ADVANCE RESEARCH JOURNAL OF MULTIDISCIPLINARY DISCOVERIES
ISSN : 2456-1045
VOL.39 I ISSUE-1 I CHAPTER-5
PUBLISHER : INTERNATIONAL JOURNAL FOUNDATION (IJF)

An improved secret sharing scheme based on (*K,N*) threshold*

Haibing Sun[1], Shirong Feng[2], Simin Wang[3], *Tianxiu Lu[4]

[1,3,4] *School of Mathematics and Statistics, Sichuan University of Science and Engineering, Zigong 643000;*
[2] *School of Automation and Information Engineering, Sichuan University of Science and Engineering, Zigong 643000*

ABSTRACT

The issue of secure sharing of information was studied. The (K,N) secret threshold scheme which proposed by Shamir was improved. The secret sharing system is divided into two parts: information segmentation and information synthesis. The authentication part will be added to the improved secret sharing mechanism. The fragmentation information is encrypted by the RSA algorithm to prevent someone from using it for information recovery.

Keywords : Information sharing, (K,N) threshold scheme, RSA encryption algorithm.

ORIGINAL RESEARCH ARTICLE

ISSN : 2456-1045 (Online)
(ICV-APM/Impact Value): 72.30
(GIF) Impact Factor: 5.188
Publishing Copyright @ International Journal Foundation
Journal Code: ARJMD/APM/V-39.0/I-1/C-5/JULY-2019
Category : APPLIED MATHEMATICS
Volume : 39.0/**Chapter**- V/**Issue** -1 (JULY-2019)
Journal Website: www.journalresearchijf.com
Paper Received: 23.07.2019
Paper Accepted: 01.08.2019
Date of Publication: 10-08-2019
Page: 38-42

Name of the Corresponding author:
Tianxiu Lu*
School of Mathematics and Statistics, Sichuan University of Science and Engineering, Zigong 643000; China

CITATION OF THE ARTICLE

Sun H. ; Feng S. ; Wang S. ; Lu T. (2019) An improved secret sharing scheme based on *(K,N)* threshold; *Advance Research Journal of Multidisciplinary Discoveries;* 39 (5) pp. 38-42

**This project was supported by the National Natural Science Foundation of China and the College Students Innovation and Entrepreneurship Project of Sichuan Province (No. 201710622060, 201810622025, S201910622014)*

I. INTRODUCTION

In 1984, based on Lagrange interpolation, *Shamir* [1] proposed *(K, N)* key threshold scheme for information sharing security problem. It means that the secret will be segmented to *N* parts, which will be held by *N* partners. And for any *K(or >K)* partners, they can recovery the whole secrets. Otherwise, the information recovery will not be successful. 3 years later, Ito [2] and his workmates proposed key sharing scheme for general access structure, which is the promotion for *Shamir* key sharing scheme. However, it needs lots of information, which could cause data diffusion. So it is not practical. Afterwards, many domestic and foreign scholars have proposed many key sharing schemes, for example, Generalized multi-key sharing scheme [3], Verifiable multi-key sharing scheme [4], Dynamic multi-key sharing scheme [5], and so on. In order to improve the security of the solution and reduce the complexity of the system, multiple key sharing schemes were combined with the RSA. At the beginning of this century, many scholars have studied this (such as the references [7]-[14]. However, most studies lack verification of secret sharing or just verify the secret itself (e.g. [7]) but not authentication. Lack of validation may cause the secret being revealed by criminals.

This paper will improve the method that from *(K, N)* threshold key sharing scheme put forward by *Shamir*. The identity of the secrets holders will be verified. RSA algorithm was used to encrypt the fragment information. It can prevent someone from stealing fragment information for information recovery.

1. The improved *Shamir* information sharing scheme

Assume that information S will be segment for n parts and held by m people $(n>m)$. Let $F(x)=A_0+A_1x+A_2x^2+\cdots A_{k-1}x^{k-1}$.

Where $A_0=F(0)=S$, $A_1,A_2,\cdots,A_{k-1}$ coefficients from a finite field. A_0 (held by the sender) is the information we want to recover.

When the information is divided into n parts, it generates x_i $(i=1,2,\cdots,n)$ (n different sub-secrets). The sub-information distribution process is considered to send x_i $(i=1,2,\cdots,n)$ to m different recipients. The recovery process is recorded as to solve the polynomial coefficients by choose k of $(x_i, F(x_i))$ $(i=1,2,\cdots,n)$. And then, $A_0 = F(0) = S$. If at least k of the M information fragments are present, the information can be recovered.

The *RSA* algorithm is used to encrypt the fragment information. That is, the sender of the information first divides the information into *n* parts, encrypts them with the public key, and then send out. When the information needs to be recovered, the receivers of the fragment information needs authenticated first. That is, the fragmentation information is decrypted with the private key. If the decryption is successful, the identity verification is correct. This implies that the fragmentation information is not stolen. So the information can be recovered. Otherwise, the information can not be recovered.

II. MODELLING ESTABLISHMENT

Choosing a $k-1$ polynomial for Shamir secret sharing scheme

$$F(x) = A_0 + A_1 x + A_2 x^2 + A_{k-1} x^{k-1}$$

Where $A_0 = F(0) = S$, that is, the constant term is specified as the secret to be split. and then, any $k-1$ coefficients from a finite field is selected. Obviously, for this polynomial, $F(x)$ can be recovered only by k different $F(x_i)$ $(i=1,2,\cdots,k)$. There is *n* sub-information, so for any *n* different x_i $(i=1,2,\cdots,n)$, one can calculate $F(x_i)$ $(i=1,2,\cdots,n)$, that is, $(x_i, F(x_i))$ $(i=1,2,\cdots,n)$ are the sub-information segmented by sender. Any k of n sub-information can refactoring $F(x)$ and then recovering the information *S*.

2.1 Information segmentation

Let $GF(Q)$ is a finite field, and Q is a large prime number which will satisfies the condition $Q \geq n+1$. Information S is a random number from $GF(Q) \setminus \{0\}$, denoted by $S \in_R GF(Q) \setminus \{0\}$). $S = A_0$. The others $A_1, A_2, \cdots, A_{k-1}$ satisfy the condition $A_i \in_R GF(Q) \setminus \{0\}$ $(i=1,2,\cdots,k-1)$. So the polynomial on $GF(Q)$ is

$$F(x) = A_0 + A_1 x + A_2 x^2 + A_{k-1} x^{k-1}$$

n receivers are denoted by $P_1, P_2, \cdots, P_n$, where P_i is the sub-information $(i, F(i))$ $(i=1,2,\cdots,n)$.

2.2 Information recovery

If k receivers $P_{i_1}, P_{i_2}, \cdots, P_{i_k}$ $(1 \leq i_1 < i_2 < \cdots < i_k \leq n)$ want to get information S, they will use $\{i_L, F(i_L) \mid L=1,2,\cdots,k\}$.

$$\begin{cases} A_0 + A_1(i_1) + \cdots + A_{k-1}(i_1)^{k-1} = F(i_1) \\ A_0 + A_1(i_2) + \cdots + A_{k-1}(i_2)^{k-1} = F(i_2) \\ A_0 + A_1(i_3) + \cdots + A_{k-1}(i_3)^{k-1} = F(i_3) \\ \cdots\cdots \\ A_0 + A_1(i_k) + \cdots + A_{k-1}(i_k)^{k-1} = F(i_k) \end{cases}$$

So $S = A_0 = F(0)$. *m* receivers only know the constant term, rather than the whole polynomial $F(x)$.

2.3 Identity verification— *RSA* encryption algorithm

RSA algorithm [6]-[8] is a more mature algorithm in the public key mechanism. It is the first algorithm that can be used for both data encryption and digital signature. It provides a basic idea for encrypting and identifying information on public networks. Therefore, the development and research of *RSA* have a great practical significance for us to summarize knowledge and combine it with practice.

The following are procedures of *RSA*.

Step1. Select randomly two large prime numbers p and q;

Step2. Calculate $n = p * q$ (public), $\Phi(n) = (p-1)*(q-1)$ (secret);

Step3. Select randomly positive integers e which satisfies $\gcd(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$;

Step4. Calculated d using the E uclidean algorithm, s.t :

$$ed \equiv 1 (\bmod \Phi(n)) = 1, \& 1 < e < \Phi(n);$$

Step5. $E = (n, e)$ is as the public key, and $D = (n, d)$ is as the secret key.

When *RSA* public key system is used in encryption, it will first digitize the text, then group them (where the length of each group does not exceed $\log(n)$), and encryption and decryption for each group separately.

ISSN : 2456-1045 (ONLINE)

The encryption process is as follows.

Assume the text group to be encrypted is $m\,(0 \le m < n)$, then

$$c = E(m) = m^e (\operatorname{mod} n),$$

c is the secret text.

The decryption process is as follows.

$$m = D(c) = c^d (\operatorname{mod} n)$$

m is the recovered text. It should be consistent with the plaintext content which is entered earlier to be encrypted.

The flow chart is shown as follows.

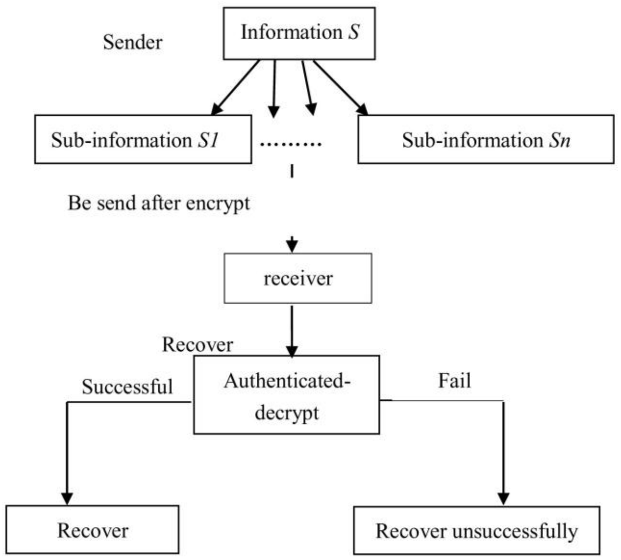

Figure 1 Information distribution & refactoring

III. ANALYSIS OF RESULTS AND TESTING OF MODELING

3.1 Information verification of all information fragments before reconstruction

3.1.1 Distribution of the fragment information

Step1. Assume S is number 11, that is, $S = A_0 = 11$. Let $n = 6, k = 3$, and the receivers is $A = \{A_1, A_2, A_3, A_4, A_5\}$ from a finite field. According to the improved Shamir scheme, The key management center P_0 randomly takes two numbers in a finite field because the threshold is 3. For example, $a_2 = 2, a_1 = 7$. So we get a quadratic polynomial.

$$g(x) = 2x^2 + 7x + 11$$

Remark This polynomial is the polynomial information to be recovered later. So it needs to be kept secret.

Step2. Put $x_1 = 1,\ x_2 = 2,\ x_3 = 3,\ x_4 = 4,\ x_5 = 5$, and calculate out $g(x_i)$.

$$\begin{cases} y_1 = g(x_1) = g(1) = 20 \\ y_2 = g(x_2) = g(2) = 33 \\ y_3 = g(x_3) = g(3) = 50 \\ y_4 = g(x_4) = g(4) = 71 \\ y_5 = g(x_5) = f(5) = 96 \end{cases}$$

Step3. As the sub information, according to *RSA* Algorithm, $(1,20),\ (2,33),\ (3,50),\ (4,71),\ (5,96)$ are encrypted to the secret text by MATLAB

ɖʜʂǬ , Ñɛſſ , Ÿ,¥ᵥ, Ǔωǘ, ʼnôΣʂ

Step4. Sending the secret text.

3.1.2 Authentication and fragmentation information reconstruction

When restoring information, it is need to verify the identity first. The process of authentication is as follows.

Step1. According to *RSA* Algorithm, by MATLAB, one can decrypt the secret text to $(1,20), (2,33), (3,50), (4,71), (5,96)$.

Step2. Put them in to the polynomial

$$f(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3 + A_4 x^4$$

separately. One can obtain a system of linear equations

$$\begin{cases} A_0 + A_1 + A_2 + A_3 + A_4 = 20 \\ A_0 + 2A_1 + 4A_2 + 8A_3 + 16A_4 = 33 \\ A_0 + 3A_1 + 9A_2 + 27A_3 + 81A_4 = 50 \\ A_0 + 4A_1 + 16A_2 + 64A_3 + 256A_4 = 71 \\ A_0 + 5A_1 + 25A_2 + 125A_3 + 625A_4 = 96 \end{cases}$$

Solve the linear equations, five coefficients $A_0 = 11,\ A_1 = 7,\ A_2 = 2,\ A_3 = 0,\ A_4 = 0$ are gotten. Therefore, the interpolation function is

$$f(x) = 11 + 7x + 2x^2.$$

So, the original secret information is 11.

3.2 Reconstruction from partial fragment information

Using arbitrary K information fragments, for example $K=3$, $n=6$, $t=3$, one can get

$f(1)=20$, $f(3)=50$, $f(5)=96$.

Assume that $f(x)=A_0+A_1x+A_2x^2$, then

$$\begin{cases} f(1)=A_0+A_1+A_2=20 \\ f(2)=A_0+3A_1+9A_2=50 \\ f(5)=A_0+5A_1+25A_2=96 \end{cases}$$

So $A_0=11, A_1=7, A_2=2$. Thus $S=A_0=11$.

Based on Shamir secret threshold scheme, RSA key is used to encrypt the sub-information to ensure the confidentiality of the information. When authenticating, the publisher encrypts the sub-information with another public key, and the receiver decrypts the private key to verify the identity and ensure the recipient's identity. Verification of sub-information before information restoration can ensures that every sub-information in the process of original information recovery is correct or found the incorrect sub-information. Using examples to test the model, the results obtained are the same as the model's explanations, which proves that the model is reasonable.

IV. MODELLING EVALUATION AND PROMOTION

4.1 Advantages of the modeling

1) Based on the (K,N) threshold key sharing scheme proposed by Shamir, the model in this paper is improved by adding the process of verifying the identity of the sub-information holder to reduce the risk of the sub-information being stolen by others.

2) The whole polynomial can be determined by any k secret shares, and other secret shares can be calculated.

3) In the case that the original shared key is not exposed, by constructing a $k-1$ polynomial with new coefficients whose constant term is still the shared key, the secret share of the new round sharer can be recalculated, thus the original secret share can be invalidated and the secret leakage can be prevented.

4) RSA algorithm is a mature algorithm in public key mechanism. It is based on the theory of "large number decomposition and prime data detection". It is easy to realize the multiplication of two large prime numbers on a computer. But the calculation of the two prime factors is quite large, which can not be realized even on a computer. This ensures the security of RSA algorithm. No one will steal the specific content of sub-information even if sub-information is stolen.

4.2 Disadvantages of the modelling

If the polynomial modelling is not complicated enough, it will be easy to be cracked by others. So it should be as complex as possible when selecting the interpolation function.

4.3 Promotion of modelling

In the era of big data, it is especially important to protect information security. Aiming at how to guarantee information security, this paper improves the original threshold model, which has a certain reference value for information security issue and information security reorganization. For secret sharing, this scheme has good security. As an important branch of modern cryptography, the direction of secret function can effectively guarantee the security of information, and plays a key role in the security preservation, transmission and legitimate use of important information and secret data, which has become a research hotspot in the field of information. In addition, this paper's "sub-information" holder authentication process has a certain role in preventing secret theft and other situations, and can improve the security of the system.

V. REFERENCES

[1] **Shamir A.** Identity-based cryptosystems and signature schemes[C]. Proceeding of CRYPTO 84, Lecture Notes in Computer Science, Springer-Verlag, 1984, 196: 47-53.

[2] **Ito M, Saito A, Nishizeki T.** Secret sharing scheme realizing general acess structure[C]. Proceeding of GLOBECOM 87, Tokyo Japan, 1987: 99-102.

[3] **Chunpong Lai, Cunsheng Ding.** Several Generalizations of Shamir's Secret Sharing Scheme[J]. International Journal of Foundations of Computer Science, 2004, 15(2): 445-458.

[4] **Ham L.** Efficient sharing (broadcasting) of multiple secrets[J]. IEE Proceedings-Computers and Digital Techniques, 1995, 142(3): 237-240.

[5] **Juan Qu , Limin Zou , Jianzhong Zhang.** A practical dynamic multi-secret sharing scheme[C]. IEEE International Conference on Information Theory and Information Security, 2010.

[6] **Jia Li.** Analysis and realization of public key cryptosystem of RSA algorithm[J]. Science Mosaic, 2012, 08: 21-24. (in Chinese)

[7] **Ruchun Fei.** Cryptographic application of one-way functions[J]. Journal of Liaoning Institute of Science and Technology, 2017, 19(01): 1-3. (in Chinese)

[8] **Liaojun Pang, Yumin Wang.** A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing[J]. Applied Mathematics and Computation, 2005, 167(2): 840-848.

[9] **Mulan Liu.** Secret Sharing Schemes and Secure Multi-party Computation[J]. Journal of Beijing Electronic Science and Technology Institute, 2006, 14(4): 1-8. (in Chinese)

[10] **Mustafa Ulutas, Guzin Ulutas, Vasif V.** Nabiyev. Medical image security and EPR hiding using Shamir's secret sharing scheme[J]. Journal of Systems and Software, 2011, 84(3): 341-353.

[11] **Yanxiao Liu.** Research of (k, n) Threshold Secret Sharing Technology[D]. XiDian University, 2012. (in Chinese)

[12] **Guohua Chen, Chengdong Wei.** Mathematical models and mathematical modeling method [M]. Tianjin: Nankai University Press, 2012. (in Chinese)

[13] **Huan Zhang.** Reasearch and Application of Sharing Scheme Based on Threshold[D]. Lanzhou University of Technology, 2013. (in Chinese)

[14] **Shoukui Si, Xiqing Sun.** Mathematical Modeling[M]. Beijing: National Defence Industrial Press, 2014: 351-353. (in Chinese)

******