Application of the Source Encryption Algorithm Model in the Power Industry

Jiao Longbing
Shaanxi Huabiao Network Technology Co., Ltd.
Xi’an, 610041, China
E-mail: james9894@163.com

***Abstract*—With the development of Internet technology and Internet of Things technology, the Internet of Everything has become a hot topic, and in March 2019, the National Grid for the first time clarified the definition of the Pan-In Power Internet of Things, pointing out that the company's most urgent and important task is to accelerate the construction of the Pan-In Power Internet of Things. The security of Data Transfer on-line at any time is particularly important, in order to ensure the security of data, in the process of data transmission, data needs to be encrypted. This paper expounds a model of the information source data encryption algorithm, analyzes the encryption algorithm and the encryption method, and then provides a reference basis for the data transmission data security of power system.**

Keywords-Data Communication; Encryption Algorithm Model; Encryption Technology

I. INTRODUCTION

Driven by intelligence and informatization, ubiquitous electric Internet of things is just at the right time. The construction of power Internet of things puts forward higher requirements for data management and information management. At present, the state grid system is connected to more than 500 million terminal devices, and with the construction of electric Internet of things and the surge, there will be a huge amount of data. Data is an important asset, data privacy protection, the construction of data security grading system, based on different security levels to determine the open rights of data, to ensure the efficiency of business execution and smooth management.

Internet of things technology is developing rapidly, but the corresponding infrastructure and security protection capabilities do not adapt to it. Network security is the biggest hidden danger of the power Internet of things. On the one hand, non-ip communication protocol is often used to transmit data in the Internet of things, which lacks effective security measures. On the other hand, the increasingly intelligent and professional means of network attack have brought new problems to network security protection, leading to frequent network security incidents in the field of power grid in recent years.

Therefore, strengthening the security risk control and management of intelligent and informationized power Internet of things will be a key point of China's ubiquitous power Internet of things construction.

This paper will focus on the introduction of a source encryption algorithm model, hoping to provide a digital security model reference for the application of digital business in the power industry.

II. INTRODUCTION TO ENCRYPTION TECHNOLOGY

As an important part of network security, data encryption technology plays a very important role in the network. It involves the confidentiality, authentication, non-repudiation and integrity of data. Key is the key of data encryption, which controls the

DOI: 10.21307/ijanmc-2019-073

implementation of encryption and decryption algorithms. According to the different keys, the encryption technology is divided into symmetric encryption technology, asymmetric encryption technology, mixed encryption technology.

A. *Symmetric encryption*

Symmetric encryption means that the encryption key can be inferred from the decryption key, and the decryption key can also be inferred from the encryption key. In most symmetric algorithms, the encryption key and the decryption key are the same. For this algorithm, its key (secret key) usually needs messenger or secret channel to transmit, and it is difficult to transmit and manage the key. In this case, the secret preservation of the key determines the security of the algorithm. RC4, chaos algorithm, DES, IDEA, RCZ algorithm are typical representative of symmetric key encryption system. Because both parties have the same key, symmetric encryption technology is easy to implement and fast, so it is widely used in communication and storage data encryption and decryption. The security of symmetric encryption depends on the key, so the secret of the key is very important to the security of communication. The symmetric encryption process is shown in the figure 1.

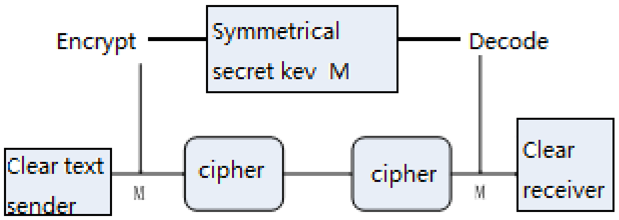

Figure 1. Symmetric encryption flow chart

B. *Asymmetric encryption*

This technique can also be called public key cryptography. The encryption key (public key) can be made public, that is, it can be obtained by strangers and used to encrypt the information, but the information can only be decrypted with the corresponding decryption key (private key). Compared with symmetric encryption algorithms, asymmetric encryption algorithms usually require two keys: public key and Private key. When data is encrypted with a key, if it is encrypted with a public key, it can only be decrypted with the corresponding private key. Instead, it is decrypted with the corresponding public key. The advantage of public key cryptography is that it can adapt to the open requirements of the network, but the speed is relatively slow, not suitable for encrypting files. The asymmetric encryption process is shown in the figure 2.

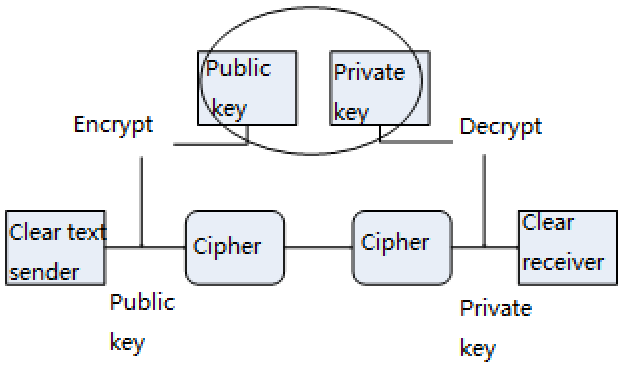

Figure 2. Asymmetric encryption flowchart

C. *Hybrid encryption*

Hybrid encryption is not a single encryption technology, but a combination of the above two data encryption technology combined product. The communication process of the communication parties is divided into two parts. The parties first use asymmetric encryption technology to transmit the symmetric key used in the communication, and then use symmetric encryption technology to encrypt and transmit the file.

III. TEMPORAL AND SPATIAL VARIABLES PARTICIPATE IN THE SOURCE ENCRYPTION MODEL

A. *Time variable definition：*

1) *Year, month, day, hour and time variables*

TABLE I. TIME VARIOMETER

		1	2	3	4	5	6	7	8	9	10	11	12
		A	B	C	D	E	F	G	H	I	J	K	L
1	a	Aa	Ba	Ca	Da	Ea	Fa	Ga	Ha	Ia	Ja	ka	La
2	b	Ab	Bb	Cb	Db	Eb	Fb	Gb	Hb	Ib	Jb	kb	Lb
3	c	Ac	Bc	Cc	Dc	Ec	Fc	Gc	Hc	Ic	Jc	kc	Lc
4	d	Ad	Bd	Cd	Dd	Ed	Fd	Gd	Hd	Id	Jd	kd	Ld
5	e	Ae	Be	Ce	De	Ee	Fe	Ge	He	Ie	Je	ke	Le
6	f	Af	Bf	Cf	Df	Ef	Ff	Gf	Hf	If	Jf	kf	Lf
7	g	Ag	Bg	Cg	Dg	Eg	Fg	Gg	Hg	Ig	Jg	kg	Lg
8	h	Ah	Bh	Ch	Dh	Eh	Fh	Gh	Hh	Ih	Jh	kh	Lh
9	i	Ai	Bi	Ci	Di	Ei	Fi	Gi	Hi	Ii	Ji	ki	Li
10	j	Aj	Bj	Cj	Dj	Ej	Fj	Gj	Hj	Ij	Jj	kj	Lj

Year, month, day and hour variables are added to the partial key format of data information source, as shown in figure format, 12 bits and 10 bits are combined to form a unique time variable. Year, month, day, and hour cycle with 60 and map to Gregorian calendar time.

2) Increase position variable

The position variable is assigned to map the location of the source to the latitude and longitude coordinates. As the key bit.

TABLE II. LOCATION VARIABLES

4 southeast	9 south	2 southwest
3 east	5 center	7 west
8 northeast	1 north	6 northwest

3) The source data is rearranged and encrypted according to location, time and solar term variables

The data format conversion of an encryption depends on a unique time point, and the time point of data encryption determines that the data conversion mode in the figure below is unique.

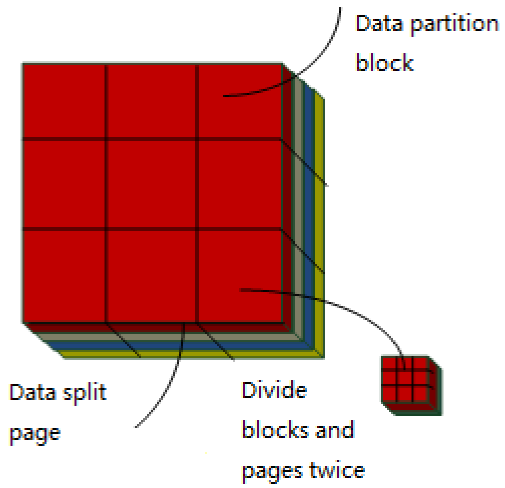

Figure 3. Data conversion mode

Determine the starting time of the data encryption variable, time variable form the basis for packet rotation changes, packets after be confirmed time and location, the data layer, and then each layer of blocks, each block in the above order to secondary polarization, and then according to the law of time each block and the PAGE will be rotating, and the rule of each PAGE rotation, eventually forming the smallest unit, each unit to block position number.

After the above sequence of data format and order is completely disrupted, according to the unconventional format of the order, is to refer to the passage of time and position rotation.

After such data arrangement, data, pictures, videos and other files, even if they are intercepted, cannot obtain the key encryption variables of time, solar term and location, and cannot obtain useful key information even if they are enumerated.

4) Law of rotation arrangement of source data format

After the data is divided into different pages, it is rotated and changed according to the hierarchy of layers. For example, the bottom layer is the rotation mode, the third layer is the feig reordering, the second layer is the rotation according to the third layer of feig, the first layer is the rotation according to the second layer of rotation. To this data page is partitioned and rearranged. Then the quadratic element is carried out, and the data block of the first part is redistributed into 16 blocks. After three dimensions, three dimensions and four dimensions are differentiated to the smallest data unit bit.

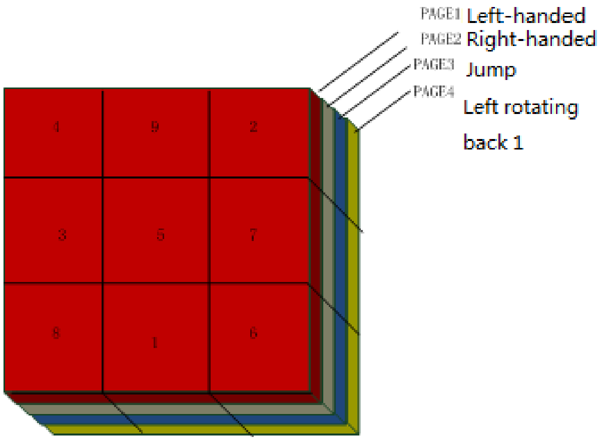

Figure 4. Rotation arrangement rule

5) *Data decryption process model*

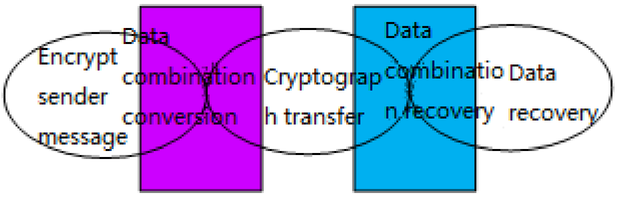

Figure 5. Data decryption model

a) The sender rearranges the blocks and pages of the data format according to the time variable and the position marker bit, and the quadratic element and cubic element are segmented and arranged according to the same method to form the minimum bit of scatter random data.

b) Transfer process: the file transfer process is transmitted with three-point random minimum bit data, and the time at this time is a shift. After the time shift, the information received by the receiver should be arranged according to the change of time variable for time key mapping.

c) C. Data receiver, the receiver is minimum scatter data, the receiver must key is according to the sender to the time, location, variables and receiving time to time, location, and, according to the minimum level to the smallest unit according to position the label to the reverse calculation into pieces, and then pushing block reverse page to the model, and then push the page to the original data model. The process record of backward calculation is the decryption key.

The above data encryption model is the data encryption model established based on the cubic dimension secret calculation model, which can be used to split and switch the top secret data multiple times. In addition, it is not only applicable to data, but also applicable to audio and image data.

6) *The programming language realizes the model construction idea of the encryption model*

- Data type definition

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
namespace FateJudge.Core.QM
{
    public class  QM Data
    {
        public static int[] ShunZhuan = new int[] { 1,
8, 3, 4, 9, 2, 7, 6 };
         public static int[] NiZhuan = new int[]
{ 1,6,7,2,9,4,3,8};
        public static String[] jushu=new string[]{
            "174","285","396",
            "852","963","174",
            "396","417","528",
            "417","528","639",
            "936","825","714",

            "258","147","936",

            "714","693","582",

            "693","582","471"};

        public static String QYYW="

    public static String[] RPQM = new string[] { " };

        public static String[] tianpanxingyuanwei =
new string[] { };

        public static String[] SPQM = new string[]
{   };

        public static String[] renpanxingzhuanxu =
new string[] {}; public static String[]
tianpanxingzhuanxu = new string[] { }; public static
String[] shenpanzhuanxu = new string[] { };/

      }

    }
```

- Data rotation

```
public int getRPG (string yinyan, int zhishigong,
string zhishi, string ren)
    {
        int ret = 0;
        int n =
getStringArrayIndex(QMData.rpxzx, ren);// -
getStringArrayIndex(QMData. rpxzx, zS) + 8) %
8;
        int n1 = 0;
        n1 =
(getIntArrayIndex(QMData.ShunZhuan,
zhishigong) + n) % 8;
        ret = QMData.ShunZhuan[n1];
        return ret;
    }
    public int getIntArrayIndex(int[] sa, int n)
    {
        int ret = 0;
        for (int i = 0; i < sa.Length; i++)
            if (sa[i].Equals(n))
            {
                ret = i;
                break;
            }
        }
            return ret;
        }
        public string getPostRenPan(string zhishi, int
zhishigong, int p)
            {
                string ret = string.Empty;
                int n1 = 0;
                int n2 = 0;
                int n3 = 0;
                n1 =
(getIntArrayIndex(QMData.ShunZhuan, p) -
getIntArrayIndex(QMD.ShunZhuan, zhishigong)
+ 8) % 8;
                n2 =
getStringArrayIndex(Qi=M=Data. rpxzx, zhishi);
                n3 = (8 + n2 + n1) % 8;
                ret = QiMenData. rpxzx [n3];
                return ret;
            }
```

IV. CONCLUSION

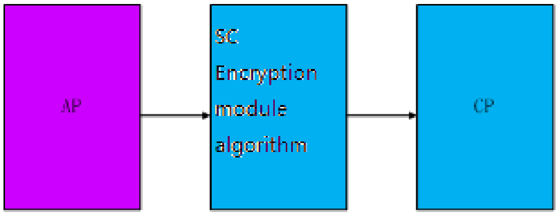

Figure 6. Data encryption model

Power data is the lifeblood of a country's economy and people's life. With the great development of Internet of things, Internet and ubiquitous electric Internet of things, the security of data connection is particularly important. Through the practice of the above data encryption model, the source information can be encrypted, which is different from several symmetric encryption algorithms and asymmetric encryption algorithms. This kind of model calculation can be encapsulated into IC or T card to form an encryption module, which is widely used in power inspection terminals, smart electricity meters and power big data cleaning applications, to increase the security means of data transmission, and to provide some enlightenment and reference for the data transmission encryption methods of power companies.

REFERENCE

[1] Song Lei, Luo Qiliang, Luo Yi, Tu Guangyu. Encryption scheme of real-time data communication in power system [J]. Power system automation, 2004 (07)

[2] Liu gang, liang ye et al. Realization and application of digital certificate technology in power secondary system [J]. Power grid technology,2006,10

[3] Xingyuan Wang,Hongyu Zhao,Le Feng,Xiaolin Ye,Hao Zhang. High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices[J]. Optics and Lasers in Engineering,2019,122.

[4] Chen changqing. Research on computer network communication intrusion prevention method based on data encryption technology [J]. Information and computer (theoretical edition),2019(14):171-172.

[5] DOE/Oak Ridge National Laboratory; ORNL to take on nine power grid modernization projects as part of DOE award[J]. NewsRx Health &amp; Science,2019.

[6] Chen zhiguang. Analysis and design of power project management system of state grid fuzhou power supply company [D]. Yunnan university,2016.