Computer and Information Science

www.ccsenet.org/journal.html

Vol. 2, No. 3

August 2009

Study on the Multiple-Key-Pair Generation Scheme Based on Grey Half-generation

Peng Li, Yulian Shang, Jifeng Wang & Yufei Zhang

College of Information Engineering, Taishan Medical University, Tai'an 271016, China

Abstract

The generation of the multi-key-pair in the RSA iterative encryption system was studied, and from the generation algorithm of key, a sort of multi-key-pair generation scheme was proposed in the article. In the scheme, the encryption key set and the decryption key set used in the encryption system were managed by the improved half-generation algorithm, and the management scheme that one secrete key was used to generate multiple key pairs could solve the difficult management problem for multiple key sets. Finally, the key generation algorithm was simulated by VB6.0 in the article.

Keywords: Iterative encryption, Key Management, Grey half-generation, Key generation

1. Introduction

The key safety is the key factor to ensure the safety of the encryption system, and the key is the core of the whole cipher system, so the safety of the key must be guaranteed. The key generation is the base of the key management, and it is one factor to directly influence the safety of the key, and one important part in the encryption system. Yulian Shang et al studied the RSA encryption system and gave a sort of iterative encryption scheme based on RSA which acquired better encryption effect in their article (Shang?, 2008, P.120-124). However, in that iterative encryption system, large numbers of encryption key sets and encryption key sets would be used, and their article didn't describe how to manage these key sets. In addition, in the RSA key generation, the effective method to generate any big random number has not been found. Based on the grey system theory (J.L. Deng, 1982, P.285-294 & J.L. Deng, 1989, P.1-24), the superset theory and the data generation technology, literatures (J.L. Deng, 1989, P.1-24 & K.Q. Shi, 2000, P.331-340 & T.S. Chen, 2001, P.57-64 & K.Q. Shi, 2000, P.215-224 & T.S. Chen, 2000, P.255-262) offered the concept of grey encryption, and the grey half-generation algorithm was proposed in this encryption system. Based on the grey half-generation algorithm, a sort of new parameter set (big prime number) generation scheme was proposed, which could improve the generation of the key set and enhance the safety of the key. The grey half-generation algorithm was proposed by Professor K.Q. Shi in the grey encryption system theory, and in the article, above algorithm would be improved. In the former grey differential equation, $z^{(1)}$ and $x^{(0)}$ are the neighboring average generation sequence $z^{(1)}(k)=0.5x^{(1)}(k)+0.5x^{(1)}(k-1)$ ($k=2,3,\cdots,n$), and in the article, the general form was adopted, i.e. $z_k^{(1)}=(1-\alpha)x_k^{(1)}+\alpha x_{k-1}^{(1)}$ ($k=2,3,\cdots,n$). And because of $\alpha=\frac{1}{a}-\frac{1}{(e^a-1)}$, $z_k^{(1)}$ changes according to the values of α, and the iterative method is adopted to confirm the grey half-generation set. The research result indicated that the algorithm could enhance the safety of the key.

2. Grey half-generation algorithm (J.L. Deng, 1989, P.1-24 & K.Q. Shi, 2000, P.331-340 & T.S. Chen, 2001, P.57-64 & K.Q. Shi, 2000, P.215-224 & T.S. Chen, 2000, P.255-262)

The correlative concept about the grey half-generation will be defined as follows, and it is the base of the grey encryption theory.

Definition 1: Supposes both sides of the encryption communication select one initial sequence *x*, *x* is the sequence composed by positive integers.

$$x=\{x_1,x_2,\cdots,x_n\} \tag{1}$$

$|x|\geq 4$, $\forall x_i\in N^+, i=1,2,\cdots,n$, $n\geq 4$, so the sequence *x* is called as the key seed sequence, *x* is secret.

Definition 2: Call $x^{(1)} = \{x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}\}$ is the 1-AGO generation data sequence of *x*, and if

$$x_{(k)}{}^{(1)} = \sum_{j=1, x_j \in x}^{k} x_j; \quad k = 1,2,\cdots n \tag{2}$$

Suppose $x^{(0)}$ is the non-negative sequence, $x^{(1)}$ is the 1-AGO sequence of $x^{(0)}$, $z^{(1)}$ is the neighboring average generation sequence of $x^{(0)}$, $(a,b)^T = (B^T B)^{-1} B^T Y$, the definitions of parameters are seen in reference articles (J.L. Deng, 1989, P.1-24 & K.Q. Shi, 2000, P.331-340 & T.S. Chen, 2001, P.57-64 & K.Q. Shi, 2000, P.215-224 & T.S. Chen, 2000, P.255-262).

Definition 3: The complete solution of the grey differential equation $x^{(0)}(k) + az^{(1)}(k) = b$ is

$$\hat{x}_{k+1}^{(1)} = (x_1^{(1)} - \frac{b}{a})e^{-ak} + \frac{b}{a} \tag{3}$$

Definition 4: The half-solution of the grey differential equation $x^{(0)}(k) + az^{(1)}(k) = b$ is

$$\bar{x}_{k+1}^{(1)} = (x_1^{(1)} - \frac{b}{a})e^{-ak} = \beta e^{-ak}, \quad k = 1,2,\cdots,n \tag{4}$$

Obviously, if $k = 1,2,\cdots,r$, from (4), the data sequence $\bar{X}^{(1)}$ can be obtained.

$$\bar{X}^{(1)} = \{\bar{x}_1^{(1)}, \bar{x}_2^{(1)}, \cdots, \bar{x}_r^{(1)}\} \tag{5}$$

Because above definitions are based on the grey model *GM (1,1)*, so they are respectively called as grey complete solution generation and grey half solution generation.

Definition 5: Suppose x'' is the half-solution key set of the grey encryption system, and

$$x'' = \{x_1'', x_2'', \cdots, x_r''\} \tag{6}$$

Where, $x_i'' = x_i' \bmod p$, p is one big prime number selected randomly, $\forall \bar{x}_i^{(1)} \in \bar{X}^{(1)}$, $x_i' = INT(\bar{x}_i^{(1)})$, $i = 1,2,\cdots r$, and *INT* is the operator of Int.

3. Multi-key-pair generation scheme based on grey half-generation

3.1 Key generation scheme

Iterative encryption algorithm established by Yulian Shang et al (Shang, 2008, P.120-124) based on RSA enhanced the safety of the key, and the key generation algorithm would be studied in the article. When generating the key in the RSA system, the selections about correlative parameters such as the big prime number *p* and *q* are the necessary condition to generate the key set. Based on the grey half-solution generation algorithm, a new parameter set (big prime numbers) generation scheme would be proposed as follows, which could improve the generation of the key set and enhance the safety of the key. The concrete generation algorithm of the parameter set (selecting prime parameters) includes following steps.

Convention: Both sides of the encryption communication are A and B, and A is the sender and B is the receiver. Both A and B should first generate their respective key set before the communication.

3.1.1 Selecting data column

Both A and B respectively select one data sequence *x* as the key seed sequence, i.e. $x = \{x_1, x_2, \cdots, x_n\}$, $|x| \geq 4$, and the sequence is secret. The data sequence *x* can be composed by the birth date, telephone number, or correlative biological characters (such as fingerprint or eye iris) about the identity signs.

3.1.2 Confirming 1-AGO data column

Solve the 1-AGO generation data sequence $x^{(1)}$ of x according to the formula (2), where, $x^{(1)} = \{x_1^{(1)}, x_2^{(1)}, \cdots, x_n^{(1)}\}$ and

$$x^{(1)} = \sum_{j=1, x_j \in x}^{k} x_j, \quad k = 1,2,\cdots n.$$

3.1.3 Confirming grey half-generation set

From above theory introduction, according to the data sequence x, $x^{(1)}$ and definition 1~definition 5, the half-solution set $\overline{x}_{k+1}^{(1)} = (x_1^{(1)} - \frac{b}{a})e^{-ak} = \beta e^{-ak}$ ($k = 1,2,\cdots,n$) of the grey differential equation $x^{(0)}(k) + az^{(1)}(k) = b$ can be confirmed.

The least-square estimation parameter sequence $\hat{a} = (a,b)^T$ of the grey differential equation $x_k + az_k^{(1)} = b$ could fulfill

$$\hat{a} = (B^T B)^{-1} B^T Y$$

$$Y = \begin{bmatrix} x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}, \quad B = \begin{bmatrix} -z_2^{(1)} & 1 \\ -z_3^{(1)} & 1 \\ \vdots & \vdots \\ -z_n^{(1)} & 1 \end{bmatrix}.$$

Here, based on the modeling mechanism and the application condition of *GM* (1,1), the scheme will improve the above algorithm. In the grey differential equation, $z^{(1)}$ is the neighboring average generation sequence $z^{(1)}(k) = 0.5x^{(1)}(k) + 0.5x^{(1)}(k-1)$ ($k = 2,3,\cdots,n$) of $x^{(0)}$. In the article, the general form $z_k^{(1)} = (1-\alpha)x_k^{(1)} + \alpha x_{k-1}^{(1)}$ ($k = 2,3,\cdots,n$) is adopted. Because $\alpha = \frac{1}{a} - \frac{1}{(e^a - 1)}$, $z_k^{(1)}$ changes with the value of α, and the iterative method is adopted to confirm the grey half-solution set.

(1) From $z_k^{(1)} = (1-\alpha)x_k^{(1)} + \alpha x_{k-1}^{(1)}$, first take $\alpha = 0.5$, and replace it into the formula, i.e. $z_k^{(1)} = 0.5x_k^{(1)} + 0.5x_{k-1}^{(1)}$, and solve $z_k^{(1)}$;

(2) According to the method in formulas (4)~(7), solve the parameter sequence $\hat{a} = (a,b)^T$;

(3) Replace the parameter *a* into the expression $\alpha_{m-1} = \frac{1}{a} - \frac{1}{(e^a - 1)}$ to confirm the new value of α, and note it as α_{m-1};

(4) Replace the value of α into the expression $z_k^{(1)} = (1-\alpha)x_k^{(1)} + \alpha x_{k-1}^{(1)}$ to confirm the value of new $z_k^{(1)}$, and solve the value of the new parameter sequence $\hat{a} = (a,b)^T$. Repeat (1), (2) and (3) in turn.

(5) According to the iterative times set in advance, the solved parameter sequence $\hat{a} = (a,b)^T$ can be used to confirm the grey half-solution set $\overline{x}^{(1)} = \{\overline{x}_1^{(1)}, \overline{x}_2^{(1)}, \cdots, \overline{x}_r^{(1)}\}$.

3.1.4 Confirming parameter set and selecting big prime numbers *p* and *q*

Perform the Int operation to the grey half-solution set $\overline{x}^{(1)} = \{\overline{x}_1^{(1)}, \overline{x}_2^{(1)}, \cdots, \overline{x}_r^{(1)}\}$, and obtain the data sequence x', where, $\forall \overline{x}_i^{(1)} \in \overline{x}^{(1)}, x_i' = INT\left(\overline{x}_i^{(1)}\right)$ ($i = 1,2,\cdots r$), and *INT* is the operator of the Int operation. According to the formula (6), take an enough big prime number *p*, and solve the sequence $x'' = \{x_1'', x_2'', \cdots, x_r''\}$, where, $x_i'' = x_i' \bmod p$, i.e. the parameter set.

A and B respectively select two big prime numbers according to the conditions randomly from the parameter set x'', *p* and *q*, finally, generate the multi-key-set with iterative encryption by the key generation method based on the RSA cipher system.

3.2 Example of key generation

To explain the concrete implementation method and approach of the key pair generation algorithm, the following simple example is offered. The generation algorithm of the big prime number parameter set and the key set generation algorithm have been implemented by Matlab6.0 and VB6.0, and the key generation interface by the VB6.0 is seen in Figure 1.

The concrete implementation process includes following steps.

Step 1. The key seed sequence selected by any side of the encryption communication is *x*, $x = \{8,3,9,4,2,9,9\}$ (secret), and convenient for the computation, randomly select a seven bits data sequence as *x*;

Step 2. Seek the 1-AGO generation data sequence $x^{(1)}$ of the key seed sequence *x*, and obtain $x^{(1)} = \{8,11,20,24,26,35,44\}$;

Step 3. Replace data sequence x and $x^{(1)}$ into the following expressions,

$$Y = \begin{bmatrix} x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}, \quad B = \begin{bmatrix} -z_2^{(1)} & 1 \\ -z_3^{(1)} & 1 \\ \vdots & \vdots \\ -z_n^{(1)} & 1 \end{bmatrix}$$

Take $\alpha = 0.5$ to seek the parameter sequence, $\hat{a} = (a,b)^T$;

Compute and obtain a= -0.1475, b= 2.5080;

Replace a into the formula $\alpha_1 = \frac{1}{a} - \frac{1}{(e^a - 1)}$,

And obtain $\alpha_1 = 0.5123$ (without loss of generality, the iterative times is two in the example)

Step 4. According to the value of α_1, compute and obtain $a_1 = -0.1482$, and $b_1 = 2.4814$;

Replace values of a_1 and b_1, and $x_1^{(1)} = 8$ into $\bar{x}_{k+1}^{(1)} = (x_1^{(1)} - \frac{b}{a})e^{-ak} = \beta e^{-ak}$, takes values of k are $k = 1,2,\cdots,n$ (n is random) in turn, and perform the Int operation, and obtain the grey half-solution generation set x';

$$x' = \{29,33,39,45,52,60,70,81,94,109,126,147\cdots\}$$

Take any big prime number, *p*=347, and obtain the parameter data sequence $x'' = x' \bmod p$;

$$x'' = \{29,33,39,45,52,60,70,81,94,109,126,147\cdots\}$$

Step 5. In the parameter set x'', select any big prime number, *p*=29, *q*=94 (in actual application, the prime number test is needed);

Obtain one key pair:

Public key e=37, private key d=2041.

End.

4. Conclusions

Based on the grey half-generation algorithm, a sort of multi-key-pair generation scheme based on the RSA iterative encryption system is proposed in the article, and the scheme possesses following characteristics.

(1) The algorithm thought of the scheme can be described as follows. In each key exchange and secret communication, both sides of the encryption communication select one secret key (secret key seed sequence) to randomly generate t encryption key sets and decryption key sets used in the encryption communication. Each encryption can replace key seed sequence and multi-key-pair, and from certain meaning, this scheme is closed to one-time-one-encryption, and its encryption performance and safety are higher than general cipher system. The key is established only when it is needed, and it is not necessary to be stored, or else, which will bring the exposed danger. That is obviously advanced for the key generation mode.

(2) When the algorithm is used to generate the key, one random key seed sequence (private key) needs to be stored or selected temporarily, and the large-sized key set is not necessary to be managed, or the safety of KDC is not necessary to be worried, and this method makes the key more easily to be managed.

(3) The safety of the method that that the grey half-solution generation theory is used to generate the key parameter set is based on "the problem to solve the discrete logarithm", so the generation scheme of the multi-key-pair and the iterative encryption system is safe for the algorithm, and the key is safe.

(4) The algorithm of the scheme is safe, and it is difficult to get all t keys for the attackers of the cipher system, because the key seed sequence is secrete, and even if the grey half-solution algorithm is known, the key can not be obtained. If the grey half-solution set is leaked by certain reason, it is still impossible to deduce key seed sequence from the half-solution key set, because its difficulty equals to "solve the problem of discrete logarithm", and the elements in the key set is infinite ($n \in N$), and p is the enough big prime number which can be selected randomly, and the possibility that the cipher attackers want to find the big prime number used in the generation of the key parameter set. Therefore, it is safe to adopt this algorithm to generate the key, and the safety of the key can be guaranteed.

References

J.L. Deng. (1982). Control Problems of Gray System. *Systems and Control Letters.* No.1(5). P.285-294.

J.L. Deng. (1989). Introduction to Gray System Theory. The Journal of Grey System. No.1(1). P.1-24.

K.Q. Shi & T.S. Chen. (2000). A Grey General Lock and Central Public Cryptosystem (I). *The Journal of Grey System.* No.12(4). P.331-340.

K.Q. Shi & T.S. Chen. (2000). On the Grey Encryption Problems of Information Security (I). *The Journal of Grey System.* No.12(3). P.215-224.

Yulian Shang, Wuyuan Jia & Peng Li etc. (2008). Study on the Scheme for RSA Iterative Encryption System. *Computer and Information Science.* No.1(3). P.120-124.

T.S. Chen & K.Q. Shi. (2001). A Grey General Lock and Central Public Cryptosystem (II). *The Journal of Grey System.* No.13(1). P.57-64.

T.S. Chen & K.Q. Shi. (2000). On the Grey Encryption Problems of Information Security (II). *The Journal of Grey System.* No.12(3). P.255-262.

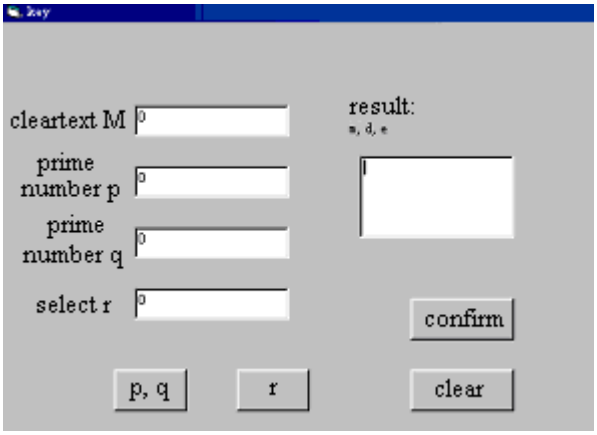

Figure 1. Key Generation and Parameter Selection