INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2021.15.135 Volume 15, 2021

Network communication data encryption method based on wireless channel characteristics

Jingxiang Zhong*
Network and Information Administration, China West Normal University,
Nanchong, 637009
China

Received: February 4, 2021. Revised: August 8, 2021. Accepted: August 28, 2021. Published: August 31, 2021.

Abstract—In order to improve the secure transmission capability of wireless transmission network communication data, a network communication data encryption design is required. An encryption and secure transmission method of wireless transmission network communication data based on wireless channel feature detection is proposed. The ECC (Elliptic Curves Cryptography) algorithm analyzes by monitoring single-channel and multi-channel samples separately. The ciphertext protocol for data secure transmission is constructed, the Hash dynamic transmission protocol is used for data access control, the data dynamic symmetric key, the key construction and arithmetic coding design are constructed. Combined with the ellipse linear mapping method, the data is encrypted safely. According to the intensity of the wireless channel feature distribution, the scrambling degree is rearranged for the random scrambling and encryption of the data, and the random linear coding method is used to realize the random scrambling and encryption of the data, so as to realize the secure transmission of network communication data and the secure storage of information. The simulation test results show that using this method to encrypt and transmit wireless transmission network communication data has better security and stronger anti-attack ability, thereby improving the secure transmission performance of network communication data.

Keywords—Characteristics, data, encryption, network communication, wireless channel.

I. Introduction

With the development of network information transmission technology, a large amount of network communication data and data need to be transmitted over the network. The security of network communication data transmission has received great attention. During the transmission process of wireless transmission network communication data, the wireless transmission network communication data is easy to leak due to plaintext invasion [1]. Therefore, it is necessary to design a secure transmission of wireless transmission network communication data and construct a secure transmission protocol model for wireless transmission network communication data. The encryption method is adopted for the encryption design of the wireless transmission network communication data, and a key protocol for the encryption of the wireless transmission network communication data is constructed. Combined with arithmetic coding and encryption key construction method, the secure transmission of the wireless transmission network communication data is realized [2]. The research on the encrypted secure transmission method of the wireless transmission network communication data is of great significance in ensuring the output security of the wireless transmission network communication data [3].

The design of secure transmission of wireless transmission network communication data is based on the encryption design of wireless transmission network communication data [4]. The data encryption methods mainly include elliptic encryption method, curve encryption method and linear encryption method. The design of secure transmission of wireless transmission network communication data is carried out by constructing wireless transmission and combining random coding design method. In the traditional method, literature [5] improves the quality index of big data processing engineering under the manifold coordinate system, including high-performance coding design, transmission speed and reliability. The system consists of a limited number of basis vectors. The modulus and set of vectors including themselves form a t-dimensional torus coordinate grid on the torus, the basis of which is a subset of the general number of the grid coordinate set. These design techniques make it possible to configure high-performance information technology for big data coding design and vector signal processing. The basic mathematical principles involve

optimizing the position of structural elements in a space or time distribution system through appropriate algebraic construction based on the cyclic group in the Galois field extension, and the development of the scientific basis for the best solution to a broad category of technical problems. Data processing engineering and computer science. Literature [6] uses the robustness and flexibility of the TLS protocol to be reflected in the characteristics of the existing encryption keys in its list, "cipher suite" for network communication encryption. The traditional method transmits the security key of network communication data encryption. The arithmetic coding design scheme is adopted to carry out the adaptive feature classification and vector quantization coding design of wireless transmission network communication data storage information.

Due to the simple combination structure of wireless transmission network communication data and the self-organization in network space, the security encryption performance of wireless transmission network communication data is not good, and the optimized encryption key design of wireless transmission network communication data is required [6]. Therefore, this paper proposes a wireless transmission network communication data encryption security transmission method based on wireless channel feature detection. A ciphertext protocol for safe transmission of wireless transmission network communication data is constructed, Hash dynamic transmission protocol is adopted for access control of wireless transmission network communication data, dynamic symmetric keys of wireless transmission network communication data are constructed, key construction and arithmetic coding design in a safe encryption process of wireless transmission network communication data are carried out by combining an elliptic linear mapping method. According to the intensity of the wireless channel characteristic distribution, the scrambling degree rearrangement of the random scrambling encryption of the wireless transmission network communication data is carried out, the random scrambling encryption of the wireless transmission network communication data is realized by adopting the random linear coding method, the safe transmission of the network communication data and the safe storage of information are realized, and finally the simulation experiment analysis is carried out, which shows the superior performance of the method in improving the safe encryption transmission of the wireless transmission network communication data.

II. Wireless Channel Characteristic Analysis

A. Wireless Channel

Channel is the general term of the media between the transmitter and the receiver. It is an indispensable part of any communication system. According to the classification of propagation medium, channel can be divided into two categories: Wired channel and wireless channel, in which wireless channel is the path of information transmission through the propagation of electromagnetic wave in space.

(a) Propagation characteristics of wireless channel

In the transmission process from the transmitting antenna to the receiving antenna, the signal will experience a variety of complex propagation paths, including direct path, reflection path, diffraction path, scattering path and random combination of these paths. When wireless signal propagates, it not only has the inherent transmission loss in free space, but also suffers from the signal power attenuation caused by the block of buildings, terrain, etc. this attenuation will also change randomly due to the movement of mobile station and the change of channel environment. The propagation path between the transmitter and the receiver is very complex, from the simple line of sight propagation to the reflection, diffraction and scattering caused by various complex terrain can form the propagation path.

Therefore, the propagation mechanism of electromagnetic wave is various. The propagation model of electromagnetic wave in free space is the most basic model to analyze the characteristics of wireless channel. It is mostly used to predict the field strength of the signal between the receiver and the transmitter when there is no barrier between them.

(b) Sample listening in single channel and multi-channel respectively

(1) The existing single channel sample listening technology is analyzed. It is found that the existing single channel sample listening technology uses the channel probe of the network layer. First of all, using the channel probe in the network layer will lead to the confirmation mechanism and packet loss retransmission mechanism in the link layer, which will make the interaction of channel characteristic samples very complex, and the pairing algorithm is difficult to design, resulting in the problem of inaccurate pairing of samples. Secondly, using the channel probe in the network layer will increase the processing time of the protocol stack.

(2) The existing multi-channel sample listening technology is analyzed, and it is found that the existing multi-channel sample listening technology does not achieve effective channel feature sample pairing.

B. Elliptic Curve Encryption Algorithm Analysis

First of all, we need to define the elliptic curve involved in the operation. Method representation of curve:

All points on the curve are nonsingular, which is a prior condition. In order to meet the universality, the shape of the curve is not only an ellipse, but also can contain some special curve forms. The specific method is shown in Fig. 1.

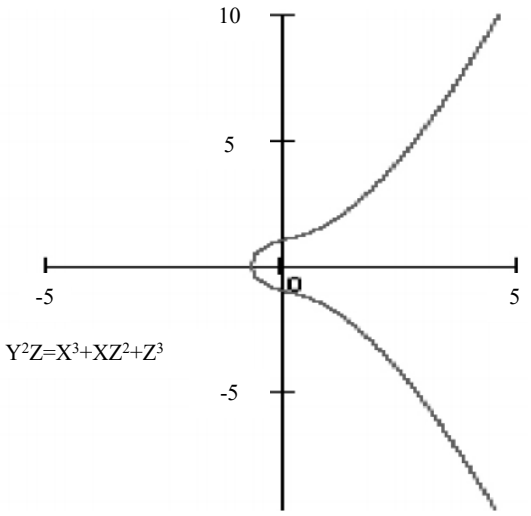


Fig. 1 elliptic curves 1

Nonsingularity needs to be constrained by mathematical methods. The result of partial derivative in three directions cannot be equal to zero at the same time, which can effectively ensure that all points on the curve are nonsingularity. Of course, there are some special forms, that is to say, the method of satisfying the curve does not necessarily represent the ellipse, as shown in Fig. 2.

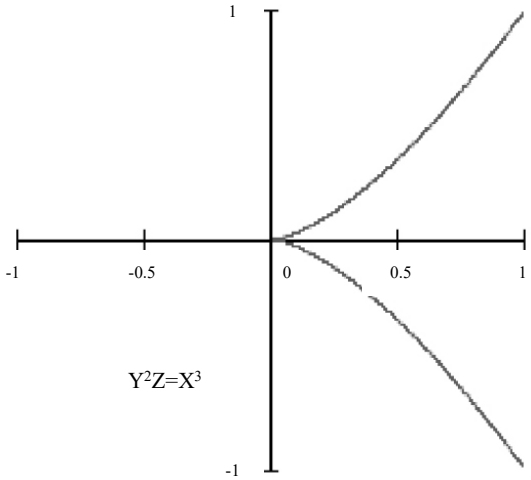


Fig. 2 non-elliptic curves 1

The process of network intrusion detection using elliptic curve is shown in Fig. 3.

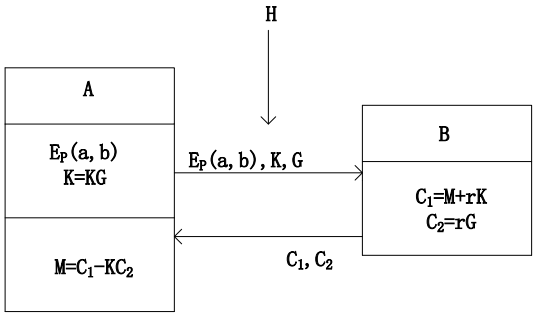


Fig. 3 elliptic curve coded communication process schematic drawing

If there is a H, he can only see EP (a, b), K, G, C1, C2, but it is relatively difficult to find K through K, g or R through C2, G. Therefore, H cannot get the plaintext information transmitted between A and B. If you want to correctly describe a n encrypted ellipse, you need multiple variables, set to t = (P, a, B, G, N, H). (P, a and B are used to determine a n elliptic curve. G is the base point, n is the order of point G, and H is the integral part of dividing the number of points m and N on the elliptic curve.). This is the reasonable selection of parameters is very important to the effect of encryption.

C. Ciphertext Protocol for Secure Transmission of Network Communication Data

There are many ways to classify cryptography, which can be divided into symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography is also called traditional cryptography, and asymmetric key cryptography is also called public key cryptography. Traditional passwords can be subdivided into sequence ciphers and block ciphers.

Symmetric encryption. Its typical feature is that encryption and decryption use the same key. For symmetric key cryptography, encryption and decryption operations are exactly the same. Therefore, the symmetric encryption algorithm used will be simple and efficient, because the key is very short, it is quite difficult to decipher, because the security of the system mainly depends on the security level of the key, so the main problem at present is how to ensure the security of information transmission and how to keep the key on the public computer network. Because both the receiver and the sender use the same key in symmetric cryptography, it is difficult to achieve all data signature and nonrepudiation. Because encryption and decryption are very fast, symmetric encryption is now widely spread. The des method used by the US government before is one of the symmetric encryption methods.

Asymmetric encryption. The difference between asymmetric encryption and symmetric encryption is that the key used in the process of decryption and encryption is totally different. Generally, asymmetric encryption has two sets of keys - “public key” and “private key”. They are paired during encryption. “Public key” is usually public, and “private key” must not be public. The biggest advantage of this method is that in the process of decryption, the receiver only needs to open the “private key”, and the data is well protected. “Public key” is more flexible than “private key”, which is an advantage, while

the disadvantage is that the encryption and decryption speed is much slower than "private key".

In order to realize the safe transmission of the communication data of the wireless transmission network, firstly, a ciphertext protocol for the safe transmission of the communication data of the wireless transmission network is constructed, the access control of the communication data of the wireless transmission network is carried out by adopting the Hash dynamic transmission protocol [7]-[9]:

The elements in the hash table are determined by the hash function. The key K of the data element is taken as an independent variable, and the calculated value is the storage address of the element through a certain functional relationship (called hash function). Expressed as:

Addr = H (key)

There are two main problems to be solved before establishing a hash table:

(1) construct a proper hash function

The value of uniformity H (key) is evenly distributed in the hash table;

Simple to improve the speed of address calculation

(2) handling of conflicts

Conflict: In a hash table, different key values correspond to the same storage location. That is, the keyword K1 ≠ K2, but h (K1) = H (K2). A uniform hash function can reduce conflicts, but it cannot avoid them. After a conflict has occurred, it must be resolved; That is, it must look for the next available address.

Solution to conflict:

(1) Link method (zipper method). Records with the same hash address are stored in a linear linked list. For example, the key word (18, 14, 01, 68, 27, 55, 79) and the divisor (13) are set in the method of remainder. The hash address is (5, 1, 1, 3, 1, 3, 1, 1), and the hash hash is shown in the figure.

(2) Open location method. If h (k) has been occupied, probe in the following sequence: (H (k) + P (1))% tsize, (H (k) + P (2))% tsize , (h (k) + p (i))% tsize, …

Where H (k) is hash function, tsize is hash table length, and P (I) is probe function. On the basis of H (k) + P (i-1)) % tsize, if a conflict is found, incremental P (I) is used for new detection until no conflict occurs. According to the difference of exploration function p (I), open addressing method is divided into linear exploration method (P (I) = I: 1, 2, 3, ...). Second exploration method (P (I) = (- 1) ^ (i-1) * ((I + 1) / 2) ^ 2, the sequence of exploration is: 1, -1, 4, -4, 9, ...), random probe method (P (I): random number), double hash function method (double hash function H (key), HP (key) if h (key) conflicts, then use HP (key) to find the hash address. The detection sequence was: H (k), H (k) + Hp (k), h(k)+ i*hp(k)).

(3) Barrel location method. Bucket: a large enough storage space. Bucket address: associate a bucket for each address in the table. If the bucket is full, open addressing can be used. For example, insert A5, A2, A3, B5, A9, B2, B9, C2, and use linear exploration to resolve conflicts. Pictured here.

The safe ciphertext transfer function for the encryption of the communication data of the wireless transmission network is constructed in a limited domain as $Decrypt(sk,c^*)\boldsymbol{A}^{-1}=\boldsymbol{T}=(t_{i,j})_{i,j=1}^{m}$, the key construction is carried out based on a symmetric encryption algorithm, and the searchable encryption key for the safe transmission of the communication data of the wireless transmission network is obtained as follows:

$$Decrypt(sk,c^*)\boldsymbol{A}^{-1}\boldsymbol{A}=\begin{pmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{pmatrix}\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,m} \end{pmatrix} \quad (1)$$

In the formula, t represents the network node. An access control supporting method is adopted to carry out authorization encryption control on unencrypted data in wireless transmission network communication data, a structural analysis model of wireless transmission network communication data is constructed [10], and an agent re-encryption key protocol of wireless transmission network communication data $\boldsymbol{E}$ is obtained:

$$\begin{aligned} &Decrypt(sk,c^*)(\boldsymbol{A}^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^T}\boldsymbol{A}^{(\alpha_1,\cdots,\alpha_m)} \\ &=\begin{pmatrix} \alpha_1^{-1}t_{1,1} & \cdots & \alpha_1^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_m^{-1}t_{m,1} & \cdots & \alpha_m^{-1}t_{m,m} \end{pmatrix}\begin{pmatrix} \alpha_1 a_{1,1} & \cdots & \alpha_m a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_1 a_{m,1} & \cdots & \alpha_m a_{m,m} \end{pmatrix} \\ &=\boldsymbol{E} \end{aligned} \quad (2)$$

In the formula, α represents the network communication data. Considering the randomness of the parameters, the encryption key is reset to obtain a key length of n, the key expansion is carried out by using a re-encryption key protocol to obtain a key expansion sequence $X=x_1,x_2,...,x_n$, in the process of searching key ciphertext, the proxy re-encryption ciphertext of wireless transmission network communication data is obtained as $S_n=x_1+x_2+...+x_n$, ciphertext reorganization is carried out by using the own private key, and the output is as follows:

$$Decrypt(sk,c^*)\boldsymbol{A}\boldsymbol{A}^{-1}=\begin{pmatrix} t_{1,1} & \cdots & t_{1,m} \\ \vdots & \ddots & \vdots \\ t_{m,1} & \cdots & t_{m,m} \end{pmatrix}=\boldsymbol{E} \quad (3)$$

In the formula, t represents the encryption period. The key encryption algorithm is adopted to carry out random linear processing of wireless transmission network communication data, and the public key encryption explicit sequence for constructing wireless transmission network communication data is as follows:

$$\begin{aligned} &Decrypt(sk,c^*)\boldsymbol{A}^{(\alpha_1,\cdots,\alpha_m)}Decrypt(sk,c^*)(\boldsymbol{A}^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^T} \\ &=\begin{pmatrix} \alpha_1 a_{1,1} & \cdots & \alpha_m a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_1 a_{m,1} & \cdots & \alpha_m a_{m,m} \end{pmatrix}\begin{pmatrix} \alpha_1^{-1}t_{1,1} & \cdots & \alpha_1^{-1}t_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha_m^{-1}t_{m,1} & \cdots & \alpha_m^{-1}t_{m,m} \end{pmatrix} \\ &=\boldsymbol{E} \end{aligned} \quad (4)$$

Linear encryption is carried out on the designated key words to obtain the characteristic distribution value $e=h(m)$ of the ciphertext protocol, the key word ciphertext is adopted to return

to the user [11], and arithmetic coding design is carried out to obtain the quantization characteristic equation for safe transmission of communication data in the wireless transmission network as follows:

$$Decrypt(sk,c^*)(\boldsymbol{A}^{(\alpha_1,\cdots,\alpha_m)})^{-1}=\begin{pmatrix}\alpha_1^{-1}t_{1,1} & \cdots & \alpha_1^{-1}t_{1,m}\\ \vdots & \ddots & \vdots\\ \alpha_m^{-1}t_{m,1} & \cdots & \alpha_m^{-1}t_{m,m}\end{pmatrix}=(\boldsymbol{A}^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^T} \tag{5}$$

According to this, a ciphertext protocol for secure transmission of communication data in wireless transmission network is constructed. Combined with elliptic linear construction method, a ciphertext transmission structure model for encryption of communication data in wireless transmission network is obtained as shown in Fig. 4.

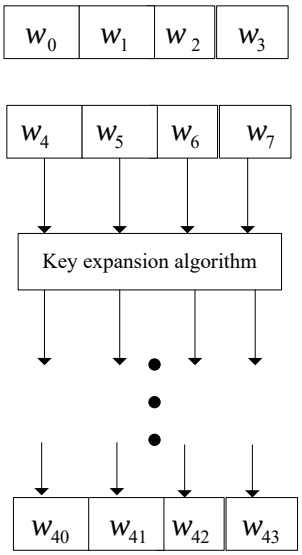


Fig. 4 ciphertext transmission structure model of wireless transmission network communication data encryption

D. Dynamic Symmetric Key Construction of Wireless Transmission Network Communication Data

The dynamic symmetric key of the communication data of the wireless transmission network is constructed, and the key construction and arithmetic coding design in the secure encryption process of the communication data of the wireless transmission network are carried out by combining the elliptic linear mapping method [12]. According to the indistinguishability of ciphertext, the hash function P-value of the encryption of the communication data of the wireless transmission network is obtained as follows:

$$\begin{aligned}P\text{-value}&=2\left[1-\varphi\left(S_{obs}\right)\right]\\&=2\left(1-\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{Sobs}e^{-u^2/2}du\right)\\&=\frac{2}{\sqrt{2\pi}}\int_{Sobs}^{+\infty}e^{-u^2/2}du\\&=\frac{2}{\sqrt{\pi}}\int_{\frac{Sobs}{\sqrt{2}}}^{+\infty}e^{-t^2}dt\\&=erfc\left(\frac{S_{obs}}{\sqrt{2}}\right)\end{aligned} \tag{6}$$

If the statistic $P-\text{value}\geq 0.01$ indicates that the public parameters of the public system satisfy $KS\in\{0,1\}$, it is expressed as a 1-bit coding map, and the data owner will first select a random value to obtain the linear coding characteristic distribution function of the wireless transmission network communication data:

$$f^{-1}(I)=\begin{cases}p*I, & s="0"\\ 1-(1-p)*I, & s="1"\end{cases} \tag{7}$$

wherein I represents the private key of the wireless transmission network communication data sender, sets the initial value $I=[0,1]$, divides the plaintext message into n blocks along with any sender, adopts a random scrambling encryption method, and obtains the public key encryption protocol as follows:

$$f(x)=\begin{cases}x/P_1, & x\in I_1\\ (x-P_1)/P_2, & x\in I_2\\ \quad\cdots\cdots & \quad\cdots\cdots\\ (x-\sum_{i=1}^{n-1}P_i)/P_n, & x\in I_n\end{cases} \tag{8}$$

wherein the ciphertext distribution probability interval $P_i(i=1,.....,n)$ of the wireless transmission network communication data is represented, an arithmetic coding model of the wireless transmission network communication data is constructed according to the number of public key components [13], and the key satisfies the following requirements:

$$\begin{cases}KC_1=KC_1\oplus\left\{t_j,t_{j+1},t_{j+2},.....,t_{j+m-2}\right\}\\ KS_1=KS_1\oplus\left\{t_{j+m-2}\right\}\end{cases} \tag{9}$$

wherein, $j=r \bmod 128$, the homomorphic encryption scheme is adopted to design the key for random scrambling encryption, and the inverse function is:

$$f^{-1}(x)=\begin{cases}P_1x\\ P_2x+P_1\\ \quad\cdots\cdots\\ P_nx+\sum_{i=1}^{n-1}P_i\end{cases} \tag{10}$$

Read the ciphertext sequence to realize the dynamic symmetric key construction of wireless transmission network communication data, as shown in Fig. 5.

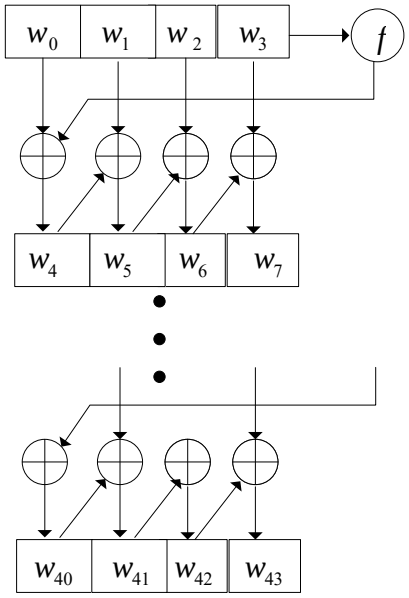


Fig. 5 dynamic symmetric key construction of wireless transmission network communication data

III. Optimization Of Encryption And Decryption Algorithm And Implementation Of Secure Transmission

A. Encryption and Decryption Algorithm

(1) Symmetric Encryption algorithm

Commonly used algorithms include: Des (Data Encryption Standard): Data Encryption Standard, faster, suitable for Encryption of a large number of Data occasions. 3DES (Triple DES): is based on DES, a piece of data with three different keys for three times encryption, higher strength. AES (Advanced Encryption Standard): Advanced Encryption Standard, the next-generation Encryption algorithm Standard, fast, high-level security;

a. Encryption and decryption using the same key.

b. Encryption and decryption of the faster speed, suitable for the use of long data.

c. The process of key transmission is not secure, and it is easy to be cracked, and the key management is more troublesome.

d. Encryption algorithms: Des (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard, Encryption with 128, 192, 256, 512 bit keys), Blowfish.

e. Encryption tools: OPENSSL, GPG PGP TOOLS.

(2) public-key cryptography

RSA, a public key Algorithm developed by RSA, is a public key Algorithm that supports variable-length keys. The length of the file block to be encrypted is also variable, is a standard DSS (digital signature standard); ECC (Elliptic Curves Cryptography): Elliptic Curve Cryptography. Compared with RSA, ECC has absolute advantage in many aspects, which is mainly reflected in the following aspects: strong attack resistance. With the same key length, it is many times more attack-resistant. The computation is small, the processing speed is fast. The total speed of ECC is much faster than RSA and DSA. Small memory footprint. ECC's key size and system parameters are much smaller than RSA and DSA, which means it occupies much less storage space. This is of great significance for the application of encryption algorithm on IC card. Low Bandwidth requirement. When encrypting and decrypting long messages, the three kinds of cryptosystems have the same bandwidth requirements, but ECC has much lower bandwidth requirements when applied to short messages. ECC has a wide application prospect in wireless network because of its low bandwidth requirement.

a. Each user has a pair of keys for encryption: Public and private.

b. Public key encryption, private key decryption; Private key encryption, public key decryption.

c. The process of public key transmission is insecure and prone to theft and substitution.

d. Because the public key uses a very long key length, the public key encryption speed is very slow, generally does not use its to encrypt.

e. One user encrypts with his private key, and other users decrypt with his public key to realize the function of digital signature.

f. Another use of public key cryptography is for key exchange.

g. Encryption and signature algorithm: Rsa, ELGamal.

h. Public key signature algorithm: DSA.

i. Encryption tools: GPG, openssl.

Table I. The next two are a comparison of the security and speed of RSA and ECC

Attack Time MIPS years	Rsa / DSA key length	ECC key length	Rsa /ECC key length ratio
104	512	106	5:1
108	768	132	6:1
1011	1024	160	7:1
1020	2048	210	10:1
1078	21000	600	35:1

Table II. Comparison of RSA and ECC security modulus

Function	Key pair generation	Sign it	Attestation
Security Builder 1.2	3.8	2.1 (ECNRA)	9.9 (ECNRA)
BSAFE 3.0		3.0 (ECDSA)	
163 ECC (ms)			10.7 (ECDSA)
A 1023 - bit RSA (ms)	4708.3		228.4

(3) One-way encryption (Hashing Algorithm)

Hashing is the extraction of information, usually its length is much smaller than the information, and for a fixed length. A highly encrypted hash must be irreversible, which means that no part of the original information can be derived from the hash result. Any change in the input information, even one bit, will cause a significant change in the hash result, which is called the avalanche effect. Hashes should also be conflict-resistant, in that no two pieces of information with the same hash result can

be found. Hash results with these characteristics can be used to verify that the information has been modified.

One-way Hash function is generally used to produce a Message Digest, key encryption, such as:

1) MD5 (Message Digest Algorithm 5): Rsa Data Security Company developed a one-way Hash Algorithm, non-reversible, the same text to produce the same ciphertext.

2) SHA (Secure Hash Algorithm): Generates a 160-bit value for data operations of any length;

SHA-1 is similar to MD5 because both are derived from MD4. Accordingly, their strengths and other characteristics are similar, but with the following differences: 1) Security against coercion: The most significant and important difference is that the SHA-1 digest is 32 bits longer than the MD5 digest. Using the brute force technique, the difficulty of producing any message with a digest equal to a given digest is an order of magnitude 2128 for MD5 and 2160 for SHA-1. As a result, SHA-1 is more effective against force attacks. 2) Security for cryptanalysis: Due to the MD5 design, vulnerable to cryptanalysis attacks, SHA-1 appears to be vulnerable to such attacks. 3) Speed: SHA-1 runs slower than MD5 on the same hardware.

Features: Avalanche effect, fixed length output, and irreversibility.

The idea is to ensure the integrity of the data.

ENCRYPTION ALGORITHMS: MD5 (standard key length 128 bits), SHA1(standard key length 160 bits), MD4, CRC-32.

Encryption tools: md5sum, Sha1sum, OPENSSL DGST.

Calculate a hash value for a file, such as md5sum / Shalsum FileName, openssl dgst something MD5 /-sha1.

On the basis of the above-mentioned ciphertext protocol for the secure transmission of communication data in wireless transmission network, dynamic symmetric key design and encryption algorithm optimization is carried out [14]. In this paper, a secure transmission method for encryption of communication data in wireless transmission network based on wireless channel feature detection is proposed. The average mutual information function of key construction and arithmetic coding design encryption in the secure encryption process of communication data in wireless transmission network combined with elliptic linear mapping method is as follows:

$$H = -\sum_{i=1}^{n} P_i \log_2(P_i) \tag{11}$$

For the coded extension sequence $s = \{s_i, i = 1...M \mid s_i \in S\}$ of elliptic linear mapping, the information entropy of homomorphic encryption is calculated as:

$$P_n = \frac{1}{M} card\{s_i \mid s_i = S_n\} \tag{12}$$

The $S_n \in S, n = 1...N$ obtains an extended key $\boldsymbol{x} = (x_1, \cdots, x_m)^T \in \boldsymbol{GF}(2^n)^m$ for wireless transmission network communication data security by adopting a random permutation method, and obtains an encryption function for wireless transmission network communication data security transmission through key mapping as follows:

$$I^i = f^{-1}(x)(I^{i+1}) \tag{13}$$

$$size(I^i) = P_i size(I^{i+1}) \tag{14}$$

The coding protocol for constructing wireless transmission network communication data encryption in a limited domain is:

•**RkeyGen**($param, rsk_{ID_i}, ID_i, \mathrm{ID}_j$) . According to the dynamic symmetric encryption key protocol, the combined sequence $x_1 x_2 x_3 ..... x_r$ of wireless transmission network communication data obtains the public key of the nth encryption bit sequence. Setting a key $k_i, l_i \in Z_q^*$ for encrypting communication data of a wireless transmission network, and enabling the homomorphic public key rk_{ij} to obtain an arithmetic coding protocol for encrypting communication data of the wireless transmission network:

$$\begin{aligned}&(rk_{1ij}, rk_{2ij}, rk_{3ij}, rk_{4ij}, rk_{5ij}, rk_{6ij})\\ &= (g^{x_i k_i}, (g^{t_0} h)^{x_i k_i}, \frac{x_j}{x_i}, sr_i^{x_i^{-1}(t_0 - t_i)} sr_j^{x_i^{-1}(t_j - t_0)}, k, g^{k_i})\end{aligned} \tag{15}$$

wherein

$$k = e\left(g^{k_i}, g_1^{u_i(t_0 - t_i)} g_1^{u_j(t_j - t_0)}\right) \frac{e\left(g^{k_i}, sk_{i1} g_1^{l_i}\right)}{e\left(\left(g^{t_0} h\right)^{k_i}, g^{u_i}\right)} e(g, g_1)^{-k_i l_i} \tag{16}$$

Using integer polynomial closed-loop encryption method, the output encryption results are as follows:

$$\mathrm{C} \to \mathrm{S}: \mathrm{ClientHello}\{\mathrm{Ver_c}, \mathrm{CipherSuite_c}, R_c, \mathrm{SessionID}\}$$

$$\mathrm{S} \to \mathrm{C}: \mathrm{ServerHello}\{\mathrm{Ver_s}, \mathrm{CipherSuite_s}, R_s, \mathrm{SessionID}\}$$

The decryption algorithm is:

Decrypt $\left(sk, c^*, z\right)$: The ciphertext of the wireless transmission network communication data is q_0 . When $q_0 \leftarrow Z \cap \left[0, 2^\gamma / \pi\right)$ is satisfied, the dynamic symmetric key for the secure transmission of the wireless transmission network communication data is $\overrightarrow{m} = \left(m_{i,j}\right)$, and the output decryption key is $param = \{G_1, G_2, e, g, g_2, g_3, h, H_1, H_2\}$, thus realizing the encryption and decryption algorithm design for the secure transmission of the wireless transmission network communication data [15].

B. Implementation of Secure Transmission of Communication Data in Wireless Transmission Network

The linear bit sequence flow model for secure encryption of communication data in wireless transmission network is given as $s = \{s_i, i = 1...M \mid s_i \in S\}$, the sensitive characteristic coefficient is initialized [16], and the dynamic symmetric key for network communication data encryption is obtained as follows:

$$\mathrm{C} \to \mathrm{S}: \mathrm{Certificate}\left\{\mathrm{Cert_c}\right\}$$

$$\mathrm{C} \to \mathrm{S}: \mathrm{ClientKeyExchange}\left\{K_c\right\}$$

$$\mathrm{C} \to \mathrm{S}: \mathrm{CertificateVerify}\left\{\left\{\mathrm{hash}\left(\mathrm{messages}\right)\right\}_{P_c^{-1}}\right\}$$

Combined with homomorphic encryption scheme, the

optimal transmission control equation of network communication data is obtained as follows:

$$f(x)=\begin{cases} x/p, & x\in[0,p) \\ (1-x)/p, & x\in[p,1] \end{cases} \quad (17)$$

The key structure and adaptive coding in the process of safe transmission and encryption of wireless transmission network communication data are realized through the parameter p, the scrambling degree rearrangement of random scrambling encryption of wireless transmission network communication data is carried out according to the intensity of wireless channel characteristic distribution [17]-[19], and the random scrambling encryption of wireless transmission network communication data is realized by adopting a random linear coding method.

IV. Simulation Experiment And Result Analysis

In order to test the performance of this method in realizing secure encryption of communication data in wireless transmission network, simulation experiments are carried out. The experiments are designed by Matlab 7. The experimental environment configuration is specific as shown in Table III.

Table III. Experimental environment configuration

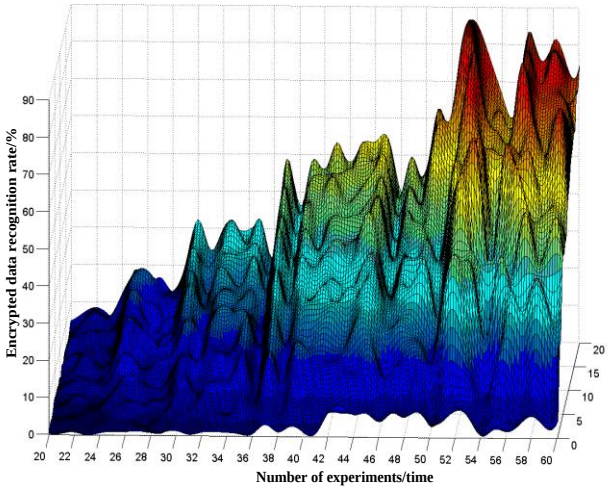
Serial number	Configuration	data
1	Computer hardware configuration	CPU: AMD Athlon (TM) II X4 640 Main frequency: 3. O1 GHz RAM: 3.25 GB
2	operating system	Microsoft Windows XP
3	Metadata editing and course content packaging	Reload Editor 2.5.5
4	Low-level software	Xampp1.7.7 Java
5	testing platform	Joomla 1.7.3
6	Use templates	schoolnerdfree-1. 0. 0
7	Use plug-ins	Google Analytics

The random coding sequence length of communication data in wireless transmission network is 1024, the length of plaintext bit sequence is 200, the intensity of wireless channel characteristic distribution is 20dB, and the initial encryption bit sequence is: 10100100100101100101010100. The encryption parameters of the wireless transmission network communication data are set as initialization parameters, and the wireless transmission network communication data encryption simulation is performed according to the parameter settings in Table IV.

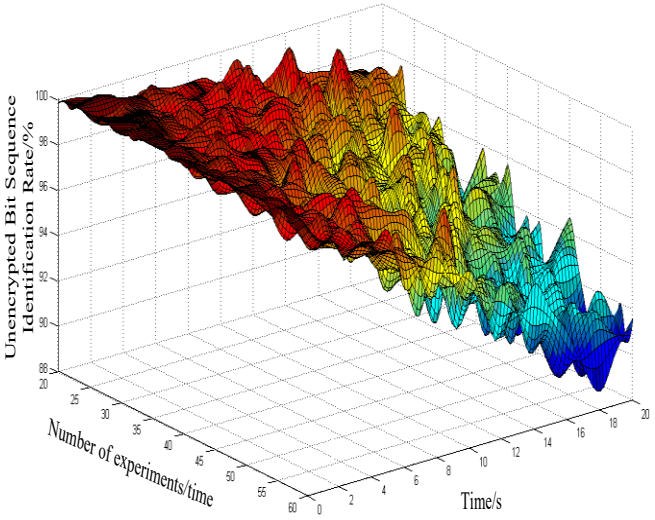
Table IV. Setting of experimental parameters

Parameter setting	t_{max}	M	l	p_m	p_c
Value	46	32	15	0.67	0.89

The dynamic symmetric key of the wireless transmission network communication data is constructed, and the random scrambling encryption of the wireless transmission network communication data is realized by adopting a random linear coding method, so that the encryption performance test result of the terminal network communication data is obtained as shown in Fig. 6.



(a) encrypted network communication data detection results



(b) test result of unencrypted network communication data

Fig. 6 encryption performance test

The test results show that the encryption and secure transmission of wireless transmission network communication data by the method in this paper has better performance and stronger anti-attack capability, thus improving the secure transmission performance of network communication data.

V. Conclusion

In this paper, the encryption method is used to encrypt the communication data of the wireless transmission network, and a key protocol for encrypting the communication data of the wireless transmission network is constructed. Combined with arithmetic coding and encryption key construction method, the secure transmission of the communication data of the wireless

transmission network is realized. This paper proposes a secure transmission method for encrypting the communication data of the wireless transmission network based on wireless channel characteristic detection. A ciphertext protocol for safe transmission of wireless transmission network communication data is constructed. Hash dynamic transmission protocol is adopted for access control of wireless transmission network communication data, dynamic symmetric keys of wireless transmission network communication data are constructed, key construction and arithmetic coding design in a safe encryption process of wireless transmission network communication data are carried out by combining an elliptic linear mapping method. According to the intensity of the wireless channel characteristic distribution, the scrambling degree rearrangement of the wireless transmission network communication data random scrambling encryption is carried out, and the random scrambling encryption of the wireless transmission network communication data is realized by adopting a random linear coding method, thus realizing the safe transmission of the network communication data and the safe storage of information. Research shows that the method in this paper has better anti-attack performance in encrypting network communication data for wireless transmission and improves the security of network communication data transmission. This method has good application value in network communication data security encryption. However, the method in this paper does not consider the time issue in the process of network communication data encryption. The calculation time is relatively long, resulting in low network communication data encryption efficiency. Therefore, the next research will focus on the network communication data encryption time problem. Designed to improve encryption efficiency.

References

[1] Y. C. Zhou, "Application of data encryption technology in computer network communication security," Communication Power Technology, vol. 36, no. 8, pp. 200-201, 2019.

[2] L. Barolli, F. Xhafa, and J. Conesa, "[Lecture notes on data engineering and communications technologies] advances on broad-band wireless computing, communication and applications Volume 12," A Light Weight Data Encryption Method for WSN Communication, (Chapter 70), pp. 788-795, 2018.

[3] L. Guo, H. Xie, and Y. Li, "Data encryption based blockchain and privacy preserving mechanisms towards big data," Journal of Visual Communication and Image Representation, vol. 70, no. 8, pp. 102741, 2019.

[4] K. L. Tsai, F. Y. Leu, I. You, and S. W. Chang, "Low-power AES data encryption architecture for a LoRaWAN," IEEE Access, vol. 7, pp. 146348-146357, 2019.

[5] V. Riznyk, "Big data process engineering under manifold coordinate systems," WSEAS Transactions on Information Science and Applications, vol. 18, pp. 7-11, 2021.

[6] H. Touil, N. E. Akkad, and K. Satori, "Secure and guarantee QoS in a video sequence: a new approach based on TLS protocol to secure data and RTP to ensure real-time exchanges," International Journal of Safety and Security Engineering, vol. 11, no. 1, pp. 59-68, 2021.

[7] A. Fan, Q. Wang, and J. Debnath, "A high precision data encryption algorithm in wireless network mobile communication," Discrete & Continuous Dynamical Systems, vol. 12, no. 4&5, pp. 1327-1340, 2019.

[8] H. Y. Zhang, "Application of data encryption technology in computer network communication security," Digital Technology and Application, vol. 36, no. 12, pp. 168-169, 2018.

[9] W. Cai and H. Yao, "A Secure transmission method of network communication data based on symmetric key encryption algorithm," Wireless Personal Communications, no. 4, pp. 1-12, 2021.

[10] L. Harn, C. F. Hsu, and Z. Xia, "Lightweight aggregated data encryption for wireless sensor networks (WSNs)," IEEE Sensors Letters, vol. 5, no. 4, pp. 1-4, 2021.

[11] Y. J. Kim, S. Y. Lee, and T. K. Park, "High-speed video data encryption on lte-based swarm UAS," International Review of Aerospace Engineering, vol. 11, no. 5, pp. 186-193, 2018.

[12] J. Zhang, H. Liu, and L. Ni, "A secure energy-saving communication and encrypted storage model based on RC4 for EHR," IEEE Access, vol. 8, pp. 38995-39012, 2020.

[13] K. L. Tsai, Y. L. Huang, F. Y. Leu, I. You, Y. L. Huang, and C. H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," IEEE Access, vol. 6, pp. 45325-45334, 2018.

[14] M. F. Hassan and M. Hammuda, "A new approach for constrained chaos synchronization with application to secure data communication," Journal of the Franklin Institute, vol. 356, no. 12, pp. 6697-6723, 2019.

[15] J. Sancho, J. García, A. Alesanco, and L. Maglaras, "Oblivious inspection: on the confrontation between system security and data privacy at domain boundaries," Security and Communication Networks, vol. 2020, pp. 1-9, 2020.

[16] J. A. P. Artiles, D. Chaves, and C. Pimentel, "Image encryption using block cipher and chaotic sequences - science direct," Signal Processing: Image Communication, vol. 79, no. 6, pp. 24-31, 2019.

[17] S. Rajagopalan, S. Rethinam, S. Arumugham, H. N. Upadhyay, J. B. B. Rayappan, and R. Amirtharajan, "Networked hardware assisted key image and chaotic attractors for secure RGB image communication," Multimedia Tools & Applications, vol. 77, no. 18, pp. 1-34, 2018.

[18] L. Yepdia, A. Tiedeu, and G. Kom, "A robust and fast image encryption scheme based on a mixing technique," Security and Communication Networks, no. 18, pp. 1-17, 2021.

[19] Q. Yan, W. Li, J. Li, and J. Zhang, "Real-time air-to-ground data communication technology of aeroengine health management system with adaptive rate in the whole airspace," Mathematical Problems in Engineering, no. 7, pp. 1-13, 2021.

Jingxiang Zhong, male, was born in February 1976. His title is lecturer. In 1999, he graduated from the Department of Physics, Sichuan Normal University with a bachelor's degree in electronic technology and computer applications, and a bachelor's degree in science. In 2013, he graduated from China West Normal University with a master's degree in computer application in education technology. Now he is working in Network and Information Administration, China West Normal University. His research field includes network communication; computer application; educational information technology. He has published many academic papers. At the same time, he led the research on four subjects.

Author Contributions:

According to the strength of the characteristic distribution of the wireless channel, Jingxiang Zhong rearranges the scrambling degree, randomly scrambling and encrypting the data, and using the random linear coding method to realize the random scrambling and encryption of the data, so as to realize the secure transmission of network communication data and the secure storage of information. The simulation test results show that using this method to encrypt and transmit wireless transmission network communication data has better security and stronger anti-attack ability, thereby improving the secure transmission performance of network communication data.