Hybrid Encryption Scheme for Secure Storage of Smart Grid Data

Jie Deng[1] and Hai-Yan Kang[2(✉)]

[1] School of Computer Science, Beijing Information Science and Technology University, Beijing 100192, China
bistu_dengjie@163.com

[2] School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China
kanghaiyan@126.com

Abstract. The wide application of smart grid improves the energy utilization rate and improves the power market, but at the same time, it also introduces many security problems, such as data storage, transmission, theft and other security problems in the process of smart grid data communication. Due to the special position of power system, how to ensure the security of data storage in smart grid is of great significance for the safe and stable operation of power grid system. This paper first analyzes the smart grid and its data characteristics, combined with the relevant technologies of cloud computing, gives a data security storage model of smart grid to strengthen the reliability and storage capacity of smart grid. Then, in order to ensure the security of user data storage in the cloud in smart grid, this paper studies the data encryption algorithm, and proposes a hybrid encryption scheme for smart grid data security storage. Finally, the scheme is compared with the traditional method. The experimental results show that the scheme has the advantages of good encryption and decryption effect, fast execution speed and high security. It is an ideal scheme for smart grid data security storage.

Keywords: Smart grid · Data encryption · DES · RSA · Hybrid encryption

1 Introduction

The wide application of new smart grid improves the energy utilization rate and improves the power market, but it also introduces many security problems [1–4]. Due to the large number and variety of communication equipment in smart grid, and most of them are embedded devices, wireless communication with low cost and high flexibility is adopted [5]. In the process of information transmission, it is faced with data eavesdropping, tampering, forgery and other security threats [6–8]. At the same time, with the continuous development of the power grid, its scale will continue to expand, the structure will become more and more complex, the interactive information between the business systems will increase, and the source and distribution of data will be more extensive, which will lead to the data in the power system will present a huge increase, and the form of data

Y.-B. Lin and D.-J. Deng (Eds.): SGIoT 2020, LNICST 354, pp. 135–156, 2021.
https://doi.org/10.1007/978-3-030-69514-9_12

will be more diversified. At the same time, it also puts forward higher requirements for the reliability and real-time of the data. The traditional power hardware facilities, data calculation and processing capacity will be difficult to meet the requirements of future smart grid development. As a new rising technology in recent years, cloud computing technology provides a new way for the development of smart grid. The unique distributed computing and storage characteristics of cloud computing, as well as the advantages of high reliability, strong fault tolerance and easy expansion, can provide effective solutions for the problems encountered in the development process of smart grid. Therefore, the integration of cloud computing technology into the smart grid can ensure that the power hardware infrastructure can integrate all kinds of resources of the current system with as few changes as possible, so as to improve the real-time requirements of the smart grid for data processing, and provide effective support for the development of smart grid technology [9].

At present, the standard symmetric encryption algorithm is still used in smart grid, but the number of wireless terminals in smart grid is large and widely distributed, so the key distribution and effective update is a challenge [10, 11]. In order to solve this challenge, scholars at home and abroad have done a lot of research. For example, Li et al. [12] proposed a privacy protection method of power consumption data based on empirical mode decomposition (EMD) and homomorphic encryption, which solved the risk of leakage of user privacy in the process of power grid load balance and power supply adjustment in order to collect user power consumption data. However, the scheme calls a third-party service to generate and manage the key, and based on mathematical problems, it does not fully consider the storage space and computing capacity of communication equipment in the smart grid, and is not applicable in the process of real-time communication, which will bring additional communication burden [13, 14]. Premnath et al. [15] used NTRU (number theory research u-nit) asymmetric encryption algorithm to realize data integrity protection and identity authentication in data acquisition and monitoring control system of smart grid. However, when the length of data acquisition and monitoring control data packet is large, the storage space of communication equipment in smart grid will be seriously insufficient, and even affect the computing power. Therefore, some scholars have studied a series of lightweight cryptographic algorithms based on algebra, number theory and other basic knowledge. For example, Gao [16] proposed a lightweight key management scheme based on Elliptic Curve Cryptography (ECC) to realize the key distribution and management between the data concentrator and the smart meter. However, due to the shortage of ECC algorithm, the security of ECC key can not be guaranteed. Kumar et al. [17] proposed a lightweight elastic protocol to protect the secure communication between smart meters and smart grid infrastructure. However, the premise of normal operation of the protocol is that the initialization key in the security module of smart meters is always safe and effective, and once it is leaked, it will directly affect the safe transmission of data.

Data encryption technology is known as the core technology of information security, which is mainly divided into symmetric encryption and asymmetric encryption. Data Encryption Standard (DES) algorithm [18] and Rivest Shamir Adleman(RSA) algorithm [19] are typical representatives. DES algorithm is a block encryption algorithm with high computational efficiency and fast encryption speed, but its security depends on the

key. The RSA algorithm is based on the decomposition of large numbers. It adopts the double key system of public key and private key. Its cracking difficulty is equivalent to the decomposition of the product of two large prime numbers. It has high security, but it has high computational cost and slow encryption speed. Although there is no effective method to decipher them in a short time, with the continuous development of computer software and hardware, the performance of computer is changing with each passing day, and the traditional data encryption algorithm is no longer secure. Therefore, in order to better solve the security problem of user data stored in the cloud in smart grid, based on the traditional DES and RSA algorithm, this paper first analyzes the advantages and disadvantages of DES, and combines the advantages of Triple Data Encryption Algorithm (TDEA) and Independent Sub Key DES Algorithm (ISKDES), improves DES algorithm, and proposes a Hybrid double DES encryption algorithm (HDDES). Then, this paper makes a detailed study on the method of judging prime number which affects the operation speed of RSA algorithm. On the basis of not affecting the security of RSA, this paper improves the original method of prime number judgment, and proposes a RSA algorithm based on improved prime number decision (IPNRSA). Finally, this paper combines the HDDES encryption algorithm and IPNRSA encryption algorithm to form a hybrid encryption scheme based on HDDES and IPNRSA, which can effectively ensure the security of user data in the cloud.

2 Data Security Storage Model for Smart Grid

2.1 Symmetric Encryption Algorithm DES

Overview of DES. DES is a block encryption algorithm, which uses 64 bit block encryption mechanism to process binary data. Both packet length and ciphertext packet length are 64 bits, and there is no data extension. The system of DES is public, and the security of the system depends on the confidentiality of the key.

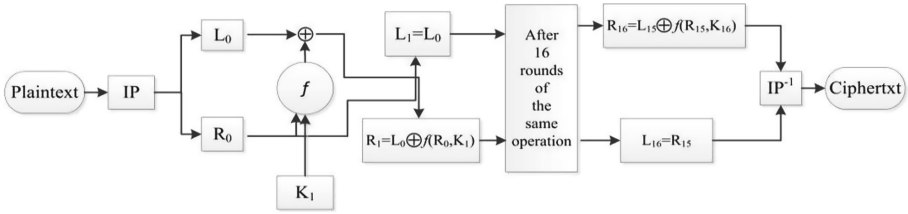


Fig. 1. Iterative flow chart of DES encryption.

The Principle of DES. The decryption process of DES algorithm adopts the same function as the encryption process, but the order of decryption key and encryption key is opposite. In DES algorithm, the key must be processed first. This step includes initial key mapping, 16 sub key calculation and key compression mapping. Then the plaintext is encrypted. The flow chart of DES iteration process is shown in Fig. 1.

2.2 Symmetric Encryption Algorithm RSA

Overview of RSA. RSA as an asymmetric encryption algorithm, one of the most important points is that when the data is transmitted in the network, the key used to encrypt the data does not need to be transmitted with the data, so it reduces the possibility of key leakage. Therefore, RSA is one of the most important encryption algorithms. It can resist most of the known key attacks so far, and ISO takes it as the public key data encryption standard.

The Principle of RSA. RSA algorithm is mainly based on the difficulty of decomposing large numbers, because it is easy to find the product of two large prime numbers, but it is difficult to decompose the product. Therefore, the product of two large prime numbers can be used as public key, and the prime number can be used as the private key generating factor. In this way, it is difficult to use public key and ciphertext to crack plaintext, which is equivalent to decomposing the product of two large prime numbers. Therefore, RSA algorithm is almost impossible to be brutally cracked, with high security. The encryption and decryption process of RSA is shown in Fig. 2.

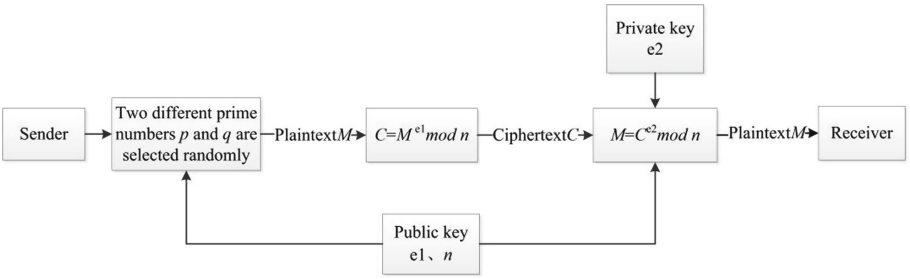


Fig. 2. RSA encryption and decryption process

2.3 Cloud Computing Related Technology Analysis

Cloud Computing Technology. Cloud computing [20] is a new data centric computing method. Its most important idea is to distribute on demand and provide dynamic services. Therefore, advanced computer technology is the pillar of cloud computing. Cloud computing includes virtualization technology, data storage technology, data management technology and some other unique key technologies.

According to different deployment methods, cloud computing has the following four deployment models [21]:

1) Private cloud, that is, a cloud platform built for an enterprise or institution to use alone, does not provide services to the outside world, and can avoid security risks and bandwidth constraints to a certain extent;

2) Public cloud refers to cloud computing services that can be obtained from third-party suppliers for free or at a lower cost, and the service objects have no special requirements;
3) Community cloud is a cloud platform constructed by many organizations with the same interests to support specific communities;
4) Hybrid cloud is composed of two or more public clouds and private clouds, which have the characteristics of the two and are independent of each other.

Hadoop Distributed File System (HDFS). Hadoop Distributed File System (HDFS) is a distributed file system, which is one of the two core technologies of Hadoop. As HDFS has the characteristics of high fault tolerance and high scalability [22], it can be designed and deployed on low-cost computer equipment, and applications can read data with higher efficiency, especially for programs with massive data.

HDFS adopts the Master/Slave structure model. An HDFS cluster is composed of a NameNode and several DataNodes, which undertake the work of Master and Worker respectively. The NameNode is the Master server, which is responsible for the allocation and scheduling in the cluster. The main work is to manage the file system's namespace and adjust the operation of client accessing files. DataNode is the execution node of the specific work in the Worker, which is mainly responsible for managing the data stored in the node. In addition, in order to store massive files reliably, each file in HDFS is stored in block form. This block is an abstract concept. By default, the size of the data block is 64MB. Users can also set data blocks of different sizes according to their actual situation [23]. The architecture of the Hadoop Distributed File System (HDFS) is shown in Fig. 3.

2.4 Construction of Data Security Storage Model for Smart Grid

Advantages of Cloud Computing Technology in Smart Grid. Cloud computing has the characteristics of distributed computing and storage, as well as high reliability, strong fault tolerance and easy expansion. Therefore, the application of cloud computing technology in smart grid can bring the following benefits [24–26]:

1) It can enhance the computing and storage capacity of smart grid. Due to the cloud computing technology in the cloud is through virtualization technology to build a large-scale cluster of computers with a large number of storage space and very efficient processing speed, which makes the massive data generated in each link of the smart grid can be calculated and stored in real time and reliably through cloud computing technology.
2) It improves the utilization rate of smart grid resources and reduces the maintenance cost. Because cloud computing provides a powerful computing and data storage capability for smart grid, all kinds of smart terminal devices in smart grid can be lightweight, without strong data processing capacity. At the same time, each region has system nodes responsible for management, maintenance and update. When a node fails, the processing tasks of this part can be assigned to other nodes to continue

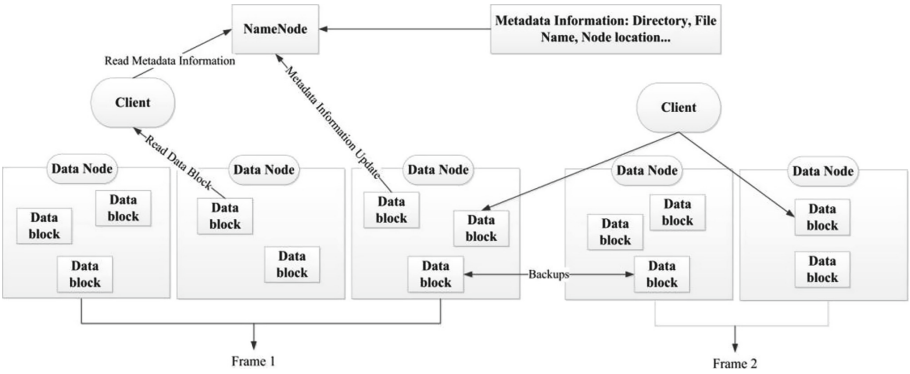


Fig. 3. Architecture of Hadoop distributed file system.

processing. Therefore, the utilization rate of resources is greatly improved and the maintenance cost is greatly reduced.

3) It improves the information and automation of smart grid. Due to the distributed computing and storage characteristics of cloud computing, the real-time and controllability of smart grid data processing are improved. Real time monitoring and timely operation response can be obtained between power systems and user interaction.
4) It improves the reliability of smart grid. Cloud computing provides a safe and reliable data storage center for smart grid. In the cloud storage system, the distributed storage mode is generally applied, and various data disaster recovery technologies and corresponding measures are used to ensure that the data in the cloud storage system can have high reliability.

Data Security Storage Model of Smart Grid (DSSMSG). According to the previous analysis, the introduction of cloud computing technology in smart grid and effective integration of existing software and hardware resources can make power system equipment as constant as possible, and greatly improve the processing and storage capacity of smart grid data [27]. As the hybrid cloud model has the characteristics of both private cloud and public cloud, Chen Jie [28] and others proposed a hybrid cloud structure for smart grid. At the same time, in order to ensure the security of data in the power system, the data with high security requirements should be stored and managed by the private cloud of the power system, while other data with low security requirements should be stored and managed by the public cloud of a third-party cloud service provider.

As the cloud service provider is not a fully trusted third party, the cloud service provider can obtain the first access to the grid related data by handing part of the power related data to the cloud service provider for storage [29]. In fact, there may be internal personnel's dereliction of duty (such as misoperation), hacker attacks, system failures and even the problems of application technology itself, which may have a certain impact on the security of data.

In this paper, we assume that the user is a secure user confirmed by the power service provider, and the operating environment of the private cloud of the power system is credible. This paper mainly studies the security of the data generated by the user in the

public cloud storage. Therefore, based on the hybrid cloud structure of smart grid, this paper presents the data security storage model of smart grid under the deployment mode of hybrid cloud, as shown in Fig. 4.

After encrypting the required data, the data can be transferred to the third-party cloud service provider for storage. The key used by the user to encrypt the data is encrypted by the public key provided by the local power service provider, and then transmitted to the local power service provider for storage. As the trusted third party of users, local power service operators can provide key storage services for users and provide regular data integrity verification services for users. The third-party cloud service provider is mainly responsible for the storage of user data, receiving integrity verification requests from local power service operators, and sending the verification results back to local power service operators.

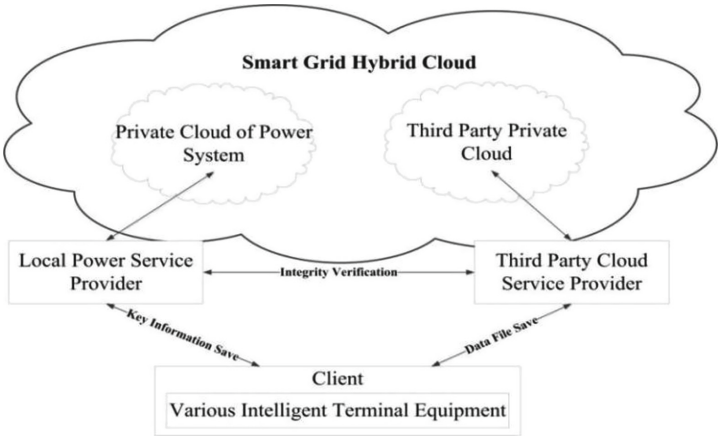


Fig. 4. Data security storage model of smart grid.

3 Hybrid Encryption Scheme for DSSMSG

3.1 A Hybrid Double DES Encryption Algorithm

Overview of DES Algorithm. DES algorithm is also called data encryption standard. It is a symmetric encryption algorithm developed by IBM in 1972. It was determined as the federal data processing standard (FIPS) by the National Bureau of standards of the federal government of the United States in 1976, and then widely spread in the world. Up to now, it still plays a very important role in the international information security stage.

DES is a block encryption algorithm, which adopts 64 bit block encryption mechanism for binary metadata. The length of data packet and ciphertext packet are both 64bit (8byte), without data expansion. The key length is also 64bit, of which 8bit is parity bit, and the remaining 56bit is the effective key length [30, 31]. The whole system of DES is public, and the security of the system depends on the degree of confidentiality of the key.

Analysis of DES's shortcomings

The Key Length is Too Short. The encryption unit of DES is only 64 bit binary, and 8 bits are used for parity check or other communication overhead, so the effective key is only 56 bits. Therefore, this will inevitably reduce the security of DES. With the development of computer performance, the method of brute force cracking des key has been found, and with the computer becoming more and more powerful, the DES with 56 bit key can not support the application with high security requirements. Due to these obvious shortcomings of DES, the National Institute of standards and technology in 1997 stopped studying DES, but studied its alternative method, namely Advanced Encryption Standard(AES) [32].

There is a Weak Key. Because the key is divided into two parts in the process of generating the sub key, if the two parts are divided into all 0 or all 1, the sub key generated in each round is the same. When all keys are 0 or all 1, or half of 1 or 0, weak key or semi weak key will be generated, which will reduce the security of DES.

The Latest Research and Analysis of DES. DES still has many shortcomings, such as its low data transmission rate, not suitable for long-term data protection, and vulnerable to differential key cracking. Therefore, scholars at home and abroad have made many attempts to improve DES algorithm. In this context, they have proposed more influential Triple DES algorithm [33] (TDEA) and independent sub key DES algorithm [34] (ISKDES).

Triple DES Algorithm. Because the key length of traditional DES algorithm is short and easy to be cracked, in order to make up for this deficiency, researchers have proposed a Triple DES Encryption Algorithm (TDEA), that is, the key length of DES is increased by three times, and three different keys are used for triple encryption and decryption. The encryption process is as follows: first encrypt with the first key $k1$, then decrypt with the second key $k2$, and finally encrypt again with the third key $k3$, that is, $C = Ek3(DK2(Ek1M))$. The decryption is in reverse order, that is, $M = Dk1(\mathrm{E}K2(Dk3C))$. The core of TDEA is to use $k1$, $k2$, $k3$ to encrypt plaintext for many times, and the key length is three times of DES. The implementation process of TDEA algorithm is shown in Fig. 5.

Although this method increases the length of the key, improves the security strength of the algorithm, and effectively avoids brute force cracking, its calculation time is increased by n-1 times, so the operation efficiency is very low. In addition, although the key bits in TDEA are 168 bits, the threat of brute force cracking cannot be avoided for the current computer computing power.

Independent Sub Key DES Algorithm. The key of ISKDES algorithm depends on using different randomly generated sub keys for encryption, that is, the sub keys in each iteration are not generated by the same 56 bit binary key. Since 48 bit key is used in each round of 16 iterations, the modified DES key length of ISKDES becomes 768 bits. This method can greatly increase the difficulty of exhaustive decryption, so as to improve the encryption strength of DES. However, the length of key is too long and the cost is also increased.

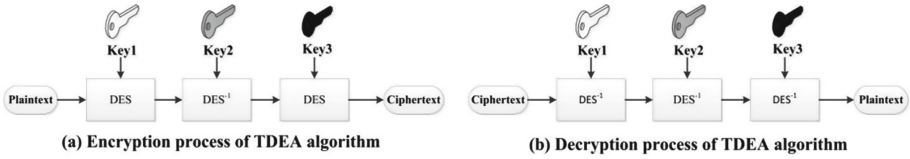


Fig. 5. Encryption and decryption process of TDEA.

Improvement Ideas of DES. Based on TDEA algorithm and ISKDES algorithm, this paper proposes a Hybrid Double DES Encryption Algorithm(HDDES). The algorithm extends the key of DES from 64 bits to 128 bits. After mapping through the mapping table (as shown in Table 1), it is divided into two sub keys (each sub key has 64 bits), which are respectively represented as key1 and key2. Then, 16 sub keys generated by key1 are used to encrypt plaintext to generate ciphertext 1, and then 16 sub keys generated by key2 are used to encrypt ciphertext 1 to generate ciphertext 2. In this way, the security strength is enhanced by double encryption. The specific process of HDDES algorithm is shown in Algorithm 1 and Fig. 6.

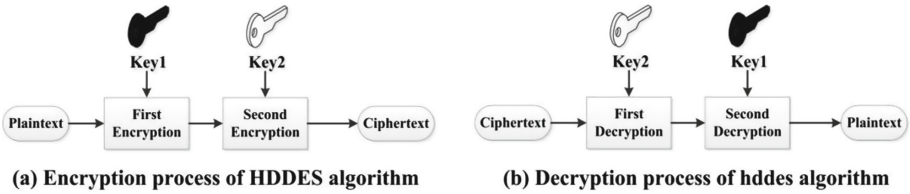


Fig. 6. Encryption and decryption process of HDDES algorithm.

Table 1. 128 bits key mapping figure of TDEA.

97	98	52	21	101	86	103	54	105	3	107	23	109	83	89	112
17	18	19	20	100	22	108	24	25	26	27	28	29	30	31	32
49	50	51	9	53	104	55	56	57	123	59	60	61	62	63	64
81	82	110	84	85	102	87	88	111	90	91	92	93	94	95	96
65	35	67	68	69	37	71	72	40	74	75	76	117	127	79	80
43	116	106	4	114	6	125	8	9	10	121	12	13	118	15	16
113	5	115	2	77	14	119	41	11	122	58	124	7	126	78	128
33	34	66	36	70	38	39	73	120	42	1	44	45	46	47	48

Algorithm 1: A Hybrid Double DES Encryption Algorithm
Input: Plaintext *M*, 128 bits key mapping table
Output: double encrypted ciphertext *C*, double decryption plaintext *M*

1. Extend the key length: The 64 bit key of the original DES is expanded to 128 bit length.
2. Key mapping processing: Input the 128 bits key and map it according to the mapping table in Fig. 6 to get two sub keys key1 and key2, each of which has 64 bits.
3. Generation of sub key: Two sub keys key1 and key2 are processed to obtain 16 sub keys respectively.
4. Plaintext double encryption: After inputting plaintext, encrypting with key1 first, and then encrypting with key2 again to generate ciphertext *C*.
5. Output double encrypted ciphertext *C*.
6. Plaintext double decryption: After inputting ciphertext, first use key2 to decrypt once, and then use key1 to decrypt the second time to restore plaintext *M*.
7. Output double decrypted plaintext *M*.

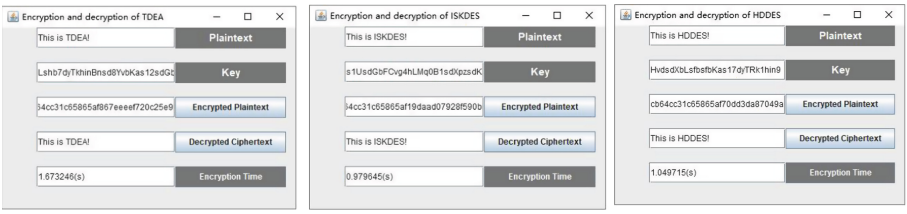
Experimental Analysis of HDDES Algorithm. In order to prove the effectiveness of the HDDES algorithm proposed in this paper, the HDDES algorithm is compared with the Triple DES algorithm (TDEA) and the independent sub key DES algorithm (ISKDES). The experimental environment is set as follows: 1) CPU: Intel Core i5; 2) 2.8 GHz Main Frequency; 3) 24.0 GB Memory; 4) Windows 10 64 bit operating system; 5) Development software: Eclipse 2018 development platform. There are 5 groups in the experiment, each group runs 30 times, and the average encryption time is taken. Table 2 shows the time taken by three encryption algorithms to encrypt 10KB user data in smart grid when they are running separately.

Table 2. Comparison of short message encryption time between two encryption schemes

Operation time	TDEA algorithm	ISKDES algorithm	HDDES algorithm
The first time	1694 ms	1084 ms	1014 ms
The second time	1636 ms	996 ms	1036 ms
The third time	1679 ms	978 ms	1022 ms
The fourth time	1683 ms	984 ms	1039 ms
The fifth time	1668 ms	993 ms	1044 ms

As can be seen from Table 2, compared with TDEA, HDDES has obvious advantages in encryption efficiency, and is almost equal to that of ISKDES algorithm. This is because HDDES algorithm combines the advantages of TDEA and ISKDES. HDDES first expands the original 64 bits key to 128 bits, which reduces the risk of exhaustive attack if the key is too short. Then HDDES uses the advantages of TDEA algorithm to encrypt the encrypted information, which strengthens the security of the algorithm. Finally, referring to the characteristics of ISKDES algorithm, HDDES maps the 12 bits key to achieve local independence and avoid the threat of brute force cracking of the

key. The two complement each other. Due to the only double encryption, the running efficiency of HDDES is higher than that of TDEA algorithm. Figure 7 shows the comparison of the encryption time of the three improved DES algorithms. It is obvious that the encryption efficiency of HDDES is better than that of TDEA.



(a)Time of TDEA (b)Time of ISKDES (c)Time of HDDES

Fig. 7. Comparison of encryption time of three improved DES algorithms.

3.2 A RSA Algorithm Based on Improved Prime Number Judgment

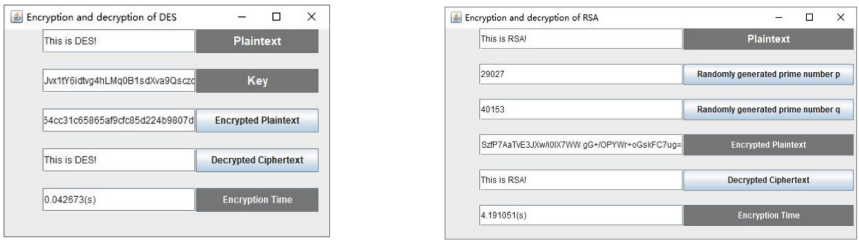
Overview of RSA Algorithm. Rivest Shamir Adleman (RSA) public key encryption algorithm was proposed by RonRivest, AdiShamir and LeonardAdleman in 1977. The algorithm was first published in 1987. RSA is asymmetric because the key used to encrypt the data is not the same as the key used to decrypt it.

RSA as an asymmetric encryption algorithm, one of the most important points is that when the data is transmitted in the network, the key used to encrypt the data does not need to be transmitted with the data. Therefore, this reduces the possibility of key disclosure. RSA is considered to be very secure, but its computing speed is much slower than DES.

Analysis of RSA's Shortcomings. At present, there are mainly the following ways to attack RSA: Forced cracking: try all private keys; Mathematical attack: factoring the product of two prime numbers; Timing attack: depends on the execution time of decryption algorithm. In order to prevent the RSA algorithm from being forced to crack, a super long key must be used. Therefore, the more bits of p and q are, the better. However, the speed of key generation, encryption and decryption is also slower and slower. For the remaining two attacks, the security of RSA is based on the difficulty of multiplication and integration of large prime numbers, so it is almost impossible to crack or the cost of cracking is very high.

Key Generation is Cumbersome. Because two large prime numbers p and q must be used to generate RSA key, it is difficult to use different key for each encryption because of the limitation of prime number generation technology.

Slow Encryption Speed. RSA algorithm not only has the high security which DES does not have, but also is very easy to understand. However, the high security is actually at the expense of encryption speed. In this paper, we compare the encryption time of DES algorithm and RSA algorithm for a group of simple data (2KB) to further illustrate their encryption speed gap, as shown in Fig. 8. In addition, the p, q and other large prime



(a) Encryption time consumption of DES (b) Encryption time consumption of RSA

Fig. 8. Comparison of encryption time between DES and RSA algorithm.

numbers of RSA are randomly generated by using the deterministic property number judgment algorithm. As can be seen from Fig. 8, the encryption time of RSA and DES is almost 100 times different.

The Latest Research and Analysis of RSA. RSA algorithm is a kind of algorithm based on large number decomposition. Because large number decomposition is a recognized mathematical problem, RSA has high security. Although the rapid update of computer hardware, computer performance continues to break through the limit, but the decomposition of large numbers still needs a lot of time to crack. In addition, in order to cope with the rapid development of computer computing power, RSA algorithm gradually increases the length of the key, but the encryption speed of RSA algorithm is just limited by the speed of key generation. In order to solve the encryption speed problem of RSA algorithm, researchers at home and abroad generally adopt two methods. The first method is to improve the implementation of key algorithm [35, 36], and take some measures to speed up its operation. This paper also studies how to improve the generation of RSA key and improve its operation speed. The second method is to find a new public key encryption algorithm to replace RSA, such as the public key encryption algorithm based on elliptic curve [37] (ECC). ECC has achieved a significant breakthrough in efficiency, but it has not been widely used, so a lot of research is still based on theory.

Improvement Ideas of RSA. Since the core algorithm of RSA is the modular power operation of large prime numbers, that is, large number self multiplication module. In order to improve the efficiency of RSA algorithm, it is necessary to solve the problem of operation speed of module power operation in RSA. The core complexity of modular power operation depends on the modular operation, which includes division operation. For a computer, a division operation requires several addition, subtraction and multiplication operations, which is quite time-consuming. Therefore, assuming that RSA algorithm can reduce or even avoid the operation of modulus taking, the performance of RSA algorithm will be significantly improved. Based on this, on the premise of ensuring the security of RSA algorithm, this paper makes a detailed study on the method of judging prime number which affects the operation speed of RSA algorithm module power, and carefully compares the advantages and disadvantages of deterministic and probabilistic prime number judgment algorithms. Then, this paper uses Montgomery fast power algorithm [38] to optimize the classic probability property number judgment

algorithm (Miller-Rabin algorithm), and proposes an Improved fast prime number judgment algorithm (IFPNJA). Finally, this paper applies IFPNJA to RSA algorithm to form an RSA algorithm based on improved prime number decision (IPNRSA).

The Judgment Method of Prime Number. The judgment methods of prime number can be divided into two categories: one is deterministic prime number judgment algorithm, the other is probabilistic prime number judgment algorithm. Deterministic prime number judgment algorithm means its name, that is, the number generated through it is 100% prime, but with certain restrictions. Although the probabilistic prime number judgment algorithm can not guarantee 100% generation of prime number, there is no big restriction, and the speed of generating prime number is faster than that of deterministic prime number judgment algorithm. Generally speaking, the probabilistic prime number judgment algorithm is mostly used in real life. Although it can not guarantee 100% generation of prime number, the generation of non prime number is a small probability event after all, and the probabilistic prime number judgment algorithm can generate pseudo prime numbers quickly and irregularly, meeting most needs.

1) Deterministic prime number judgment algorithm. The most commonly used is divisibility algorithm, that is, the divisibility test. The principle of the algorithm is that all integers used as divisor are less than $\sqrt{n}$. If any of these numbers can be divisible by n, then n is a compound number. The efficiency of divisibility algorithm is very low, and its bit operation complexity is exponential growth.
2) Probabilistic prime number judgment algorithm. Among them, the more famous algorithms are: Miller-Rabin algorithm [39], Solovay-Strassen algorithm [40], Lehman algorithm [41], etc. Since this paper improves the Miller-Rabin probabilistic prime number judgment algorithm and is limited to space, only the Miller-Rabin algorithm is introduced in detail, and other famous algorithms are not described in detail.

Introduction of Miller Rabin Algorithm. If n is an odd prime number, then $n\text{-}1 = 2rm$. r is a nonnegative integer, m is a positive odd number, and a is any positive integer coprime with n, then $am \equiv 1 (\text{mod } n)$ or for some $h (0 \leq h \leq r-1)$, equation $aw \equiv -1 (\text{mod } n)$ holds, where $w = 2hm$. It can be proved that the error probability of Miller-Rabin algorithm is at most 4–1. If n passes the t-test, the probability that n is not a prime number will be $4-t$, while the error probability of Solovay-Strassen algorithm and Lehman algorithm is $2-t$.

An Improved Fast Prime Number Judgment Algorithm. Because of the low efficiency and high complexity of the deterministic prime number judgment algorithm, it is not suitable for the modular power operation of RSA algorithm. Therefore, this paper uses the probabilistic prime number judgment algorithm to improve the modular power operation of RSA algorithm. According to the principle of each probability judgment algorithm, the probability of Miller-Rabin algorithm to judge prime number is much higher than the other two mainstream algorithms. Therefore, this paper selects Miller-Rabin algorithm to improve. This paper introduces Montgomery fast power algorithm, which can greatly reduce modular power operation, to optimize Miller-Rabin algorithm and form

an improved fast prime number judgment algorithm (IFPNJA). The specific process is shown in Algorithm 2.

Algorithm 2: an improved fast prime number judgment algorithm
Input: large number A, B, Miller-Rabin algorithm, modulus N
Output: fast modular multiplication results of large numbers A and B

1. Initial input: input two large numbers A, B and modulus N
2. Base selection: select a positive integer R which is coprime with N as the cardinal number. At the same time, when R is $2k$, N should meet the following requirements: $2k\text{-}1 \leq N \leq 2k$ and $GCD(R,N)=1$
   //Here R can be any base / / In this paper, in order to facilitate the processing, the power based on 2 is adopted
3. Montgomery fast power multiplication: use Montgomery fast power algorithm to simplify Miller-Rabin algorithm and carry out modular multiplication on large numbers A and B, namely Montgomery(A,B,N)=ABR-1(mod N)
4. Output the fast modular multiplication results of large numbers A and B

The main advantage of IFPNJA using Montgomery fast power algorithm is to transform division into shift operation, which not only simplifies the calculation process, but also improves the efficiency of large number power multiplication.

A RSA Algorithm Based on Improved Prime Number Judgment. In order to improve the judging efficiency of IFPNJA applied to RSA algorithm, in the initial stage of prime number generation, all even numbers and numbers divisible by 5 are directly eliminated, and 53 small prime numbers are selected to form a filter array for in-depth filtering, and then IFPNJA is applied to the module power operation of RSA algorithm for rapid screening. All the screening methods complement each other to form a RSA algorithm based on improved prime number judgment (IPNRSA). The specific improvement steps of IPNRSA are shown in Algorithm 3.

Algorithm 3: a RSA algorithm based on improved prime number judgment
Input: plaintext M, Miller-Rabin algorithm, random large array N
Output: encrypted ciphertext C, decrypted plaintext M

1. Random large number generation: randomly generates a large array N except even numbers and numbers divisible by 5
2. Large array screening: select 53 small primes and use the remainder method to filter large array N
3. Optimizing Miller-Rabin algorithm: using Montgomery fast power algorithm to optimize Miller-Rabin algorithm
4. Generate large prime numbers p and q: combine steps 1, 2, 3 and IFPNJA to generate two large prime numbers p and q
5. RSA encryption plaintext: input plaintext M, generate RSA key with two large prime numbers p and q to encrypt plaintext and generate ciphertext C
6. Output encrypted ciphertext C
7. RSA decryption plaintext: input ciphertext C, generate RSA key with two prime numbers p and q to decrypt ciphertext and generate plaintext M
9. Output decrypted plaintext M

Experimental Analysis of IPNRSA Algorithm

In order to verify the uncertainty of the probabilistic prime number judgment algorithm, the Miller-Rabin algorithm (three tests) is compared with the deterministic property number determination algorithm in the number range of 103, 105, 107 and 109. The results are shown in Table 3.

Table 3. Uncertainty of probabilistic judgment algorithm.

Algorithm	Prime number			
	103	105	107	109
Division Algorithm	168	9592	664579	50847534
Miller-Rabin Algorithm	168	9593	664582	50847546

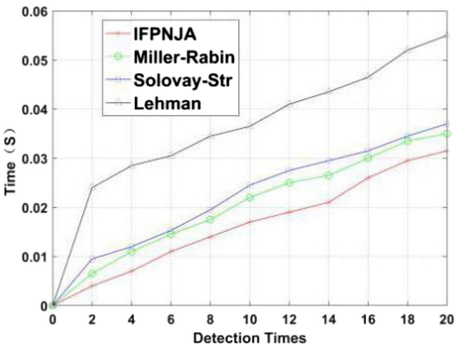
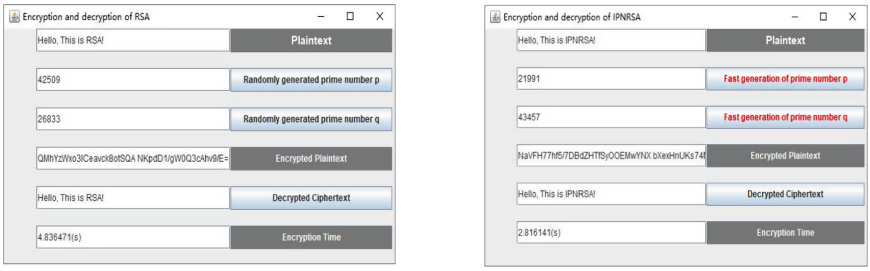


Fig. 9. Relationship between detection times and time of each algorithm.

As can be seen from Table 3, although the Miller-Rabin algorithm has a very high probability of judging a prime number, this probability will decrease with the increase of the number. In this paper, the IFPNJA judgment algorithm is compared with Miller-Rabin, Solovay-Strassen and Lehman three famous judgment algorithms. The experimental data range is [0,1000]. Finally, the relationship between the judgment times and the time is drawn in MATLAB, as shown in Fig. 9.

As can be seen from Fig. 9, the probability of IFPNJA judging prime numbers is not only higher than the other three algorithms, but also the time to generate prime numbers is greatly shortened. The improved prime number judgment algorithm is applied to RSA encryption algorithm to form a RSA algorithm based on improved prime number judgment (IPNRSA). The encryption and decryption time is compared with RSA algorithm. The running results are shown in Fig. 10.

As can be seen from Fig. 8, when producing the same bits of p and q, IPNRSA takes less time than RSA.



(a) RSA encryption and decryption (b)IPNRSA encryption and decryption

Fig. 10. Comparison of encryption time between improved RSA algorithm and RSA algorithm.

3.3 Hybrid Encryption Scheme

Because the process of encryption and decryption of symmetric encryption algorithm (such as DES) is very fast, the encryption efficiency is very high, and it is very suitable for the encryption of smart grid data with fast update frequency and large amount of data. However, because the key is easy to be stolen in the process of transmission, the security is not high. However, the encryption and decryption of asymmetric encryption algorithm (such as RSA) is very slow, and the encryption efficiency is very low, which is not suitable for the encryption of smart grid data. However, due to the difficulty of cracking and the fear of key being stolen, the security is very high. Therefore, in order to solve this problem, this paper adopts a hybrid encryption scheme combining symmetric encryption and asymmetric encryption, that is, HDDES and IPNRSA are used to encrypt the data of smart grid. The specific process is shown in Fig. 11.

Step 1: The sender encrypts the plaintext of smart grid data with HDDES key to obtain encrypted ciphertext.

Step 2: The sender encrypts the HDDES key information with the public key of IPNRSA to get the encryption key.

Step 3: The sender sends the mixed information of encrypted ciphertext and encryption key.

Step 4: After receiving the mixed information, the receiver decrypts the encryption key with the private key of IPNRSA to obtain the HDDES key.

Step 5: The receiver decrypts the encrypted ciphertext with the decrypted HDDES key to obtain the plaintext of smart grid data.

The hybrid encryption strategy based on HDDES and IPNRSA not only improves the efficiency of encrypting user data in smart grid, but also ensures the security of user data transmission in smart grid.

3.4 Verification and Analysis of Hybrid Encryption Scheme

In order to verify the effectiveness of the proposed hybrid encryption scheme based on HDDES and IPNRSA, a detailed experimental comparison and result analysis are made between the proposed hybrid encryption scheme and the traditional hybrid encryption scheme based on DES and RSA in terms of encryption time efficiency and algorithm encryption and decryption performance efficiency.

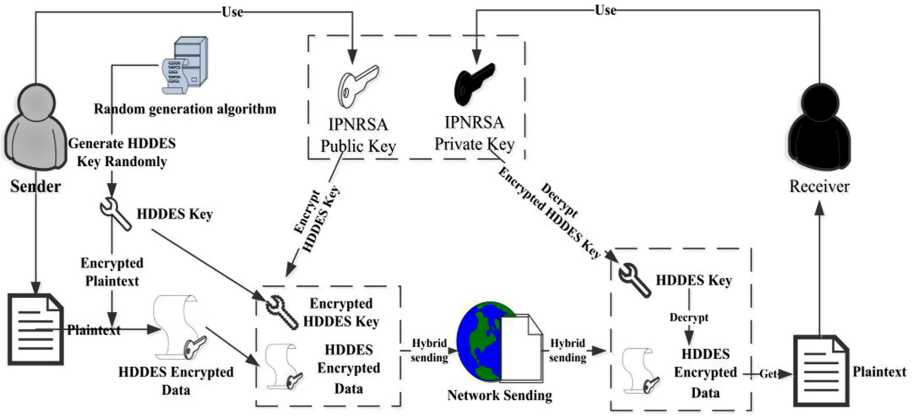


Fig. 11. Hybrid encryption scheme based on HDDES and IPNRSA.

Performance Verification and Analysis of Hybrid Encryption Scheme. This paper compares the key length and generation speed of the hybrid encryption scheme based on DES and RSA and the hybrid encryption scheme based on HDDES and IPNRSA. The length unit is bit, and the results are shown in Table 4.

Table 4. Comparison of key length and generation speed of two encryption schemes

Parameters	Hybrid encryption scheme based on DES and RSA			Hybrid encryption scheme based on HDDES and IPNRSA		
Key length	Secret key	Public key	Private key	Secret key	Public key	Private key
	64	1024	1024	128	1024	1024
Generation speed	Fast	Slow	Slow	Fast	Middle	Middle

The HDDES algorithm extends the 56 bits key of DES, that is, from 56 bits to 128 bits, but it only expands the key by one time, so it has little effect on the speed of key generation after expansion. In addition, RSA encryption algorithm uses 1024 bits key, while IPNRSA encryption algorithm uses improved fast prime number judgment algorithm (IFPNJA) to generate key, so the key generation speed is significantly faster than RSA.

Table 5 shows the comparison of the time spent on encrypting a small amount of smart grid data (200bit) when the two encryption algorithms are running separately. There are five groups of experiments, each group runs 30 times, and the average encryption time is taken.

As can be seen from Table 5, when encrypting short messages, the time difference between the two encryption schemes remains at the level of about 150 ms. Human beings can hardly perceive this subtle time gap, but it is only one encryption operation. If the

encryption times exceed a certain number, the time-consuming gap will become considerable. For example, a web page user uses static data encryption, and the result after encryption is the same, that is, each encryption uses the same key. Therefore, as long as a malicious user intercepts the encrypted message and simulates the form submission information, it can cheat the encryption system to directly invade. Obviously, this static encryption method is not feasible. Even the RSA algorithm using public key cryptosystem has the same result. This risk can be avoided only if the data encryption algorithm uses a different key for each encryption. Therefore, in normal life, it is reasonable and safe to use different keys for each encryption. In addition, if the large amount of smart grid data (more than 2000 KB) is encrypted, the time gap required will be very obvious. Take the two encryption schemes in this experiment, their encryption time will be more than 100 times of the gap. Therefore, the encryption efficiency of the hybrid encryption scheme based on HDDES and IPNRSA has obvious advantages over the traditional hybrid encryption scheme based on DES and RSA.

Table 5. Time comparison of two encryption schemes for encrypting a small amount of data.

Operation time	Hybrid encryption scheme based on DES and RSA	Hybrid encryption scheme based on HDDES and IPNRSA
The first time	511 ms	362 ms
The second time	503 ms	364 ms
The third time	497 ms	359 ms
The fourth time	499 ms	361 ms
The fifth time	507 ms	356 ms

Verification and Analysis of Hybrid Encryption Scheme. In order to verify that the hybrid encryption scheme based on HDDES and IPNRSA can effectively encrypt the user's power data in smart grid, the real power department's user power data information is used for experiment. The experimental environment is set as follows: 1) CPU: Intel Core i5; 2) 2.8 GHz Main Frequency; 3) 24.0 GB Memory; 4) Linux CentOS6.4 operating system; 5) Developing software: Hadoop and Myeclipse Development platform; 6) Server: personal alicloud server. The user power data information collected by an electric power department is encrypted and stored in the cloud. Figure 12 [10] shows part of the original content of the stored data, and Fig. 13 shows part of the encrypted data content viewed in the cloud background.

Security of Data Transmission Process. Before transmission, the data has been authenticated by both parties, and the data to be exchanged has been encrypted, which can ensure the security of the data in the communication process.

Security of Stored Data. The data generated by users in smart grid is encrypted by HDDES and encrypted to produce ciphertext. Because the key and ciphertext of HDDES

CONS_NO	CONS_NAME	CONS_SORT_CODE	ELEC_ADDR	TRADE_TYPE_COI	ELEC_TYPE_COI	VOLT_CODI
1401687584	大风 矿	01	元二 线1725	0610	401	AC00101
1401609322	赤峰 业有 任公司	0106	元二 线	0610	100	AC00101
1402016369	赤峰 业有 任公司	0105	兴二 线1036	0610	100	AC00101
1401681023	平庄 务 （古	01	平一 线728	0610	401	AC00661
1401681052	平庄 务 （东 ）	01	元二 线1726	0610	401	AC00661
3003743817	平庄 务 （元 广）1714反向	00	元二 线1714反向	0690	000	AC00661
1401680990	平庄 务 （元 广）	01	元二 线1714	0610	401	AC00661
1401681821	平庄 业 团） 责任公司	01	平一 线路0700	0610	100	AC00661
1401681834	平庄 务 （元 露天矿）	01	元一 线123	0610	401	AC00661
1401681007	平庄 务 （红 ）	01	元一 乙线124	0610	401	AC00661
1401681049	平庄 务 （风 矿）	01	元二 线1725	0610	401	AC00661
1401681010	平庄 务 （西 矿）	01	平一 线726	0610	401	AC00661

Fig. 12. Original power data information of an electric power department.

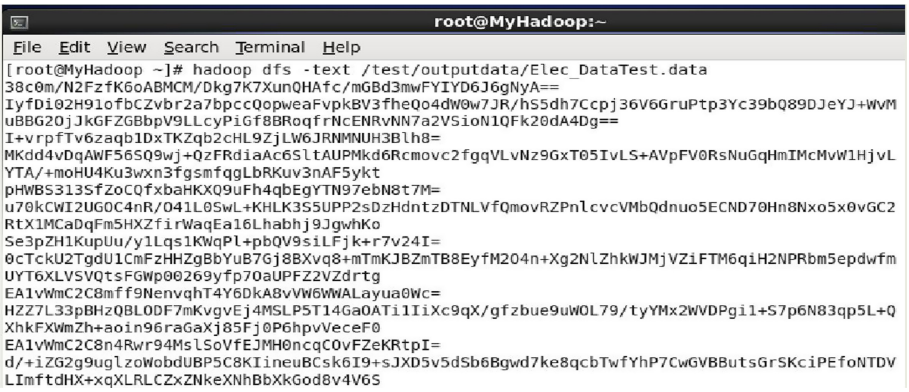


Fig. 13. Encrypted data information stored in alicloud.

are encrypted by IPNRSA, even if the malicious user obtains the ciphertext in the transmission process, it will not be cracked because there is no private key of the receiver. Moreover, the hybrid encryption scheme in this paper can use different keys for each encryption, which makes it very difficult for the attacker to crack the ciphertext. In addition, the key and ciphertext are kept separately, and the effective key length is at least 128 bits, which makes the search space of brute force cracking very large and the possibility of cracking is very small. Therefore, it can be considered that the stored data has high security.

To sum up, the hybrid encryption scheme based on HDDES and IPNRSA proposed in this paper can meet the requirements of data storage security in the development of smart grid, and has high operation efficiency.

4 Conclusion

With the further development of smart grid in the future, the scale of power grid is also expanding, and the data in smart grid is also showing a huge increase. The development of cloud computing technology provides a new direction for data storage and processing in smart grid. While cloud computing technology has helped the development of smart grid, data security in smart grid is also an important issue that can not be ignored. Because

the data confidentiality is an important factor of smart grid data security, this paper makes a more in-depth study on the data encryption algorithm, respectively makes some improvements to the data encryption method, and puts forward two improved encryption algorithms and a hybrid encryption scheme, so that the data security can be effectively improved. Finally, simulation experiments and multi angle analysis are carried out to show that the proposed hybrid encryption scheme can improve the security of smart grid data storage. Of course, the hybrid encryption scheme proposed in this paper can improve the security of data storage, but the data is only pure text, and does not cover the encryption and decryption of pictures, audio and video. In the future, we will continue to study and improve from the above aspects.

Fund Projects. Humanities and social sciences research project of the Ministry of Education (No. 20YJAZH046); National Natural Science Foundation of China (61370139); scientific research level improvement project (2019KYNH219).

References

1. Rajagopalan, S.R., Sankar, L., Mohajer, S., et al.: Smart meter privacy: a utility-privacy framework. In: IEEE International Conference on Smart Grid Communications 2011, Brussels, Belgium, pp. 190–195. IEEE (2011)
2. Lu, Z., Lu, X., Wang, W., et al.: Review and evaluation of security threats on the communication networks in the smart grid. In: Military Communications Conference 2010, San Jose, pp. 1830–1835. IEEE (2010)
3. Liu, X.Y., Zhang, Q., Li, Z.M.: A survey on information security for smart grid. Electr. Power Inf. Commun. Technol. **12**(4), 56–60 (2014)
4. Amin, S.M.: Smart grid security, privacy, and resilient architectures: opportunities and challenges. IEEE Power Energy Soc. Gen. Meet. 2012, SanDiego, pp. 1–2. IEEE (2012)
5. Wang, X., Yi, P.: Security framework for wireless communications in smart distribution grid. IEEE Trans. Smart Grid **2**(4), 809–818 (2011)
6. Lim, H., Ko, J., Lee, S., et al.: Security architecture model for smart grid communication systems. In: International Conference on IT Convergence and Security 2013, Macao, pp. 327–330. IEEE (2013)
7. Li, X., Liang, X., Lu, R., et al.: Securing smart grid: cyberattacks, countermeasures, and challenges. IEEE Commun. Mag. **50**(8), 38–45 (2012)
8. Anandhi, A., Kalpana, G.: Securing smart grid communication against false data injection attacks. Wireless Commun. **8**(5), 211–215 (2016)
9. Bitzer, B., Gebretsadik, E.S.: Cloud computing framework for smart grid applications. In: Power Engineering Conference 48th International Universities 2013, pp. 1–5. IEEE (2013)
10. Nicanfar, H., Jokar, P., Beznosov, K., et al.: Efficient authentication and key management mechanisms for smart grid communications. IEEE Syst. J. **8**(2), 629–640 (2014)
11. Smart Grid Interoperability Panel Cyber Security Working Group: Introduction to NISTIR 7628 guidelines for smart grid cyber security [EB/OL], USA, NIST Special Publication (2010). https://www.nist.gov/smart-grid/upload/nistir-7628_total.pdf
12. Li, Y.C., Zhang, P., Zheng, S.Q.: Privacy protection of power consumption big data based on empirical mode decomposition and homomorphic encryption. Power Grid Technol. **43**(05), 1810–1818 (2019)
13. Dehalwar, V., Kalam, A., Kolhe, M.L., et al.: Review of IEEE 802. 22 and IEC 61850 for real-time communication in smart grid. In: International Conference on Computing and Network Communications 2015, Trivandrum, India, pp. 571–575. IEEE (2015)

14. Fu, G., Zhou, N.R., Wen, H.: The study of security issues for the industrial control system communication protocols in smart grid system. Inf. Secur. Technol. **5**(1), 36–38 (2014)
15. Premnath, A.P., Jo, J.Y., Kim, Y.: Application of NTRU cryptographic algorithm for SCADA security. In: 11th International Conference on Information Technology: New Generations 2014, Las Vegas, pp. 341–346, IEEE (2014)
16. Gao, K.T., Mao, Y.G., Xun, P., et al.: Light-weight key management solution for OSGP. J. Chin. Comput. Syst. **36**(10), 166–170 (2015)
17. Kumar, V., Hussain, M.: Secure communication for advance metering infrastructure in smart grid. In: Annual IEEE India Conference 2014, Pune, India, pp. 1–6. IEEE (2014)
18. Tuchman, W.: Hellman presents no shortcut solutions to the des. IEEE Spectr. **16**(7), 40–41 (1979)
19. Rivest, R.L., Shamir, A.,Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
20. Feng, D.G., Zhang, M., Zhang, Y., Xu, Z.: Study on cloud computing security. J. Softw. **22**(1), 71–83 (2011)
21. Yi, Z.D., Duan, Y.Z., Xiao, C.W., et al.: Cloud computing security: concept, status quo and key technologies. Proceedings of the 27th National Conference on Computer Security (2012)
22. Gao, Y.Z., Li, B.L., Chen, X.Y.: Random detection algorithm of HDFS data theft based on MapReduce. J. Cryptologic Res. **39**(10), 15–25 (2018)
23. Sivapragash, C., Thilaga, S.R., Kumar, S.S.: Advanced cloud computing in smart power grid. In: Sustainable Energy and Intelligent Systems 2012. IET Chennai 3rd International, pp. 1–6 (2012)
24. Li, Q.L., Zhou, M.T.: Research on cloud computing in smart grid. Comput. Sci. **38**(B10), 432–433 (2011)
25. Cong, W., Qian, W., Kui, R., et al.: Ensuring data storage security in cloud computing. In: 17th International WorkShop 2009. Quality of Service IWQoS, pp. 13–15 (2009)
26. Hashmi, M., Hanninen, S., Maki, K.: Survey of smart grid concepts, architectures, and technological demonstrations worldwide. In: 2011 IEEE PES Conference 2011 in Innovative Smart Grid Technologies, pp. 19–21 (2011)
27. Chen, J., Zhang, Y.Y.: Research on application and security of cloud computing in smart grid. ZTE Technol. **18**(6), 17–21 (2012)
28. Huang, J.F., Wang, H.G., Qiang, Y.: Smart grid communications in challenging environments. In: 2012 IEEE Third International Conference 2012 in Smart Grid Communications, pp. 552–557 (2012)
29. Wright, M.A.: The evolution of the advanced encryption standard. Netw. Secur. **1999**(11), 11–14 (1999)
30. Chen, Q.C.: A hybrid encryption algorithm based on DES and RSA algorithm. Yunnan University, China (2015)
31. Jain, N., Ajnar, D.S., Jain, P.K.: Optimization of advanced encryption standard algorithm (AES) on field programmable gate array (FPGA). In: International Conference on Communication and Electronics Systems 2019. IEEE (2020)
32. Gao, N.N., Li, Z.C., Wang, Q.: A reconfigurable architecture for high speed implementation of DES, 3DES and AES. Acta electronica Sinica **34**(8), 1386–1390 (2006)
33. Yu, W.: Research on key extension method and security of DES algorithm. Central China Normal University, China (2019)
34. Sepahvandi, S., Hosseinza, M., Navi, K., et al.: IEEE 2009 International Conference on Research Challenges in Computer Science (ICRCCS), 28 November 2009–29 November 2009, Shanghai, China, 2009 International Conference on Research Challenges in Computer Science - An Improved Exponentiation Algorithm for RSA Cryptosystem, pp. 128–132 (2009)

35. Li, D.J., Wang, Y.D., Chen, H.: The research on key generation in RSA public-key cryptosystem. In: Fourth International Conference on Computational & Information Sciences. IEEE (2012)
36. Zhou, J.Z., Gao, L.: Research on improved RSA algorithm based on multi prime number and parameter replacement. Comput. Appl. Res. **36**(02), 495–498 (2019)
37. Yan, S.Y.: Elliptic Curve Cryptography. Cybercryptography: Applicable Cryptography for Cyberspace Security (2019)
38. Li, F., Gong, Z.Y., Lei, F.F., et al.: Summary of fast prime generation methods. J. Cryptologic Res. **06**(04), 463–476 (2019)
39. Qin, X.D., Xin, Y.W., Lu, G.Z.: Research and optimization of Miller Rabin algorithm. Comput. Eng. **28**(10), 55–57 (2002)
40. Zhao, Y.W., Liu, F.F., Jiang, L.J., et al.: Multi core parallelization of Sch(o)nhage Strassen algorithm for large integer multiplication. J. Soft. **29**(12), 3604–3613 (2018)
41. Fu, X.Q., Bao, W.S., Zhou, C., et al.: Integer factorization quantum algorithm with high probability. Acta electronica Sinica **39**(01), 35–39 (2011)