz7H8iHpkCFp2VW4k9V8Mz0dJ/Dcdb/kmyjk5CoVMYmXUxPwv8CupI/H91mofOjK8
y1tCClEyMUYRLMRsTmyOvlUE2owpAbWPAxeN8ou5M6ORx7gtectv9P6tubTXsBPPjR8isQIaIa/QmV4N
wHqBtbs0tKITxTRz7jiVLO3IQcxjjUsj9sNhl/VRJ3ynHMgpOks1ni/RwIBr1Nf4D/DIbl2V3o0oa/Bh
TRd0H9+oRIT5DpImwlIcFEwZc9VojUj0/WvJ7Tn7nuwYUyCuOxDuCzlEi/8oWpmpz2gB3PVTP3T9pi0m
HZgDsnAaHv8zAgr8sQoTy0Y4ZojU3KsxQ1I/qdNp2+XyE6UQJ4gMt/rQLyvnW5I/nPOnLZ6z2EikVNWT
Q=='send successed
, total send 536 bytes！
---End SSL secure communication----
```

Figure 10. Client communication interface.

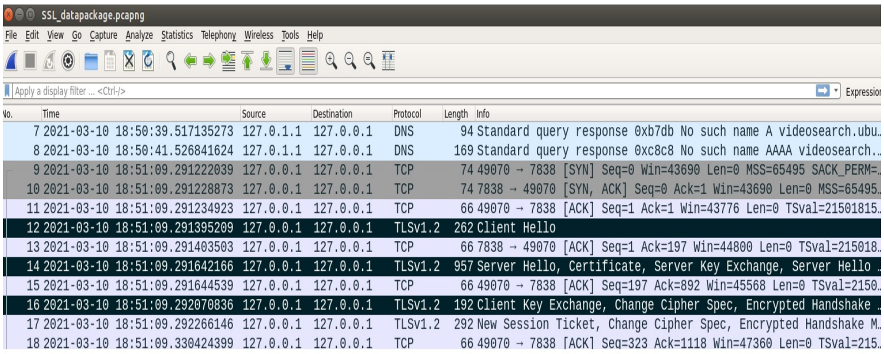


```
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 187
      Version: TLS 1.2 (0x0303)
    ▸ Random: 35b7b125453b716e0194278a94280c70a3a8a2f45143bce7...
      Session ID Length: 0
      Cipher Suites Length: 72
    ▸ Cipher Suites (36 suites)

0040  17 77 16 03 01 00 bf 01  00 00 bb 03 03 35 b7 b1   ·w······ ·····5··
0050  25 45 3b 71 6e 01 94 27  8a 94 28 0c 70 a3 a8 a2   %E;qn··' ··(·p···
0060  f4 51 43 bc e7 7e e5 8e  8d 46 a1 ce 3d 00 00 48   ·QC··~·· ·F··=··H
0070  c0 2c c0 30 00 9f cc a9  cc a8 cc aa c0 2b c0 2f   ·,·0···· ·····+·/
0080  00 9e e1 07 c0 24 c0 28  00 6b c0 23 c0 27 00 67   ·····$·( ·k·#·'·g
0090  e1 02 c0 0a c0 14 00 39  c0 09 c0 13 00 33 00 9d   ·······9 ·····3··
00a0  00 9c 00 3d 00 3c 00 35  e0 17 e0 15 e0 13 e0 11   ···=·<·5 ········
00b0  00 2f e0 1a e0 19 00 ff  01 00 00 4a 00 0b 00 04   ·/······ ···J····
00c0  03 00 01 02 00 0a 00 0c  00 0a 00 1e 00 1d 00 17   ········ ········
00d0  00 19 00 18 00 23 00 00  00 0d 00 22 00 20 06 01   ·····#·· ···"· ··
00e0  06 02 06 03 05 01 05 02  05 03 04 01 04 02 04 03   ········ ········
00f0  03 01 03 02 03 03 02 01  02 02 02 03 07 07 00 16   ········ ········
0100  00 00 00 17 00 00                                  ······

Random values used for deriving keys (ssl.handshake.random), 32 bytes
```

Figure 11. Random number for security guarantee.



SSL_datapackage.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression

```
No.  Time                          Source     Destination Protocol Length Info
   7 2021-03-10 18:50:39.517135273 127.0.1.1  127.0.0.1   DNS        94 Standard query response 0xb7db No such name A videosearch.ubu…
   8 2021-03-10 18:50:41.526841624 127.0.1.1  127.0.0.1   DNS       169 Standard query response 0xc8c8 No such name AAAA videosearch…
   9 2021-03-10 18:51:09.291222039 127.0.0.1  127.0.0.1   TCP        74 49070 → 7838 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=…
  10 2021-03-10 18:51:09.291228873 127.0.0.1  127.0.0.1   TCP        74 7838 → 49070 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495…
  11 2021-03-10 18:51:09.291234923 127.0.0.1  127.0.0.1   TCP        66 49070 → 7838 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=21501815…
  12 2021-03-10 18:51:09.291395209 127.0.0.1  127.0.0.1   TLSv1.2   262 Client Hello
  13 2021-03-10 18:51:09.291403503 127.0.0.1  127.0.0.1   TCP        66 7838 → 49070 [ACK] Seq=1 Ack=197 Win=44800 Len=0 TSval=215018…
  14 2021-03-10 18:51:09.291642166 127.0.0.1  127.0.0.1   TLSv1.2   957 Server Hello, Certificate, Server Key Exchange, Server Hello …
  15 2021-03-10 18:51:09.291644539 127.0.0.1  127.0.0.1   TCP        66 49070 → 7838 [ACK] Seq=197 Ack=892 Win=45568 Len=0 TSval=2150…
  16 2021-03-10 18:51:09.292070836 127.0.0.1  127.0.0.1   TLSv1.2   192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake …
  17 2021-03-10 18:51:09.292266146 127.0.0.1  127.0.0.1   TLSv1.2   292 New Session Ticket, Change Cipher Spec, Encrypted Handshake M…
  18 2021-03-10 18:51:09.330424399 127.0.0.1  127.0.0.1   TCP        66 49070 → 7838 [ACK] Seq=323 Ack=1118 Win=47360 Len=0 TSval=215…
```

Figure 12. Communication security interaction process.

information data requires high real-time performance, comparing the protection scheme designed in this paper with the traditional scheme can improve the transmission delay to a certain extent. At the same time, it can provide multiple security protections such as authentication to judge whether the two parties are

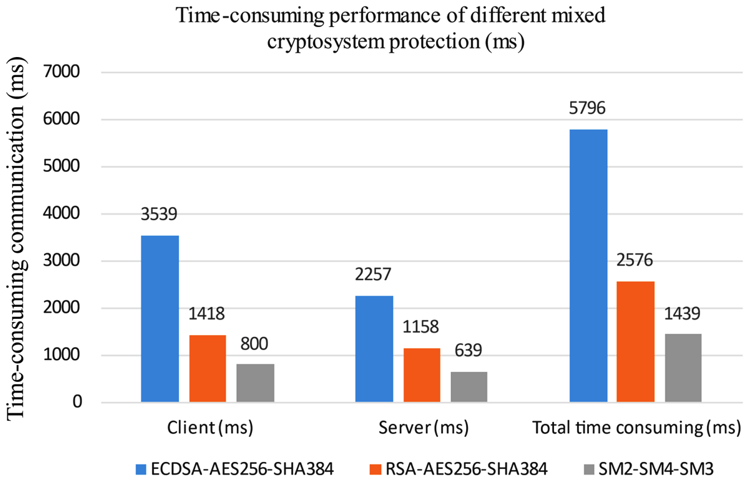


Figure 13. Different protection system solutions are time-consuming.

authentic, to ensure the confidentiality of communication data, whether the integrity of the exchanged information is lost, and the non-repudiation of the sender itself, which is more practical and valuable than a single encryption protection. It's safe and reliable.

5. Conclusion

This article mainly introduces the experimental process of the secure communication protocol, and uses the national secret algorithm to carry out the two-way communication process of the protocol, from which it can be seen that the data sent from the client to the server can be safely transmitted, ensuring the confidentiality of the data during the transmission process. The experiment shows that the protocol is safe and effective. The secure communication protocol proposed in this paper is a comprehensive utilization of multiple algorithms. Each type of algorithm application has its specific application occasions. The use of a certain technique alone cannot ensure the absolute security of the current application. In addition, the algorithm itself is mathematically safe. It does not mean that the physical equipment that actually uses the algorithm is safe. Therefore, in the next research work, we should strengthen the attack experiment on the physical equipment that actually uses the cryptographic algorithm to improve performance, so as to find a more secure program.

Fund

National Natural Science Foundation of China (61772327); Shanghai Natural Science Foundation (20ZR1455900); Development fund of National Engineering Laboratory for big data collaborative security (qax-201803).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zhang, Y.X. (2019) Design and Application of Electrical Energy Information Acquisition Software. Dalian University of Technology, Dalian.

[2] Yin, W. (2019) Design and Implementation of Power User Information Collection and Abnormal Data Analysis System. University of Electronic Science and Technology of China, Chengdu.

[3] Zhu, E.G. and Dou, J. (2015) Two-Way Interactive Function Design and Key Technology of Electricity Consumption Information Acquisition System. *Automation of Electric Power Systems*, **39**, 62-67.

[4] Liu, X., Zheng, A.G. and Zhang, L.Q. (2016) Research on the Development Trend of Data Transmission Protocol for Electricity Consumption Information Collection System. *Communication Technology*, **49**, 1057-1061.

[5] Su, Y.X. and Tian, H.B. (2020) The Mutual Signature Agreement Based on SM2 and Its Application. *Chinese Journal of Computers*, **43**, 701-710.

[6] Luo, Z., Yan, T., Xie, J.H., Zhu, J.P., Hua, W. and Wu, X.Q. (2016) Application of SM2 Encryption System in Smart Substation Telecontrol Communication. *Automation of Electric Power Systems*, **40**, 127-133.

[7] Dong, W.W., Wang, Y., Cao, K.H. and Zhou, L. (2020) A Safe Data Collection and Transmission Method for Electric Meters Based on RAHRM. *Journal of Shanghai Electric Power University*, **36**, 336-340.

[8] Chen, Y.L., Zhang, J.L., Ma, Y.H. and Feng, Y.Q. (2018) Research on Active Distribution Network Security Communication Protocol Based on National Secret Algorithm. *Electric Power Information and Communication Technology*, **16**, 14-21.

[9] Zuo, G., Fang, J.G., Xiang, C., Yu, W. and Shi, W.J. (2016) Design of Information Security Encryption Module in Distribution Automation Terminal Equipment. *Automation of Electric Power Systems*, **40**, 134-138.

[10] Yang, H.Z., Yuan, L.Y. and Wang, S. (2021) Blockchain Design Based on SM2 National Secret Algorithm Optimization. *Computer Engineering and Design*, **42**, 622-627.

[11] Hou, H.X., Yang, B., Zhang, L.N. and Zhang, M.R. (2020) Secure Two-Party Collaboration SM2 Signature Algorithm. *Chinese Journal of Electronics*, **48**, 1-8.

[12] Wu, D., Xu, T.G., Wang, Z.Y. and Liu, J.W. (2019) Hardware Design and Implementation of SM3 Algorithm with Integrated Message Filling. *Journal of Wuhan University* (*Science Edition*), **65**, 218-222.

[13] Fang, H.P., Ying, L.Y., Su, P.R., Huang, H.F. and He, L. (2015) Security Analysis of SSL Implementation of Mobile Smart Terminals. *Computer Applications and Software*, **32**, 272-276.

[14] Yang, H.T., Ru, Y.F., Sheng, L.J., Yang, J. and Zhang, Z.X. (2012) Implementation of Remote Encryption Test Software for Distribution Network Terminals Based on OpenSSL. *Automation of Electric Power Systems*, **36**, 77-81.

[15] Liu, N. and Lu, K. (2017) Cooperative Scheduling Method of Control and Communication in Real-Time Ethernet System. *Computer Engineering and Applications*, **53**, 15-20.