Information Encryption Algorithm in Power Network Communication Security Model

Chunyan Yang*, Ying Ling, Xin Li

Electric Power Research Institute of Guangxi Power Grid Co., Ltd, Guangxi Nanning, China, 530023

*Corresponding author e-mail: jyew775@126.com

Abstract. With the rapid development of communication technology in power networks, data communications are facing traditional network security risks. The information encryption algorithm is a key part of power network communication security. How to ensure the acquisition of confidential data is one of the key factors for the normal operation of the power grid system. The study of encryption algorithms is of great significance to the power grid communication security. This paper mainly researches the information encryption algorithm in the power grid communication security model. The experimental simulation results in this paper show that for the key pair generation time, the SM2 algorithm can generate a 256-bit key very quickly, which is 130 times faster than the RSA algorithm in generating a 1024-bit key, and the 2048-bit key in comparison 730 times faster. Therefore, under the same security level, the encryption and decryption efficiency of the SM2 algorithm is significantly higher than that of the RSA algorithm, and with the increase of the security strength, the superiority of the SM2 algorithm is more prominent.

Keywords: Power Network Communication, Information Encryption Algorithm, Network Security, Communication Technology

1. Introduction

With the continuous popularization of the Internet and the rapid development of information technology, computer networks and related industries have rapidly penetrated into all aspects of society and are gradually changing the way people produce and live. In recent years, there have been significant changes in the way people communicate. Emerging communication methods such as e-mail, Internet paging, and wireless communication are gradually becoming mainstream with their convenient and fast advantages. E-commerce, e-government, and electronic money are emerging. Things are based on the rapid development and popularity of communication networks, especially the
Internet. More and more materials and information are transmitted and processed by people through the Internet. Such information may contain important military, trade secrets, or personal privacy. Once leaked, it may cause serious consequences. How to protect the security of information is not only a matter of interest for military and government departments, but also for many other enterprises and institutions.

As network communication technology and the Internet become more and more closely connected, problems related to network security (host attacks, etc.) also continue to occur. Information sent on the network is intercepted and tampered with [1]. Retransmission will pose a huge threat to the further promotion of network applications. In this case, a secret code [2] is generated. Because the backup layer of the TCP/IP model has corresponding encryption protocols and technologies. This article focuses on data encryption at the session application layer [3-4]. Data encryption technology not only has the function of ensuring the confidentiality of information, but also has digital signatures, secret storage, and system security performance [5]. Therefore, the confidentiality, integrity, and verifiability of the information can be guaranteed, and the information has the possibility of being tampered with, forged, or forged [6]. Many encryption technologies have been applied in various fields. However, because of the shortcomings of encryption strength and large amount of calculation, this paper proposes a new encryption mechanism.

Electricity is a strategic energy source related to the lifeline of the national economy. The power industry is the basic industry of the national economy and an industry that serves the national economy and people's lives. It has a wide range of applications in computer and network technologies [7-8]. In particular, once information security problems occur, the rapid development of computer network and power grid automation will jeopardize the safe operation of the power grid and cause immeasurable losses and impacts [9]. The effective and stable operation of the power system is not only related to the interests of state-owned enterprises and institutions, but also to the important interests of millions of households. It is impossible to imagine how social production will occur without electricity and how people will live. Therefore, in-depth research on the characteristics of power system information security, and in the process of implementing the "digital power system", formulating measures to ensure power system information security are huge challenges facing the power industry [10-11]. With the rapid development of Internet, information security issues are facing new challenges. Information security issues in power systems are a new and important issue. The introduction of information security technologies in power system information communication is imminent. Economic, efficient and reliable encryption Technology to ensure the smooth flow of power system information transmission has great practical significance [12]. This article explores the frontier of new encryption ideas, and will likely provide practical and reliable security solutions for power system information communication.

2. Method

2.1 Key Technology Implementation of Algorithm Improvement Design

Binary code encryption technology is used to implement data encryption for smart grid information. The binary code encryption process of smart grid information is described as follows:

Let \( P(A\text{ttr}\text{Set}^{e+k}, q) \) be the complementary information attribute set \( q' \) of \( e + k \) grid safety.
information, and the self-information amount of the source code symbol \( s_i \) is 
\[ -\log_2(P(s_i)) \], then:

\[
P(q \rightarrow q') = \sum_{k=0}^{\min(\lambda-n[\eta+\frac{q}{\lambda}])} \sum_{i=1}^{\text{AttrSets}_{\lambda-k,q}} P(\text{AttrSets}_{\lambda-k,q,i}) = \sum_{k=0}^{\min(\lambda-n[\eta+\frac{q}{\lambda}])} \Pr_{k}^{\lambda,\eta}
\]

(1)

Through linear piecewise coding, when \( \lambda \) is increased by 1, the binary output of the information coding of the power grid network is as follows:

\[
\frac{\Pr_{k}^{\lambda+1,\eta}}{\Pr_{k}^{\lambda,\eta}} = \frac{\left(\frac{m-q}{\lambda+1-n-k}\right)\left(\frac{m}{\lambda+1}\right)}{\left(\frac{m-q}{\lambda-n-k}\right)\left(\frac{m}{\lambda}\right)} = \frac{(\lambda+1)(m-\lambda+1)}{\lambda+1-n-k(m-\lambda+1-q+\eta+k)}
\]

(2)

Among them, \( \frac{\Pr_{k}^{\lambda+1,\eta}}{\Pr_{k}^{\lambda,\eta}} \leq \lambda + 1 \) get any codeword \( \text{GF}(q) \) on the \([n, k]\) linear block code \( c = (c_{n-1}, c_{n-2}, \cdots, c_0) \), and \( \eta + k \leq \min(\lambda, q) \). When \( P(q \rightarrow q') \) increases and decreases with \( \lambda \), \( P(q' \rightarrow q) \), the encryption algorithm converges. The multi-variable statistical analysis and classified processing of encrypted smart grid information characteristics have improved the security guarantee function of power grid information. In order to ensure the information security of the smart grid, this article uses computer coding and information encryption technology.

2.2 Principles of Network Encryption Technology in Network Communication

In network communication, network communication security needs to ensure the consistency, confidentiality, and availability of network data sent through network communication. Network encryption technology provides confidentiality, security, and integrity of data information sent in network communications during network communications. In the transmission process of network communication, network communication has processed data encryption technology. The principle of network data encryption is actually the original format of network communication and the cipher text data format used for transmission or storage of the network. The format conversion can be cleared. To meet the needs of practical applications. In the process of network communication, there is a complementary relationship between encryption and decryption of data transmitted by network communication. The key encryption and decoding rules for network communication data information are the most important factors affecting the confidentiality of network communication data information keys in the process of network communication data information key encryption. Generally speaking, in the process of encrypting network communication data information, the calculation method of network communication encryption, in data network communication encryption and decoding processing, the keys of network communication data encryption and decoding are calculated by the same encryption rule, and the network development environment is open. Significantly
improved performance and compatibility. In the process of network communication transmission, or when network communication is decoded or intercepted, it is simple to affect the security of network communication.

2.3 Certification Technology

In the current power market technical support system, when users of power plants enter the system and access different information, they should implement different actions based on the identity of the users to limit their permissions. One method: When the client and the server are connected, the user is required to enter an account and password, and the server decides whether to establish a connection and manages user permissions. Information is divided into public information and private information. According to the user's account and password, the user can access his private information: according to his permission level, restrict viewing of other people's information. This method makes it inconvenient for the user to enter a password each time he views information. Another method: When a user accesses private data for the first time after opening a browser, the user must provide his or her account to the server. The web server generates a session ID for the user and provides his or her account to the server. The web server generates a session ID for the user and returns the session ID to the client. The session ID is unique and includes time, random values, and permissions. Before the user closes the browser or ends the session, the user uses the ID to access private data without having to frequently enter a member account, which is simple to operate and improves performance.

2.4 Reusing SNonce

The reuse SNonce method aims to eliminate the intermediate state existing on the applicant side, that is, before the applicant completes a successful four-step handshake process, it uses the first generated SNonce to calculate the PTK for different messages and forms the MIC of message 2. Message 2 is sent after verification, but the corresponding PTK is not stored. Instead, the PTK is recalculated for verification after receiving message 3. If the verification is successful, the PTK is loaded for data encryption of the session, otherwise it is terminated. The handshake process. That is, before the applicant receives and authenticates message 3, it repeatedly uses the same SNonce to respond to each received message 1. This improved method eliminates the need to cache each received ANonce and the corresponding generated PTK, which effectively avoids DoS attacks caused by exhausted memory resources.

3. Experiment

Because the encryption efficiency of asymmetric encryption algorithm and symmetric encryption algorithm are very different, and the asymmetric encryption algorithm can be used for signature and signature verification, the experiments are separated. The asymmetric encryption algorithm uses the commonly used national secret algorithms SM2 and RSA algorithms to test the encryption and decryption efficiency and signature verification efficiency, respectively. Symmetric algorithms are mainly divided into grouping algorithms and stream algorithms. The grouping algorithms are SM4, DES, AES, CAST, RC2, Blowfish, IDEA, and the typical stream algorithm is RC4. Due to the fragility of DES, the experiment uses a triple 3DES encryption algorithm, where the first key and the third key use the same key, and the second key uses a different key. The algorithm measures the time required to continuously encrypt the plaintext one million times, and then calculates the number of
times the algorithm encrypts per second, and the data is retained to the single digits. The above algorithm is implemented by calling the algorithm provided in Openssl. The Chinese secret asymmetric algorithm SM2 and the national secret symmetric algorithm SM4 are implemented by themselves and encapsulated in Openssl. The encryption and decryption efficiency of the above symmetric algorithm was tested and compared with subsequent experiments.

(1) In the same operating environment, the length of the plaintext is 128b, no mode is used, and experiments are performed using the symmetric algorithms SM4, AES, 3DES, CAST, RC2, RC4, Blowfish, and IDEA to compare the encryption and decoding efficiency of each algorithm. The experiments were performed by asymmetric algorithms SM2 and RSA, and the algorithm's encryption and decryption efficiency and signature verification efficiency were compared.

(2) Under the same operating environment, the length of the plaintext is 128B. The SM4, AES, and 3DES algorithms are selected to perform experiments in different modes of ECB, CBC, and CFB, and the effect of each encryption mode on the efficiency of the encryption algorithm is compared.

(3) Under the same operating environment, the plaintext length is 128B. The AES algorithm was selected to test the encryption and decryption efficiency of the algorithm under 128-bit, 192-bit, and 256-bit key lengths, and the effect of the key length on the algorithm's encryption and decryption efficiency was compared.

4. Discuss

4.1 Comparative Analysis of Encryption and Decryption Efficiency of Symmetric Algorithms

As shown in Table 1, the length of the plaintext is 128, and the length of the data packet is 16 bytes. Each algorithm is encrypted 1 million times and decoded 1 million times. The encryption and decoding efficiency of each algorithm has been improved. The algorithm AES has the highest encryption and decryption efficiency. The delays for one encryption and one decryption are 5.89 and 7.82, respectively. The second one is the algorithms CAST and RC4. The delay between encryption and decryption is 8 to 9, but the security is not as good as the AES algorithm. State secret algorithm SM4 continues. The delay of encryption and decryption is between 10 ~ 11, which has high security. Among them, the test environment of the SM1 algorithm is dual-core Pentiem (R) Dual-CoreCPUE5300@2.6GHz, and the memory is 2049768kb. The national secret algorithm SM1 has not been disclosed, only exists in the chip in the form of an IP core, has the highest security, and is widely used in important fields such as e-commerce, e-government, and online banking securities. Experiments show that the algorithm's encryption and decoding efficiency is much lower than the SM4 algorithm.

| Algorithm | Times per encryption(times/s) | Times per decryption(times/s) | Encryption delay(μs ) | Decryption delay(μs ) |
|-----------|------------------------------|------------------------------|-----------------------|----------------------|
| SM1       | 10794                        | 18214                        | 92.64                 | 54.90                |
| SM4       | 94786                        | 94696                        | 10.55                 | 10.56                |
### 4.2 Comparative Analysis of Encryption and Decryption Efficiency of Asymmetric Algorithms RSA and SM2 under Different Key Lengths

![Bar chart comparing encryption and decryption efficiency of asymmetric algorithms RSA and SM2 under different key lengths](image)

**Figure 1.** Encryption and decryption efficiency table of asymmetric algorithms RSA and SM2 under different key lengths

As shown in Figure 1, RSA signatures are very slow, signature verification is very fast, public key encryption is very fast, and private key decryption is very slow. The efficiency of SM2 decoding and signature is similar, but the 256-bit SM2 algorithm has a higher level of security than the 2048-bit RSA algorithm, the SM2 key length is short, the computation and encryption heads are fewer, the processing speed is faster, and storage space is used. Small advantage: In the generation time of the key pair, the SM2 algorithm quickly generates a 256-bit key. It is 130 times the RSA algorithm that generates 1024-bit keys and 730 times the RSA algorithm that generates 2048-bit keys. Therefore, at
the same level of security, the encryption and decoding efficiency of the SM2 algorithm is also significantly improved compared with the encryption efficiency of the RSA algorithm, and the security strength is continuously improved.

From the experimental results in this paper, we can find that the encryption and decoding speed of the asymmetric algorithm is slower than that of the symmetric algorithm. Therefore, asymmetric algorithms are often used to encrypt and decrypt small amounts of data, such as the encryption and decryption of symmetric keys in key protocols, or the signature and verification of ID verification. According to the experimental results of the experimental asymmetric encryption algorithm, the state secret SM2 algorithm has higher efficiency and security, and is more suitable for the signature verification and key agreement processes of power network communications.

5. Conclusion

With the innovation of information technology, various new technologies emerge endlessly, new applications bring new security issues, and the threats are constantly evolving. It can be seen that the construction of the power network information security system is a systematic project, not a simple one. A process that can be accomplished by establishing some systems, norms, or adopting some new technology. Therefore, the construction of the power network information security system should be coordinated with the development of enterprise business and informatization. At the same time, the information security system should be an open system with the ability of continuous improvement. Only by combining the characteristics of its own business and establishing a long-term mechanism of information security and information security protection, and truly eliminating hidden security threats, can the effective management of information security be achieved.

References

[1] Chen Liang, Qun Zhang, Jianfeng Ma. Research on neural network chaotic encryption algorithm in wireless network security communication[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 2019(1):151.

[2] Tareq Alhmiedat, Ghassan Samara. A Low Cost ZigBee Sensor Network Architecture for Indoor Air Quality Monitoring[J]. International Journal of Computer Science & Information Security, 2017, 15(1):140-144.

[3] Mona Shokair, Waleed Saad, Shady M. Ibraheem. Statistical analysis of a class of secure relay assisted cognitive radio networks[J]. China Communications, 2018, 15(12):174-189.

[4] Alberto Pittolo, Marco De Piante, Fabio Versolatto. In-Vehicle Power Line Communication: Differences and Similarities Among the In-Car and the In-Ship Scenarios[J]. IEEE Vehicular Technology Magazine, 2017, 11(2):43-51.

[5] YAN Ling-kun, HOU Yue-xing. The Optimization Strategies and Application of Transmission Network in Power System[J]. Electric Power Information & Communication Technology, 2017(7):107-112.

[6] Y. Li, W. Zhu, C. Huang. Research on power heterogeneous communications network stability
with SOC[J]. Power System Protection & Control, 2017, 45(5):118-122.

[7] Luis González-Sotres, Pablo Frias, Carlos Mateo. Power Line Communication Transfer Function Computation in Real Network Configurations for Performance Analysis Applications[J]. Iet Communications, 2017, 11(6):897-904.

[8] Junqi Duan, Deyun Gao, Dong Yang. An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications[J]. IEEE Internet of Things Journal, 2017, 1(1):58-69.

[9] Asma Mabrouk, Ahmed El Shafie, Kamel Tourki. AN-Aided Relay-Selection Scheme for Securing Untrusted RF-EH Relay Systems[J]. IEEE Transactions on Green Communications & Networking, 2017, 1(4):481-493.

[10] Ting Liu, Jue Tian, Yuhong Gui. SEDEA: State Estimation-Based Dynamic Encryption and Authentication in Smart Grid[J]. IEEE Access, 2017, 5(99):15682-15693.

[11] Fei Xiong, Aijing Li, Hai Wang. An SDN-MQTT Based Communication System for Battlefield UAV Swarms[J]. IEEE Communications Magazine, 2019, 57(8):41-47.

[12] T. Gomes, F. Salgado, Sandro Pinto. A 6LoWPAN Accelerator for Internet of Things Endpoint Devices[J]. IEEE Internet of Things Journal, 2017, 5(1):371-377.