Application of the Central Encryption System in the Dynamic Secret Sharing Scheme (II)

Yulian Shang, Min Feng & Peng Li

College of Information Engineering, Taishan Medical University, Taian 271016, China

Kaiquan Shi

School of Mathematics and System Sciences, Shandong University, Jinan 250061, China

Abstract

Based on the simple introduction of the multi-teeth encryption-decryption algorithm (Shang, 2010, P.1500-1502.), a dynamic secret sharing scheme based on the multi-teeth central encryption system is proposed in this article. In this research, for any K system members $B=\{B_1,B_2,\cdots,B_k\}$, they respectively select the positive integer in the set of $X_{B_i}=\{x_{i1},x_{i2},\cdots,x_{im}\}$ distributed randomly, and $i=1,2,\cdots,k$, and X_{Bi} is opened. By P <*G, X,* X'>, any *l* (or more) B_i could reconstruct the shared secret key, and $k,l\in N, l\le k$. The result indicates that the scheme proposed in this article has good characteristics of security and encryption.

Keywords: Generation lock, Central encryption system, Secret sharing scheme, Multi-teeth encryption-decryption algorithm

1. Introduction

In 1979, Shamir and Blakley independently proposed the concept of secret key decentralization (Shamir, A, 1979, P.612-613 & Backly, G. R, 1979), and the mechanism implementing this idea was called as the (*t*, *n*)-threshold scheme. In two schemes, one secret key (the secret key of the system) was divided into n parts (n sub-secret keys) respectively kept by n persons, and for certain integer *t*(*t*<*n*), it fulfills (1) in these n persons, any r $(r\ge t)$ persons could cooperate to recovery the private key of the system; (2) any r $(r\ge t)$ persons could offer little help to recovery the private key of the system. This idea of private key decentralization makes the private key management more safe and flexible. After the idea of the (*t*, *n*)-threshold was proposed, many scholars proposed many schemes to implement it. At present, except of the management of secret key, it has been applied in other domains of cryptology such as signature and group attestation (Du, 2009, P.21-23).

The grey system theory was proposed by the famous scholar of China, Professor Deng Julong, in 1982 (J. L. Deng, 1982, P.285-294 & J. L. Deng, 1989, P.1-24). In 2000, Professor Shi Kaiquan integrated the extension sets theory, the grey system theory and the data generation technology, and proposed a new public encryption system, i.e. the grey encryption system, and gave the frame characteristics and the encryption-decryption algorithm of this encryption system (K. Q. Shi, 1994, P.121-124 & K. Q. Shi, 2000, P.331-340 & T. S. Chen, 2001, P.57-64 & K. Q. Shi, 2000, P.215-224 & K. Q. Shi, 2000, P.255-262). In this article, by successfully applying the multi-teeth encryption-decryption algorithm in the grey encryption system in the secret key sharing, a dynamic secret sharing scheme based on the multi-teeth central encryption system was proposed, and the result indicates that the scheme proposed in this article has good characteristics of security and encryption.

2. Prepared concepts (K. Q. Shi, 1994, P.121-124 & K. Q. Shi, 2000, P.331-340 & T. S. Chen, 2001, P.57-64 & K. Q. Shi, 2000, P.215-224 & K. Q. Shi, 2000, P.255-262)

Supposing that $X=\{x_1,x_2,\cdots,x_n\}$ $n\ge 4$ is the set distributed without rules, $X^*=\{x_1{}^*,x_2{}^*,\cdots,x_n{}^*\}$ $\forall x_j{}^*\in R^+$, is the 1-AGO generation set of X, X^* forms one poly-line $<X>$, so the index curve

$$\hat{x}(k+1)=(x_1-\frac{u}{a})e^{-ak}+\frac{u}{a} \tag{1.1}$$

, exists and approaches to the poly-line $<X>$.

The parameters *a*, *u* in the formula (1.1) are confirmed by

$$\begin{pmatrix} a \\ u \end{pmatrix}=(B^TB)^{-1}B^TY_N \tag{1.2}$$

$$B=\begin{bmatrix} -\frac{1}{2}(x_1{}^{*}+x_2{}^{*}) & 1 \\ -\frac{1}{2}(x_2{}^{*}+x_3{}^{*}) & 1 \\ \vdots & \vdots \\ -\frac{1}{2}(x_{n-1}{}^{*}+x_n{}^{*}) & 1 \end{bmatrix}, \quad Y_N=\begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix}$$

For $k=1,2,\cdots,p$, the real number set $X'=\{x'_1,x'_2,\cdots,x'_p\}$ could be confirmed by the formula (1.1), and X' is called as the extension set of X generated by the formula (1.1).

Proposition 1: The poly-line $<X>$ composed by the set X^{*} has similar index rule, and the converse is also true.

Proposition 2: For the model (1.1), the set X' exists, and it is generated by the formula (1.1).

Theorem 1.1 (non-reversible theorem): The model (1.1) is noted as $\mathsf{P}<G,X,X'>$, $\mathsf{P}<G,X,X'>(X)$ and $\mathsf{P}<G,X,X'>(X')$ respectively are the conversion of $\mathsf{P}<G,X,X'>$ about the set X and the conversion of $\mathsf{P}<G,X,X'>$ about the set of X', so

$$\mathsf{P}<G,X,X'>(X)\neq \mathsf{P}<G,X,X'>(X') \tag{1.3}$$

The meaning of the theorem: If X' is defined as the cryptograph encrypted by A, and X' is stole, the clear-text X of A could not be obtained by $\mathsf{P}<G,X,X'>$.

Theorem 1.2 (Extension and deduction non-equivalence theorem): For the model (1.1), x'_i,x'_j are extension values of the model (1.1) at the point of (i, j), and if $i\neq j$, so

$$x'_i\neq x'_j \tag{1.4}$$

$$x'_i,x'_j\in R^{+},i,j\in(1,2,\cdots,r)$$

Proposition 1 and 2, and Theorem 1.1 and 1.2 are mathematical facts obviously.

3. Generation lock $\mathsf{P}<G,X,X'>$ and multi-teeth central encryption system

Because of the limitation of the length, some prepared concept about the multi-teeth central encryption system are introduced as follows, and detailed encryption and decryption algorithms are seen in relative literatures (K. Q. Shi, 1994, P.121-124 & K. Q. Shi, 2000, P.331-340).

To ensure the safety of information and prevent bad men's cracking and attack to the cryptograph C_k, the discussion in the former section will be extended as follows. In this section, X'_A is a non-unit element set $\{x'_i\}$, and $X'_A=\{x'_1,x'_2,\ldots,x'_\alpha\}$.

Theorem 2.1 (Digital Signature Uniqueness Theorem 1): Supposing that $\varphi<X,X'>$ is the key to open $\mathsf{P}<G,X,X'>$, and X , X' respectively are the rough and teeth set of $\varphi<X,X'>$, $|X'|$, $|X''|$ are two teeth numbers of the rough *X*, and if $|X'|\neq|X''$, $\forall\, m_k\in M$ fulfills

$$C_k\neq C'_k \tag{2.1}$$

Where, $C_k=X'\oplus m_k$, $C'_j=X''\oplus m_k$, C_k ,C'_k respectively are two digital signatures of the clear-text m_k.

Prove: For $X=\{x_1, x_2, \ldots, x_n\}$, $\forall\, x_j\in N^{+}$, $X'=INT\{x'_1, x'_2, \ldots, x'_p\}$, $X''=INT\{x''_1, x''_2,\ldots, x''_q\}$ (Backly, G. R, 1979 & Du, 2009, P.21-23 & J. L. Deng, 1982, P.285-294), and supposing $p<q$, p, $q\in N^{+}$, so $|X'|\neq|X''|$, and for same one $m_k\in M$,

$C_k=X'\oplus m_k\neq X''\oplus m_k=C'_k$.

For example, $|X'|=4$, $|X''|=7$, $X'=INT\{x'_1, x'_2, x'_3, x'_4\}=\{2,3,7,9\}$, $X''=INT\{x''_1, x''_2, x''_3, x''_4, x''_5, x''_6, x''_7\}=\{2,3,7,9,10,12,14\}$, $m_k=108$, so $X'\oplus m_k\neq X''\oplus m_k$, $C_k=\{2,3,7,9\}$

$\oplus \{108\} \neq \{2,3,7,9,10,12,14\} \oplus \{108\} = C'_k$. For appointed $|X'|$, the digital signature C'_k of the clear-text m_j is exclusive. The uniqueness of the digital signature is very important in the generation lock $\mathrm{P} < G, X, X' >$ and its central encryption system.

Theorem 2.2 (Digital Signature Uniqueness Theorem 2): Supposing that $\varphi < X, X' >$ is the key to open $\mathrm{P} < G, X, X' >$, X is the rough of $\varphi < X, X' >$, X', X'' are two teeth sets, $|X'|$, $|X''|$ are two teeth numbers of the rough X, and if $|X'| = |X''|$, $X' \neq X''$, $\forall\, m_k \in M$ fulfills

$$C_j \neq C'_j \tag{2.2}$$

Theorem 2.2 can be easily proved by the Theorem 2.1.

A and B respectively select the roughs X_A, X_B of $\varphi < X, X' >$, $X_A=\{x_1, x_2, \ldots, x_n\}$, $X_B=\{x_1, x_2, \ldots, x_m\}$, m, $n \geq 4$; $\forall\, x_i \in X_A$, $\forall\, x_j \in X_B$, x_i , $x_j \in N^+$, and X_A, X_B are opened. A and B respectively select the teeth numbers $|X'_A|$, $|X'_B|$, $X'_A=\{x'_1, x'_2, \ldots, x'_\alpha\}$, $X'_B=\{x'_1, x'_2, \ldots, x'_\beta\}$, of $\varphi < X, X' >$, M is the set of the clear-text m_j, $M=\{m_1, m_2, \ldots, m_t\}$. A is strictly secret for X'_A and B is strictly secret for X'_B.

4. Dynamic secret sharing scheme based on the multi-teeth central encryption system

The dynamic secret sharing scheme based on the multi-teeth central statistic encryption system is considered in this article, and the dynamic secret sharing scheme based on the multi-teeth central dynamic encryption system is similar.

Supposed that A is the manager of the secret key, $B = \{B_1, B_2, \cdots, B_k\}$ are k legal members of the system, and any l (or more) B_i could reconstruct the shared secret key, where, $k, l \in N, l \leq k$.

This scheme could be divided into following stages.

(1) The stage of system initialization

a. A, B_i respectively select the positive integer sets $X_A = \{x_1, x_2, \cdots, x_n\}$ and $X_{B_i} = \{x_{i1}, x_{i2}, \cdots, x_{im}\}$, where, $i = 1,2,\cdots,k$, X_A and X_{Bi} are opened.

b. The secret key manger A randomly selects k different elements $s_1, s_2, \cdots, s_k$, as the secret sub-secret key of B_i, and s_i is secretly transmitted to B_i ($i = 1,2,\cdots,k$) by the safe channel, at the same time, the interpolation polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1} \bmod p$ is constructed to fulfill $f(0) = a_0 = s$, where, S is the secret key kept by the system. Compute

$$y_i = f(C_i), i = 1,2,\cdots,k$$

Where, $C_i = \{ \underset{\substack{j=1,2,\cdots,m \\ x_j \in X_{B_i}}}{x_j} \} \oplus (\{ \underset{\substack{t=1,2,\cdots,\alpha_i \\ x'_t \in X'_A}}{x'_t} \} \oplus s_i)$

c. A opens the ordered array $y_1, y_2, \cdots, y_k$ on the bulletin board.

(2) The stage of secret key recovery

Supposing any l secret key holders ($B_1, B_2, \cdots\ B_l$) want to recovery the secret key of the system, and each member only needs to inquire y_i on the bulletin board, and uses his secret sub-key s_i to inquire α_i for A, and computes

$$C_i = \{ \underset{\substack{j=1,2,\cdots,m \\ x_j \in X_{B_i}}}{x_j} \} \oplus (\{ \underset{\substack{t=1,2,\cdots,\alpha_i \\ x'_t \in X'_A}}{x'_t} \} \oplus s_i)$$

, and puts in C_i. After collecting all (C_i, y_i), confirm $f(x)$ by the Lag-range interpolation polynomial $f(x) = \sum_{i=1}^{t} y_i \prod_{1 \leq j \leq t,\, j \neq i} \frac{x - C_j}{C_i - C_j}$ to recovery the system secret key $s = f(0)$.

5. Application of the dynamic secret sharing scheme based on the multi-teeth central encryption system

In the same way, supposing that A is the manager of secret key, B_1, B_2, B_3 are three legal members in the system, and any two of them could cooperate to reconstruct the shared secret key.

5.1 Stage of system initialization

(1) A, B_1, B_2, B_3 respectively select data sets $X_A = \{1,2,4,3\}$, $X_{B1} = \{2,7,1,4\}$, $X_{B2} = \{8,3,9,5\}$, $X_{B3} = \{2,9,5,3\}$; q=13, and $q, X_A, X_{B1}, X_{B2}, X_{B3}$ are opened.

(2) Secret manager A randomly selects three different elements, $(s_1, s_2, s_3) = (3,1,8)$, and secretly transmits s_i to B_i $(i = 1,2,3)$. Construct one interpolation polynomial $f(x) = 3 + 11x$, where, $f(0) =$ $a_0 = 3$ is the secret key kept by the system. So,

$X'_A = \{4,7,10,14,\cdots\}$

Supposing for A, $\alpha_1 = 2, \alpha_2 = 4,$ $\alpha_3 = 1$, so

$$C_1 = \{\underset{\substack{j=1,2,\cdots,4\\ j\in X_{B_1}}}{x_j}\} \oplus (\{\underset{\substack{t=1\ 2,\cdots,\alpha_i\\ x'_t\in X'_A}}{x'_t}\} \oplus s_1) = \{\underset{\substack{j=1,2,\cdots,4\\ j\in X_{B_1}}}{x_j}\} \oplus (\{\underset{\substack{t=1,2\\ x'_t\in X'_A}}{x'_t}\} \oplus s_1)$$

$$= (00000010,00000111,00000001,00000100) \oplus$$
$$\{(00000010,00000111\ 00001010) \oplus (00000011)\}$$
$$= (00001010) = 10$$

$$C_2 = \{\underset{\substack{j=1,2,\cdots,4\\ j\in X_{B_2}}}{x_j}\} \oplus (\{\underset{\substack{t=1,2,\cdots,\alpha_2\\ x'_t\in X'_A}}{x'_t}\} \oplus s_2) = \{\underset{\substack{j=1,2,\cdots,4\\ j\in X_{B_2}}}{x_j}\} \oplus (\{\underset{x'_4\in X'_A}{x'_4}\} \oplus s_2)$$

$$= (00000010,00000111,00000001,00000100) \oplus$$
$$\{(00000010,00000111\ 000001010\ 00001110) \oplus (00000011)\} \quad = (00000001) = 1$$

$$C_3 = \{\underset{\substack{j=1,2,\cdots,4\\ j\in X_{B_3}}}{x_j}\} \oplus (\{\underset{\substack{t=1,2,\cdots,\alpha_3\\ x'_t\in X'_A}}{x'_t}\} \oplus s_1) = \{\underset{\substack{j=1,2,\cdots,4\\ j\in X_{B_3}}}{x_j}\} \oplus (\{\underset{\substack{t=1\\ x'_t\in X'_A}}{x'_t}\} \oplus s_3)$$

$$= (00000010,00001001,00000101,00000011) \oplus \{(00000100) \oplus (00001000)\}$$
$$= (00000001) = 1$$

So,

$y_1 = f(C_1) = 47$

$y_2 = f(C_2) = 91$

$y_3 = f(C_3) = 14$

(3) A opens the ordered array $(y_1, y_2, y_3) = (47,91,14)$ on the bulletin board.

5.2 Stage of secret key recovery

Supposing any l secret key holders (B_1, B_2) want to recovery the secret key of the system, and they inquire y_1 47 , $y_2 = 91$ on the bulletin board, and inquire t_1 and t_2 for A, and use the secret sub-keys $s_1 = 3, s_2 = 1$ to obtain $C_1 = 4, C_2 = 8$, and then use the Lag-range interpolation polynomial

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1\le j\le t,\ j\ne i} \frac{x - C_j}{C_i - C_j}$$

to compute

To compute

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1\le j\le t,\ j\ne i} \frac{x - C_j}{C_i - C_j} = 47\frac{x-8}{4-8} + 91\frac{x-4}{8-4} = 3+11x \bmod 13$$

So the secret key of the system is $s = f(0) = 3$.

6. Discussions

Based on the grey encryption system, a new secret key sharing scheme is proposed in this article. Except for security and feasibility, this scheme also has following characteristics.

(1) The secret sub-key can be used many times.

When recovering the secret key, each member puts in

$$C_i = \{ \underset{\substack{j=1,2,\cdots,m \\ j \in X_{Bi}}}{x_j} \} \oplus (\{ \underset{x'_{t_i} \in X'_A}{x'_{t_i}} \} \oplus s_i)$$

, to screen the secret sub-key, and other members could not solve the secret sub-key s_i of B_i by C_i, i.e. each member's secret sub-key has not been opened because of the recovery of the system secret key and used continually.

(2) System updating

When it needs to change the system secret key because of certain cause, the system only needs to reselect one $(l-1)$-order multinomial $f'(x)$ to fulfill $f'(0) = s'$ (it is the new system secret key), and the new $(l-1)$-order multinomial $f'(x)$ could be used to update the ordered array $(y_1, y_2, \cdots y_k)$ on the bulletin board.

(3) Deleting or adding members

a. When new member joins, the system only needs randomly generate the secret sub-key s_{k+1} for the new member B_{k+1}, and adds one element y_{k+1} ($y_{k+1} = f(C_{k+1})$) in the ordered array $(y_1, y_2, \cdots y_k)$ on the bulletin board.

b. When deleting certain one member B_i, the system only needs to reselect one $(l-1)$-order multinomial $f'(x)$ to fulfill $f'(0) = s'$ (it is the new system secret key), and uses $(l-1)$-order multinomial $f'(x)$ to update the ordered array $(y_1, y_2, \cdots y_k)$ on the bulletin board, and here, the y_i (y_i is the original value of empty) needs not be computed, so the original sub-key s_i of B_i is inefficient.

(4) Updating individual secret sub-key

When the secret sub-key of certain one member B_i is told, the system only needs to redistribute the sub-key s'_i for this member, and reselect one $(l-1)$-order multinomial $f'(x)$ to fulfill $f'(0) = s'$, and uses new s'_i and $f'(x)$ to update the ordered array $(y_1, y_2, \cdots y_k)$ on the bulletin board, and other members' sub-keys need not to be modified.

References

Backly, G. R. (1979). Safeguarding Cryptographic Keys. In Proceedings of the National Computer Conference of AFIPS. [Online] Available: http://citeseer.nj.nec.com/contest/7527/0.

Du, Chaoyang, Kou, Yanan, Wang, Wei & Lu, Shan. (2009). A Design of Identify Authentication Model-Based of ECC Algorithm in Man-Net. *Control & Automation.* No.21. P.21-23.

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, et al. (1994). *Gray Information Relation Theory.* Taibei: Quan Hua science and Technology Press. Taipei, Taiwan. P.121-124.

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.

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

Shamir, A. (1979). How to Share a Secret. *Communications of the ACM.* No.22(11). P.612-613.

Shang, Yulian, Zhao, Xuejun & Song, Wuli. (2010). Study on Application of Central Public Cryptosystem in Dynamic Secret Sharing Scheme (I). *Application Research of Computers.* No.27(4). P.1500-1502.

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.