On the K-Q Lock Problems of Information Security

Kai-Quan Shi
Department of Automation Engineering,
Shandong University of Technolog
Jinan, Shandong 250061P.R. C

Tzer-Shyong Chen
Department of Computer Science and
Information Engineering, Da-Yeh University
112 Shan-Jeau Rd., Da-Tsuen, Chang-Hwa
51505 Taiwan, R.O.C.
arden@aries.dyu.edu.tw

Hai-Cheng Chu
Department of International Trade,
Feng Chia University

Shih-Lin Wen
Department of Electrical Engineering,
Da-Yeh University
112 Shan-Jeau Rd., Da-Tsuen, Chang-Hwa
51505 Taiwan, R.O.C.
r8703021@aries.dyu.edu.tw

Abstract

In this paper, a new concept called "K -Q lock" for ensuring the security of information is proposed. The nomenclature K(kaleidoscope)-Q(queer) lock is itself a combination of a lock and key, which filters the entry of information so that the authorization for information can be performed strictly.

There are three parts in the K-Q lock (<GM(1), $\dot{X}(1)$>, a $S_x(1)$). The GM(1) is an inside lock; the $\dot{X}(1)$, an outside lock; and $S_x(1)$, a secret key which is expressed as a function. The structures of the inside and outside lock s constitute two layers for distinguishing the passing objects. Therefore, the designer can transfer the threshold of entrance according to different demands such as objects or authorization to set up a lock and key in the K-Q lock. In other words, the range in the application of the security area becomes wider. The K-Q lock can produce an encryption ladder for a plaintext document automatically. By protecting the encr yption information from being attacked, the order of the encryption ladder accomplishes the necessary requirements for securit . In addition four new concepts are introduced:(1) a bearing-reproduction theorem, (2) a resolution and dispersion theorem, (3) a ladder encryption theorem , and (4) a ladder-climbi algorithm. These four offer the K -Q lock a more trustworthy support.

Keywords: K-Q lock, inside lock, outside lock, ladder encryption algorithm

1. Introduction

In computer communication systems, both computer cryptography and information security have become quite important requirements. An unauthorized user will not be able to access secret data which is well protected. In consideration of the advancement of computer networks and computer technologies in multi-user systems, sharing resources becomes urgent. Thus, the necessity for resource administration is becoming important in multi-user computer environments. In other words, onl through authorization can objects be accessed.

Thus, the K-Q Lock, which can be applied in information security, is presented in this paper. Before discussing the central topic (K-Q Lock) of this paper, it is necessary to introduce the grey system theory.

The grey system theory was proposed by Deng[1] in 1982, and further research [2] was done in 1989. This theory discusses data analysis mainly. Some might wonder if the above-mentioned theory can be applied to information security because it seems to be independent of security and belong to a different field of research. Howe ver, the fact is that the use of grey theory can induce a new encryption and decryption method for securing information in computers.

The focal points concerning the K-Q Lock in this paper are listed below

1. First, grey theory is applied to computer communi-cation and information security.
2. Secondly, the structures and characteristics of the K -Q Lock are introduced.
3. Finally, several methods for unlocking the K-Q Lock and decrypting the information.

Briefly speaking, the K -Q Lock is provided with the followin characteristics: Bearing-reproduction, indepen-dent encryption and decryption, and high security. So far, no one has attempted to apply the grey system theory to information security.

In the next section, several preparatory concepts about grey system research are presented. The K-Q lock (<GM(1), $\dot{X}(1)$)>, and $S_x(1)$) will be introduced in Section 3. The encryption ladder and its structure are described in Section 4. Section 5 describes the encryption criterion for the ladder and ladder encryption algorithm. Section 6 describes the opening of the K -Q Lock. A discussion of the K-Q lock appears in Section 7. Section 8 presents the conclusions.

2. Several Preparatory Concepts

In this section, the relative concepts of the grey system theory are first introduced.

Definition 2.1

A finite nonnegative real number set
$X^{(0)}=\{x^{(0)}(1), x^{(0)}(2), \dots, x^{(0)}(n)\}$ (2.1)

is the basic set of the GM(1,1) model of the grey system, $\forall x^{(0)}(k)\in R^{+}, k\in(1,2,\cdots,n)$.

Definition 2.2

A finite nonnegative real number set

$$X^{(1)}=\{x^{(1)}(1), x^{(1)}(2), \ldots, x^{(1)}(n)\} \tag{2.2}$$

is the set which can be taken to generate GM(1,1) while $X^{(1)}$ conforms to 1-AGO (Accumulated generating operation)

$$\forall x^{(1)}(k)\in X^{(1)}, x^{(1)}(k)=\sum_{i=1}^{k} x^{(0)}(i) \tag{2.3}$$

Note: Therefore, $X^{(1)}$ is called the1-AGO of $X^{(0)}$ in the grey system theory. From definition 2.1 and 2.2, one obtains the following characteristics:

1. Through 1-AGO in the sequence $X^{(0)}=\{x^{(0)}(1), x^{(0)}(2), \cdots, x^{(0)}(n)\}$ that is irregularly distributed, one can obtain a data sequence $X^{(1)}=\{x^{(1)}(1), x^{(1)}(2), \ldots, x^{(1)}(n)\}$. However, the new sequence increases regularly.
2. $X^{(0)}$ and $X^{(1)}$ have the same cardinal number; that is $|X^{(0)}| = |X^{(1)}|$ (2.4)
3. Suppose that $X^{(1)}$ is defined as a broken line< $X^{(1)}$>, <$X^{(1)}$> obtains a closed value corresponding to the exponential regular under the solution αe^{x} of one-order differential equation.

Definition 2.3 One calls

$$\frac{dX^{(1)}}{dt}+aX^{(1)}=u \tag{2.5}$$

the shadow equation of the grey differential equation. The solution of (2.5)

$$\hat{X}^{(1)}(k+1)=\left(x^{(0)}(1)-\frac{u}{a}\right)e^{-ak}+\frac{u}{a} \tag{2.6}$$

is regular for the broken line <$X^{(1)}$>.

In the above, $\begin{pmatrix} a \\ u \end{pmatrix}=\left(B^{T}B\right)^{-1}B^{T}Y_{N}$ (2.7)

$$B=\begin{bmatrix} -\frac{1}{2}\left(x^{(1)}(1)+x^{(1)}(2)\right) & 1 \\ -\frac{1}{2}\left(x^{(1)}(2)+x^{(1)}(3)\right) & 1 \\ \vdots & \vdots \\ -\frac{1}{2}\left(x^{(1)}(n-1)+x^{(1)}(n)\right) & 1 \end{bmatrix} \tag{2.8}$$

$$Y_{N}=\left(x^{(0)}(2),x^{(0)}(3),\cdots,x^{(0)}(n)\right)^{T} \tag{2.9}$$

Definition 2.4

Suppose that k=1, 2, ..., p. One can then obtain the following sequence from (2.6):

$\dot{X}^{(1)}=\{x^{(1)}(2), x^{(1)}(3), \ldots, x^{(1)}(p+1)\}$, $\forall x(k)\in R^{+}$, (2.10)

in which $\dot{X}^{(1)}$ is a set generated by (2.6) .

In order to maintain consistency in symbols throughout the entire paper, the symbols of function are unified. Henceforth, equation (2.6) means GM(1), which is a model of $X^{(1)}$, and $\dot{X}^{(1)}$ represents $\dot{X}(1)$. For example, in (2.9), $\dot{X}^{(1)}=\{x^{(1)}(2), x^{(1)}(3), \ldots, x^{(1)}(p+1)\}$can be rewritten as $\dot{X}(1)=\{x(1), x(2), \cdots, x(p)\}$. These new symbols appear in the following sections repeatedly.

From Fig.1, One observes that $\dot{X}(1)$ is obtained through GM(1) under an extrapolation method at point k, k=1,2,...,p.

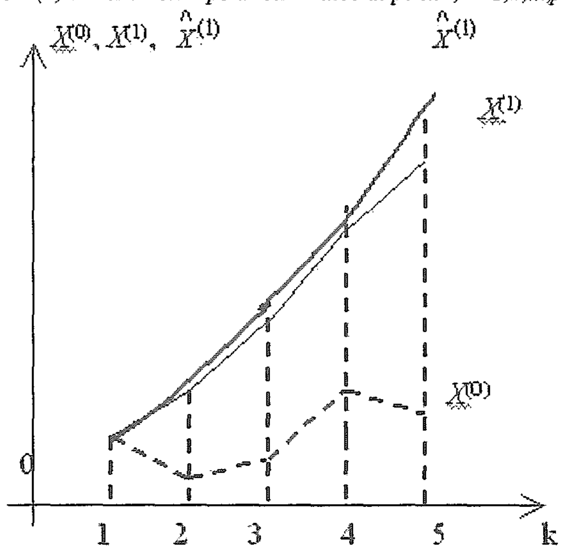

Fig.1. $X^{(0)}=\{x^{(0)}(1), x^{(0)}(2), \cdots, x^{(0)}(5)\}$, $\forall x^{(0)}(k)\in R^{+}$; $X^{(1)}$ is the 1-AGO generating set of $X^{(0)}$, $X^{(1)}=\{x^{(1)}(1), x^{(1)}(2), \cdots, x^{(1)}(5)\}$, $\forall x^{(1)}(k)\in R^{+}$. In the exponential curve, $\hat{X}^{(1)}$ is the solution to the first-order differential equation.

3. K-Q lock(<GM(1), $\dot{X}$ (1)>, and S_x(1))

Definition 3.1

For information security, an ordin al 3-element group (<GM(1), $\dot{X}$(1) >, and S_x(1)) is a 1-phase K-Q lock; GM(1) is a model formed b $X^{(1)}$, and $\dot{X}$ (1) is a set generated b GM(1) at point k=1,2, $\cdots$, p. In addition, S_x(1) is a function of $\dot{X}$ (1). In brief, a 1-phase K-Q lock is expressed as K-Q lock, and $X^{(1)}$ is the 1-AGO by the given $X^{(0)}$, and $|X^{(1)}|\geq 4$.

Definition 3.2

The term GM(1) is the inside lock and $\dot{X}$(1) the outside lock in the K-Q Lock (<GM(1), $\dot{X}$(1)>, and S_x(1)). The term S_x(1) is the key to the K-Q Lock (< GM(1), $\dot{X}$(1)>, and S_x(1)).

Definition 3.3

The term K-Q lock (<GM$^{(j)}$(1), $\dot{X}^{(j)}$ (1)>, and $S_x{}^{(j)}$(1)) is called the "bearing -reproduction lock" of the K -Q Lock (<GM (1) , $\dot{X}$(1)>, and S_x(1)) , GM$^{(j)}$ (1) is a bearin -reproduction inside lock of GM (1) and $\dot{X}^{(j)}$ (1) is a bearin -reproduction outside lock of $\dot{X}$(1). The term j here is a series of bearing-reproduction steps; j=1, 2, $\cdots$, q.

Theorem 3.1 (inside-lock unique existence theorem)

Suppose that $X^{(0)}$ is a finite nonnegative real number set, $X^{(1)}$ can be generated after 1-AGO of $X^{(0)}$, and $|X^{(0)}|\geq 4$, then the unique GM(1) will exist on $X^{(1)}$.The term GM(1) here is the inside lock of the K-Q lock.

Theorem 3.2 (outside-lock unique existence theorem)

Suppose that GM(1) is the inside lock of the K -Q lock, and N is a natural number set; then, $N=\{1, 2, \ldots, p\}$. In the process, one can obtain a unique set $\mathring{X}(1)$ through GM(1) and N. The term $\mathring{X}(1)$ is the outside lock of the K-Q lock.

Proof: In general, suppose that a finite nonnegative real number set $X^{(0)}=\{x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(n)\}$ is given. Then one can obtain $X^{(1)}=\{x^{(1)}(1), x^{(1)}(2), \ldots, x^{(1)}(n)\}$ through 1-AGO. Suppose that $n\geq 4$. One obtains GM(1) through (2.1)~(2.6). Suppose that N=1, 2, …, p, through GM(1). One obtains:

$$\mathring{X}(1)=\{x(2), x(3), \ldots, x(p+1)\} \tag{3.1}$$

Let $x(i)=x(i+1)$. Equation (3.1) can be rewritten as follows

$$\mathring{X}(1)=\{x(1), x(2), \ldots, x(p)\} \tag{3.2}$$

According to definition 3.2, it is clear that $\mathring{X}(1)$ is the outside lock of the K-Q Lock.

Theorem 3.3 (inside-lock generation theorem)

Suppose that $X^{(0)}$ is a finite nonnegative real number set, and $X^{(1)}$ can be generated after 1-AGO of $X^{(0)}$. In the process, shadow equation of the grey differential equation will generate the inside lock GM(1) of the K -Q Lock.

Theorem 3.4 (outside lock generation theorem)

Suppose that GM(1) is the inside lock of the K -Q Lock, Z is a natural number set, $Z\neq\{z\}$ and $\{z\}$ is a set of simple points. Then GM(1) and Z will generate the outside lock $\mathring{X}(1)$.

Theorem 3.5 (K-Q lock unique existence theorem)

Suppose that $X^{(0)}$ is a finite nonnegative real number set and $|X^{(0)}|\geq 4$, then The K -Q Lock (<GM(1), $\mathring{X}$ (1) >, and $S_x(1)$) is the unique existence.

Theorem3.6 (finite bearing-reproduction theorem of th K-Q Lock)

Suppose that T= {(<GM$^{(i)}$(1) , $\mathring{X}^{(i)}$(1)>, and $S_x{}^{(i)}$(1)) | i = 1, 2,···, q} is a bearing-reproduction set of (<GM(1), $\mathring{X}$(1) >, S_x(1)) and conforms to the following equation.

$$(\langle \mathrm{GM}^{(j)}(1), \mathring{X}^{(j)}(1)\rangle, S_x{}^{(j)}(1)) = \underset{j=1,2,\cdots q}{BR}(\langle \mathrm{GM}(1), \mathring{X}(1)\rangle, S_x(1)) \tag{3.3}$$

In the above equation, j is the bearing-reproduction step, and $\underset{j=1,2,\cdots q}{BR}$ is the abbreviation for bearing-reproduction.

Proof: According to definition 3.3, $\forall i\in(1, 2, \cdots, q)$, (<GM$^{(i)}$(1), $\mathring{X}^{(i)}$(1)> , and $S_x{}^{(i)}$(1)) is the K-Q Lock. The steps to obtain the K-Q Lock are as follows $Z=\{1,2,\cdots,p\}$, and if one lets $X^{(1)}=\mathring{X}^{(0)}(1)$. However, $\mathring{X}^{(0)}(1)$ is obtained b GM(1) and Z. GM$^{(1)}$(1) will exist on these points $X^{(1)}$, and GM$^{(1)}$(1) and Z generate $\mathring{X}^{(1)}(1)$. From definition 3.1, one knows that the K-Q Lock (<GM$^{(1)}$(1), $\mathring{X}^{(1)}$(1)>, and $S_x{}^{(1)}$(1)) is obtained through GM$^{(1)}$(1) and $\mathring{X}^{(1)}$(1). $S_x{}^{(1)}$(1) is the key of the K-Q Lock.

In a manner similar to the above -mentioned process, suppose that $X^{(2)}=\mathring{X}^{(1)}(1)$. One will obtain the K-Q Lock (<GM$^{(2)}$(1), $\mathring{X}^{(2)}$(1)>, and $S_x{}^{(2)}$(1)).Thus, $S_x{}^{(2)}$(1) is the key of the K-Q Lock (<GM$^{(2)}$(1), $\mathring{X}^{(2)}$(1)> , and $S_x{}^{(2)}$ (1)), ···, etc.. Suppose that $X^{(q)}=\mathring{X}^{(q-1)}(1)$, one obtains the K-Q Lock (< GM$^{(q)}$(1), $\mathring{X}^{(q)}$(1)>, and $S_x{}^{(q)}$(1)). Then, $S_x{}^{(q)}$(1) is the key of the K-Q Lock (<GM$^{(q)}$(1), $\mathring{X}^{(q)}$(1)>, and $S_x{}^{(q)}$(1)).

Theorem 3.6 introduces the K-Q Lock (<GM(1), $\mathring{X}$(1)>, and S_x(1)) has the characteristic of an organism' bearin -reproduction instinct. Equation (3.3) shows that all (<GM$^{(j)}$(1), $\mathring{X}^{(j)}$(1)>, and $S_x{}^{(j)}$(1)) is born-reproduced b (<GM(1), $\mathring{X}$(1)>, and S_x(1)). Such a characteristic as bearin -reproduction is quite important in encryption application. A series of relative keys thus can be produced in the same way.

From theorem 3.6, one concludes with the following propositions

Proposition 3.1 : Every element in P ={ GM$^{(j)}$(1)| j = 1,2,···,p} is the B-R inside the lock of GM(1).

Proposition 3.2: Every element in F={ $\mathring{X}^{(j)}$(1)| j =1,2,···, p is the B-R outside the lock of GM(1) and Z.

4. Encryption Ladder and Its Structure

Definition 4.1:

Suppose that X_1 and X_2 are finite nonnegative real-number simply ordered sets, $|X_1|=|X_2|$, and both X_1 and X_2 conform to the following equations:

1. $x_2(j)\in X_2$; $x_1(i)$, $x_1(i+1)\in X_1$, and these two relationships conform to: $x_1(i) \leq x_2(j) \leq x_1(i+1)$ (4.1)

2. $$\max_{\substack{i=1\\ x_1(i)\in X_1}}^{p}\left(x_1(i)\right) < \max_{\substack{j=1\\ x_2(j)\in X_2}}^{p}\left(x_2(j)\right) \tag{4.2}$$

Then, X_2 is called the "equal dimension ladder set" of X_1, or the "ladder set".

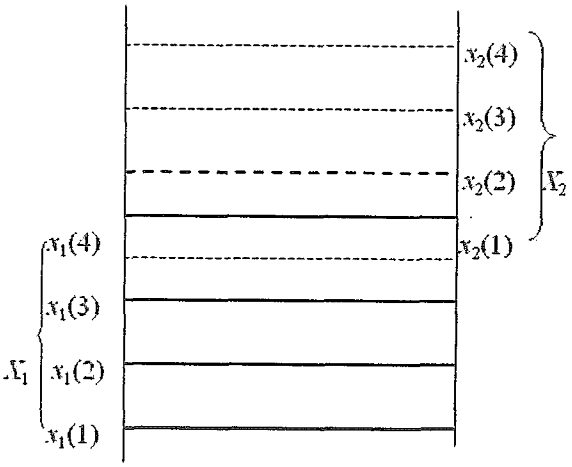

Fig. 2 Both X_1 and X_2 are nonnegative integer sets, X_1= { $x_1(1)$, $x_1(2)$, $x_1(3)$, $x_1(4)$ }={4, 7, 10, 14}, and X_2= { $x_2(1)$, $x_2(2)$, $x_2(3)$, $x_2(4)$ }={11, 21, 35, 54}, and $x_1(3) < x_2(1) < x_1(4)$. X_2 is a ladder set of X_1.

Example: For the sake of convenience in calculation, X_1 and X_2 are selected to be nonnegative integer sets. Suppose that $X_1 = \{ x_1(1), x_1(2), x_1(3), x_1(4) \} = \{4, 7, 10, 14\}$ and $X_2 = \{ x_2(1), x_2(2), x_2(3), x_2(4) \} = \{11, 21, 35, 54\}$; therefore, both X_1 and X_2 are simply ordered sets. Suppose that $X_1(3)$ and $X_1(4) \in X_1$, and $X_2(1) \in X_2$; the two such relationships will conform to $X_1(3)<X_2(1)<X_1(4)$ and $\overset{4}{\underset{i=1}{\max}}(x_1(i)) = x_1(4) < \overset{4}{\underset{i=1}{\max}}(x_2(i)) = x_2(4)$. Therefore, X_2 is the ladder set of X_1.

Definition 4.2

Suppose that $X_1, X_2, \ldots, X_q$ are finite real-number simply-ordered sets, $\forall i$, $|x_i| = \eta$, and η is a nonnegative integer. Incidentally, one calls $X_1, X_2, \ldots, X_q$ an equal dimensional q-th-order ladder $X^{\#}(1)$ which is named q-order ladder for short. It is expressed as follows

$$X^{\#}(1) = (X_1 \# X_2 \# \ldots \# X_q) \tag{4.3}$$

Suppose that X_t is the ladder set of X_{t-1}, $t=2, 3, \ldots, q$; then X_i is the i-th-order of ladder $X^{\#}(1)$; $i=1,2, \ldots,q$.

Definition 4.3

Suppose that both $X^{\#}(1)$ and $\mathring{X}^{\#}(1)$ are q-order ladders, $X^{\#}(1)=(X_1 \# X_2 \# \ldots \# X_q)$, and $\mathring{X}^{\#}(1)=(\mathring{X}_1 \# \mathring{X}_2 \# \ldots \# \mathring{X}_q)$. Then, $\#(1)$ is a q-order ladder generated by the combination of $X^{\#}(1)$ and $\mathring{X}^{\#}(1)$. The expressional model is as follows,

$$\#(1)=\{ \psi(1)_1 \# \psi(1)_2 \# \ldots \# \psi(1)_q\} \tag{4.4}$$

Suppose that $\mathring{X}_j$ is the ladder set of X_j; then $\psi(1)_j=(X_j \circ \mathring{X}_j)$ is the j-th-order of ladder $\#(1)$. The mark " $\circ$ " is the combination of X_j and $\mathring{X}_j$; $j=1, 2, \ldots, q$.

Definition 4.4

Suppose that $\psi(1)_i$ is the i-th-order of ladder $\#(1)$, and

$$\psi(1)_i=(X_i \circ \mathring{X}_i)_i \tag{4.5}$$

Then, X_i is called the behind or der and $\mathring{X}_i$ the future order in $\psi(1)_i$.

Theorem 4.1 (ladder order theorem of K-Q lock)

In the K-Q Lock $(<\mathrm{GM}^{(j)}(1), \mathring{X}^{(j)}(1)>$, and $S^{(j)}{}_x(1))$, both inside lock $\mathrm{GM}^{(j)}(1)$ and outside lock $\mathring{X}^{(j)}(1)$ constitute the j-th-order $\psi(1)_j$ of ladder $\#(1)$.

Proof: Suppose that $X_j^{(0)}=\mathring{X}^{(j-1)}(1) = \{x^{(j-1)}(1), x^{(j-1)}(2), \cdots, x^{(j-1)}(p) \}$ $\forall j \in (1,2, \cdots,q)$; then one can obtain $X_j = \{ x(1), x(2), \cdots, x(p) \}$ through 1-AGO. From (2.5)~(2.9), one obtains $\mathrm{GM}^{(j)}(1)$, which is an inside lock of the K-Q Lock $(<\mathrm{GM}^{(j)}(1), \mathring{X}^{(j)}(1)>$, and $S^{(j)}{}_x(1))$. Thus, $\mathring{X}^{(j)}(1)$ is generated by $\mathrm{GM}^{(j)}(1)$ and the natural number set Z; $\{Z=1, 2, \ldots., p\}$. According to definition 4.1, $\mathring{X}^{(j)}(1)$ is a ladder set of X_j. According to definition 3.2, $\mathring{X}^{(j)}(1)$ is an outside lock of the K-Q Lock $(<\mathrm{GM}^{(j)}(1), \mathring{X}^{(j)}(1)>$, and $S^{(j)}{}_x(1))$. From definition 4.3, one knows that the combination of $X(1)_j$ and $\mathring{X}(1)_j$ will constitute the j-th-order $\psi(1)_j$ of ladder $\#(1)$ and conform to: $\psi(1)_j = (X(1)_j \circ \mathring{X}(1)_j)$. In order to avoid confusion, $\psi(1)_j = (X_j \circ \mathring{X}_j)$ in definition 4.3 is rewritten as $\psi(1)_j=(X(1)_j \circ \mathring{X}(1)_j)$.

Theorem 4.2 (q-order ladder bearing-reproduction theorem)

Suppose that $(<\mathrm{GM}^{(j)}(1), \mathring{X}^{(j)}(1)>$, and $S^{(j)}{}_x(1))$ is a bearin -reproduction lock of the K -Q Lock $(<\mathrm{GM}(1), \mathring{X}(1)>$, and $S_x(1))$ and $j = 1, 2, \cdots, q$; both inside lock $\mathrm{GM}^{(j)}(1)$ and outside lock $\mathring{X}^{(j)}(1)$ will generate a q-order ladder $\#(1) = \{ \psi(1)_1 \# \psi(1)_2 \# \ldots \# \psi(1)_q\}$, and

$$\psi(1)_j = \underset{j=1,2,\cdots q}{BR}(\#(1)) \tag{4.6}$$

in the above , behind order $X^{(1)}(j)$ in $\psi(1)_j$ is a set that generates $\mathrm{GM}^{(j)}(1)$, and future order $\mathring{X}(1)_j$ is a set generated by $\mathrm{GM}^{(j)}(1)$; $j=1, 2, \ldots, q$.

Proof: Suppose that $X^{(1)}(1)=\{ x^{(1)}(1), x^{(1)}(2), \ldots, x^{(1)}(p) \}$ and $Z=\{1, 2, \ldots, p\}$; then $\mathrm{GM}^{(1)}(1)$ will be obtained while $X^{(1)}(1)$ is 1-AGO of $X^{(0)}(1)=\{ x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(p)\}$ according to (2.2)~(2.9). From $\mathrm{GM}^{(1)}(1)$ and Z, one obtains $\mathring{X}^{(1)}(1)$. According to definition 4.4, both $\mathring{X}^{(1)}(1)$ and $X^{(1)}(1)$ constitute the 1-th-order $\psi(1)_1$ in ladder $\#(1)$. Thus, $X^{(1)}(1)$ is the behin d order of $\psi(1)_1$, and $\mathring{X}^{(1)}(1)$ is the future order of $\psi(1)_1$. Suppose that $X^{(2)}(1)= \mathring{X}^{(1)}(1)$; then one can obtain $\mathrm{GM}^{(2)}(1)$ according to (2.2) ~(2.9). Thus, one can obtain $\mathring{X}^{(2)}(1)$ according to $\mathrm{GM}^{(2)}(1)$ and Z. In the same way, both $\mathring{X}^{(2)}(1)$ and $X^{(2)}(1)$ constitute the 2-th-order $\psi(1)_2$ in ladder $\#(1)$, and $X^{(2)}(1)$ is 1-AGO of $\mathring{X}^{(1)}(1)$, which can be seen from the above. Suppose that $X^{(q)}(1)= \mathring{X}^{(q-1)}(1)$; then one can obtain $\mathrm{GM}^{(q)}(1)$ and $\mathring{X}^{(q)}(1)$. As for the q-th-order $\psi(1)_q$ in ladder $\#(1)$, it is constituted b $\mathring{X}^{(q)}(1)$ and $X^{(q)}(1)$.

Therefore, $\#(1)=\{\psi(1)_1 \# \psi(1)_2 \# \ldots \# \psi(1)_q\}$, $\forall j \in (1,2, \cdots,q)$, and $\psi(1)_j = (X(1)_j \circ \mathring{X}(1)_j)_j$.

Take the *4th*-order for example; $X^{(0)}(1)$ is a nonnegative integer set; thus $X^{(0)}(1)= \{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), x^{(0)}(4)\} = \{1, 2, 3, 4\}$, $X^{(1)}(1)$ is the 1-AGO of $X^{(0)}(1)$, and $X^{(1)}(1) = \{1, 3, 6, 10\}$.

Here the process of calculation is skipped. Bel ow is the result of the calculation： $\#(1)=\{ \psi(1)_1 \# \psi(1)_2 \# \psi(1)_3 \# \psi(1)_4\}$, $\psi(1)_1=(X^{(1)}(1) \circ \mathring{X}^{(1)}(1))=((1, 3, 6, 10) \circ (3, 6, 10, 15))$ $\psi(1)_2=(X^{(2)}(1) \circ \mathring{X}^{(2)}(1))=((3, 9, 19, 34) \circ (9, 19, 33, 56))$, $\psi(1)_3=(X^{(3)}(1) \circ \mathring{X}^{(3)}(1))=((9, 28, 61, 117) \circ (28, 59, 112, 202))$, $\psi(1)_4=(X^{(4)}(1) \circ \mathring{X}^{(4)}(1))=((28, 87, 199, 401) \circ (86, 191, 379, 718))$.

From the above-mentioned example, one can obtain:

Theorem 4.3 (simply-ordered structure theorem in $\psi(1)_j$)

Suppose that $\psi(1)_j$ is the j-th-order of ladder $\#(1)$; then both the behind order $X(1)_j$ and the future order $\mathring{X}(1)_j$ of $\psi(1)_j$ are simply-ordered sets.

Theorem 4.4 ($\psi(1)_j$ resolution and dispersion theorem in ladder #(1))

Suppose that $\#(1)$ is a q-order ladder and $\psi(1)_j$ is the j-th-order of $\#(1)$; then both $\#(1)$ and $\psi(1)_j$ will conform to

$$\#(1)= \underset{j=1,2,\cdots,q}{RD}(\psi(1)_j) \tag{4.7}$$

In the above-mentioned example, $\underset{j=1,2,\cdots,q}{RD}$ is the resolution and dispersion of #(1) in q-order$\psi(1)_j$.

Proposition 4.1 All j-order $\psi(1)_j$ in ladder #(1) are independent.

Suppose that $\psi(1)_i$ and $\psi(1)_j$ are selected at random and $i \neq j$, then one obtains $\psi(1)_i \neq \psi(1)_j$, which is an inevitable outcome.

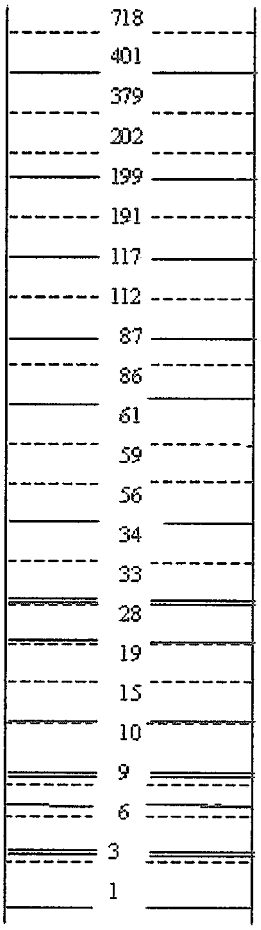

Fig.3 4th-order of ladder #(1) constituted by $\psi(1)_j$, $\forall j \in (1, 2, 3, 4)$

5. Encryption Criterion of Ladder and Ladder Encryption Algorithm

According to the above-mentioned context concerning the basic theorem and analysis of the K-Q Lock, one can induce the encryption ladder criterion of the K -Q Lock which is aimed at document $\langle m_1, m_2, \cdots, m_q \rangle$.

Suppose that document $M=\langle m_1, m_2, \cdots, m_q \rangle$ is constituted by q plaintexts; then $X^{(0)} = \{ x^{(0)}(1), x^{(0)}(2), \cdots, x^{(0)}(q) \}$ will be selected and will be a nonnegative real number set ($q \geq 4$). Moreover, the j-th-order $\psi(1)_j$ in ladder #1(1) encrypts $m_j \subset M$ into ciphertext $c_j \subset C$.

$$c_j = \psi(1)_j \oplus m_j \tag{5.1}$$

The algorithm of the ladder is aimed at the encryption of documents, two characteristics of which are stated in the below:

1. Sequential and nonsequential characteristic

m_j can be encrypted by $\psi(1)_j$ in sequence or not in sequence $j = 1, 2, \cdots, q$.

2. Independent and undisturbed characteristic

Only if $i \neq j$, both kinds of encryptions, $\psi(1)_i$ encrypting m_i and $\psi(1)_j$ encrypting m_j, can be kept independent and undisturbed when $\psi(1)_i$ is i-order and $\psi(1)_j$ j-order in ladder #(1). According to the ladder encryption cri terion, one can obtain two types of encryption algorithms.

I . Sequential full encryption and ladder encryption algorithm

Step1 Given a nonnegative real number set $X^{(0)} = \{ x^{(0)}(1), x^{(0)}(2), \cdots, x^{(0)}(p) \}$ and a natural number set , both sets $X^{(0)}$ and Z conform to $|X^{(0)}| = |Z|$.

Step2 Through (2.3), one obtains $X^{(1)}(1)$. Through (2.5)~(2.9), one obtains $\dot{X}^{(1)}(1)$, in which $X^{(1)}(1)$ is the previous behind order and $\dot{X}^{(1)}(1)$ a future order in $\psi(1)_1$, and

$$\psi(1)_1 = (X^{(1)}(1) \circ \dot{X}^{(1)}(1)) \tag{5.2}$$

$\psi(1)_1$ is the 1^{st}-order in ladder #(1).

Step3. If $T < >q$, then $T=T+1$ and go to step 2 .

Step4. Generate ladder # (1) = $(\psi(1)_1 \# \psi(1)_2 \# \cdots \# \psi(1)_q)$.

Step5 Through the calculation below, both $\psi(1)_j$ and plaintext m_j generate ciphertext c_j, $\forall j=1,2, \ldots q$, so that the following can be conformed

$$c_j = \psi(1)_j \oplus m_j \tag{5.3}$$

under the condition that $m_i \neq m_j$ and $i \neq j$.

Step6. End.

Figure 4 shows a clear explanation of the sequential full-encryption and ladder encryption algorithm. However, not all plaintext documents $M' = \langle m'_1, m'_2, \cdots, m'_q \rangle$ need t be encrypted. Only the specific parts m'_j (j=1, 2, $\cdots$, $r < q$) of M' need to be encrypted.

For example, in commercial applications, some plaintext requires full encryption so that an opponent will not access it. In contrast, some plaintext is not so important that it needs to be encrypted. Aimed at the above requirement s, the algorithm below is design.

II . Sequential Half-Encryption Algorithm and En-cryption Algorithm Ladder

Under document $M = \langle M_1, M_2, \varnothing_3, M_4, \varnothing_5, \varnothing_6, \ldots, M_{q-1}, \varnothing_q \rangle$, suppose that M_i is a item needing to be encrypted, and $\varnothing_j$ not needing to be. The methodical process is explained below. Figu re 5 illustrates the sequential half-encryption and the ladder encryption algorithm.

Step1 Given a nonnegative real number set $X^{(0)} = \{ x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(p) \}$ and a natural number set Z, both sets $X^{(0)}$ and Z conform to $|X^{(0)}| = |Z|$.

Step2 Through (2.3), one obtains$X^{(1)}(1)$; through (2.5~2.9) one obtains $\dot{X}^{(1)}(1)$. Then,

$$\psi(1)_1 = (X^{(1)}(1) \circ \dot{X}^{(1)}(1))_1 \tag{5.4}$$

$\psi(1)_1$ is the I^{st}-order of #(1).

Step3. If $T<> q$; then $T=T+1$ and go to step 2.

Step4. Generate ladder $\#(1) =(\psi(1)_1\# \psi(1)_2\# \cdots \# \psi(1)_q)$.

Step5. If $m_i<>\varnothing_i$; then c_i is generated b

$$c_i=\psi(1)_i \oplus m_i \qquad (5.5)$$

Step6. Go to step 5 .

Step7. End.

6. Opening the K-Q Lock

In section 2-6, the encryption and locking of plaintext $m_j \in M$ into ciphertext $c_j\in C$ is discussed. In encryption ladder #(1), $\psi(1)_j$ is the j-order and there exists· a kind of re-lationship between plaintext $m_j\in M$ and ciphertext $c_j\in C$ as

$$c_j = \psi(1)_j \oplus m_j \qquad (6.1)$$

The mark "⊕" means module 2 operation in a binary system.

For example, the binary code of j-order $\psi(1)_j$ in plaintext $m_j\in M$ is expressed as the following: m_j=(10101011) and $\psi(1)_j$= (01010101). According to (6.1), one obtains cipher-text c_j corresponding to plaintext $m_j \in M$ as the following:

$$c_j = \psi(1)_j\oplus m_j = (10101011) \oplus (01010101) = (11111110)$$

Next, the opening of the K -Q Lock and the decryption of plaintext m_j are introduced.

Theorem 6.1 (first decryption theorem of the K-Q Lock)

For the receivers, assume that $C=\{c_1, c_2, \ldots, c_p\}$is a ciphertext set. After encrypting for odd time, ciphertext c_j can be changed into plaintext $m_j\in M$ as follows

$$m_j = \bigoplus_{i\in(1,3,\cdots,2n-1)} (\psi(1)_j)_i \oplus c_j \qquad (6.2)$$

The mark " $\bigoplus_{i\in(1,3,\cdots,2n-1)}$ " is an odd -time encryption and $\psi(1)_j$ is the j-order in ladder #(1).

Theorem 6.1 can be obtained directly through a binar module 2 operation. The following statement explains theorem 6.1:

Ciphertext c_j=(11111110) and j-order $\psi(1)_j$ in ladder #(1)=(10101011), which after encrypting once time t c_j, m_j can be deduced.

Thus, $m_j = (\psi(1)_j)_1\oplus c_j$ = (10101011) ⊕ (11111110)= (01010101)

in the same way, after encrypting three times to c_j, m_j, can be deduced.

Then, $m_j = (\psi(1)_j)_3\oplus c_j$ = (10101011) ⊕ (10101011) ⊕ (10101011) ⊕ (11111110) = (01010101)

Similarly, after encrypting for $2n-1$ times to c_j and m_j, can be deduced.

Thus, $m_j = (\psi(1)_j)_{2n-1}\oplus c_j$ = (10101011) ⊕ (10101011) ⊕ (10101011)⊕ … ⊕ (11111110) = (01010101)

Theorem 6.2 (second decryption theorem of the K-Q Lock)

Suppose that $M=\{m_1, m_2, \ldots, m_p\}$is a plaintext set; then after encrypting for even time, plaintext m_j will keep the same plaintext as $m_j\in M$ previously in what follows

$$m_j = \bigoplus_{i\in(2,4,\cdots,2n)} (\psi(1)_j)_i \oplus m_j \qquad (6.3)$$

The mark " $\bigoplus_{i\in(2,4,\cdots,2n)}$ " is an even-time encryption, and $\psi(1)_j$ is the j-order in ladder #(1).

Theorem 6.3

Suppose that $C=\{c_1, c_2, \ldots, c_p\}$is a ciphertext set and $M=\{ m_1, m_2, \ldots, m_p \}$is a plaintext set; then, there exists a mapping relationship between the above two

$$\bigoplus_{i\in(1,3,\cdots,2n-1)} : \ C \rightarrow M \qquad (6.4)$$

$$c_j \rightarrow m_j= c_j\, (\oplus\psi(1)_j)_i\ {}_{,\, i\in(1,3,\ldots,2n-1)}$$

Theorem 6.3 is a straightforward term. According to the above-mentioned theorem, the K -Q Lock can be untied. According to theorems 6.1~6.3, one returns to the former question — how to open a K-Q Lock.

Method 1: Pass the key and untie the K-Q Lock directly.

While sending ciphertext c_j to the receiver, the sender passes $X(1)_j$, $\mathring{X}(1)_j$ secretly to the receiver. According t theorem 6.2, the receiver can obtain plaintext m_j by the following equation:

$$m_j= \psi(1)_j \oplus c_j \qquad (6.5)$$

Method 2: Copy the key and untie the K-Q Lock.

While sending ciphertext c_j to the other, the sender must send the blank of the key $X^{(0)}$ and number $p\in N$ to the receiver secretly at the same time. Then, the receiver reproduces the key of the K-Q Lock (copy key immediately to decrypt c_j into m_j. In the above, p is a cardinal number of $\mathring{X}(1)_j$. An instance of the key-copying process is cited below.

Suppose that the receiver obtains the blank of key $X^{(0)} =\{ x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), x^{(0)}(4) \}=\{1, 2, 2, 1 \}$ and $| \mathring{X}(1)_j |=3$ from the sender. On the basis of 1 -AGO, the receiver obtains $X(1) =\{ x^{(1)}(1), x^{(1)}(2), x^{(1)}(3), x^{(1)}(4) \}=\{ 1, 3, 5, 6 \}$. Since $| \mathring{X}(1)_j |=3$ the receiver gets $\mathring{X}(1)_j =\{ x^{(1)}(1), x^{(1)}(2), x^{(1)}(3)\}$ according to the model-key. Therefore, the receiver obtains $\psi(1)_j=(X(1)_j\circ \mathring{X}(1)_j)$. Thus, $\psi(1)_j$ is a copy key to the K-Q Lock. By this method, the receiver can unlock plaintext m_j.

Furthermore, if the receiver wants to revise or replenish the plaintext m_j encryption, one must operate c_j according to theorem 6.2 as follows

$$m_j= \psi(1)_j \oplus (\psi(1)_j \oplus c_j).$$

C_j is decrypted into m_j and m_j can be modified. If m_j is modifed as m'_j, the sender must compute $c'_j =\psi(1)_j \oplus m'_j$. Therefore, a new c'_j can be unlocked and the other keys need not be changed.

7. Discussion of the K-Q Lock

The aim of sections 2-6 is as follows

1. One can obtain a complete key to the encryption cryptosystem of encryption by applying (2.1), (2.2), (2.5), (2.6), and (2.10). The key is generated from the above-mentioned model called the model-key. Under such an environment, the designer can transfer the threshold of entrance according to different demands to set up the lock and key in the K-Q Lock, such as objects or authorization. In other words, the range in application in the area of security becomes wider

2. In section 5, the encryption of plaintext m_j is completed by $\psi(1)_j$, $\psi(1)_j=(X(1)_j \circ \underset{\cdot}{X}(1)_j)_j$. Only the sender of ciphertext c_j knows $\psi(1)_j$. Of course, the sender of ciphertext c_j can freely design and choose $\psi(1)_j$, which is a private key. From the structure of $\psi(1)_j$, one sees that $\psi(1)_j$ is formed b $X(1)_j$ and $\underset{\cdot}{X}(1)_j$. While taking $\psi(1)_j$ to encrypt plaintext m_j, $X(1)_j$ and $\underset{\cdot}{X}(1)_j$ will exist at the same time, and both $X(1)_j$ and $\underset{\cdot}{X}(1)_j$ conform to:

$$\forall j, \quad X(1)_j \circ \underset{\cdot}{X}(1)_j \tag{7.1}$$

(7.1) explains that the private key is a secret function with two layers.

3. The following example states the "security of private ke $\psi(1)_j$" in brief. First, the encrypters of plaintext m_j choose a sequence $X^{(0)}=\{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), x^{(0)}(4)\}=\{1, 2, 3, 4\}$at random, and then obtain $X(1)=\{x^{(1)}(1), x^{(1)}(2), x^{(1)}(3), x^{(1)}(4)\}=\{1, 3, 6, 10\}$. Only the e ncrypter knows $X(1)$, and one can select the integer numbers or nonnegative real numbers to $\underset{\cdot}{X}(1)$~$\underset{\cdot}{X}(4)$, for example, $\underset{\cdot}{X}(1)_{(1)}=\{1, 3, 6, 10\}$, $\underset{\cdot}{X}(1)_{(2)}=\{10, 30, 59, 98\}$, $\underset{\cdot}{X}(1)_{(3)}=\{10, 30, 59, 98, 154\}$, and $\underset{\cdot}{X}(1)_{(4)}=\{10, 30, 59, 98, 154, 231\}$. Obviously, the method gives the user a highly flexible range for choosing a private key $\psi(1)_j$. The user can select nonnegative real numbers such as the following for the original data. $\underset{\cdot}{X}(1)_{(1)}=\{10.0, 30.5, 59.1, 98.9\}$, $\underset{\cdot}{X}(1)_{(2)}=\{100.0, 305.5, 591.3, 989.1, 1542.5\}$, ⋯, and so on. Below are the details of private ke $\psi(1)_j$,

$\psi(1)_{j(1)}=(X(1) \circ \underset{\cdot}{X}(1)_{(1)})$, $\psi(1)_{j(2)}=(X(1) \circ \underset{\cdot}{X}(1)_{(2)})$,

$\psi(1)_{j(3)}=(X(1) \circ \underset{\cdot}{X}(1)_{(3)})$, $\psi(1)_{j(4)}=(X(1) \circ \underset{\cdot}{X}(1)_{(4)})$,

$\psi(1)_{j(5)}=(X(1) \circ \underset{\cdot}{X}(1)_{(1)})$, $\psi(1)_{j(6)}=(X(1) \circ \underset{\cdot}{X}(1)_{(2)})$.

In the example, the element $x(i) \in X(1)$ is taken as a nonnegative integer for the sake of conveniance of calculation. In general, the element $x(i) \in \mathring{X}(1)$ is a nonnegative real number. The user can choose $\psi(1)_j$ as his/her private key freely because the nonnegative real number $x(i)$ is taken as the element in $X(1)$. Furthermore, since $\psi(1)_j$ is chosen at random, the securit of documents can be insured certainly by the user's private key. Consequently, it is very difficult for attackers to decrypt ciphertext.

8. Conclusion

The basic concept of the K-Q Lock has been presented in this paper. Below is further explanation to emph asize that the K-Q Lock can be applied in many ways.

1. Because decryption ke $S_x(1)$ for the receiver is a function in extension set X, these questions do not need to be discussed in this paper. Research into extension sets is suggested as a topic for future research.
2. The encryption in the Identit -Password table, the definition of the encryption-decryption transformation in the table, and the settlement of a key distribution center can be discussed in future research.
3. Under the condition that $1<q$ and $q \in N$, one takes the K-Q Lock to encrypt plaintext from m_l to m_q. Such a process of encryption is similar to climbing a ladder therefore, the process of encryption has been named the encryption algorithm ladder.

References

[1]. J.L. Deng, "Control Problems of Grey Systems", Systems and Control Letters, 1982, Vol. 1, No. 5, 285-294.

[2]. J.L. Deng, "Introduction to Grey System Theory", The Journal of Grey Systems, 1989, Vol.1, No.1, 1-24.

[3]. K.Q. Shi, "Grey Information Relational Theory", Quan Hua Science and Technology Press, 1994, Taipei, Taiwan, 121-124.

[4]. Mike Matyas, Mohammad Peyravian, Allen Roginsky, Nev Zunic, "Reversible Mata Mixing Procedure for Efficient Public-Key Encryption", Computers and Security, 1998, Vol.17, No.3, 265-272.

[5]. Birgit Borcherding, Malte Borcherding. "Efficient and Trustworthy Key Misattribution in Webs of Trust", Computers and Security, 1998, Vol. 17, No. 5, 447-454.

[6]. M. Stioson, "Combinatorial Techniques for Universal Hashing", Journal of Computer and System Sciences, 1994, Vol. 22, No.6, 472-492.

[7]. W, Miffic, M. Hellman, "New Directions in Crypto-graphy", IEEE Transactions on Information Theory, 1976, Vol. 22, No.6, 472-492.

[8]. C.S. Laih, S.M. Yen, "Multi-Signature for Specified Group of Verifiers", Journal of Information Science and Engineering, 1996,Vol. 12 , No.1, 143 -152.

[9]. M.S. Hwang, W.G. Tzang , W.P. Yang, " Two-key-lock-pair Access Control Method Usin Prime Factorization and Time Stamp", IEICE Transactions on Information and Systems, 1994, E77-M(9), 1042-1046.

[10]. M. Wiener. "Cryptanalysis of Short RSA Secret Exponents", IEEE Transactions on Information Theory, 1990, Vol. 36, No.4, 553-558.

[11]. I. Ingemarsson, M. Tang, C. Wong. "A Conference Key Misattribution System", IEEE Transactions on Information Theory, 1982, Vol.28, No.5, 714-720.

[12]. T. Elgamal, "A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, 1985, IT-31(4), 469-472 .

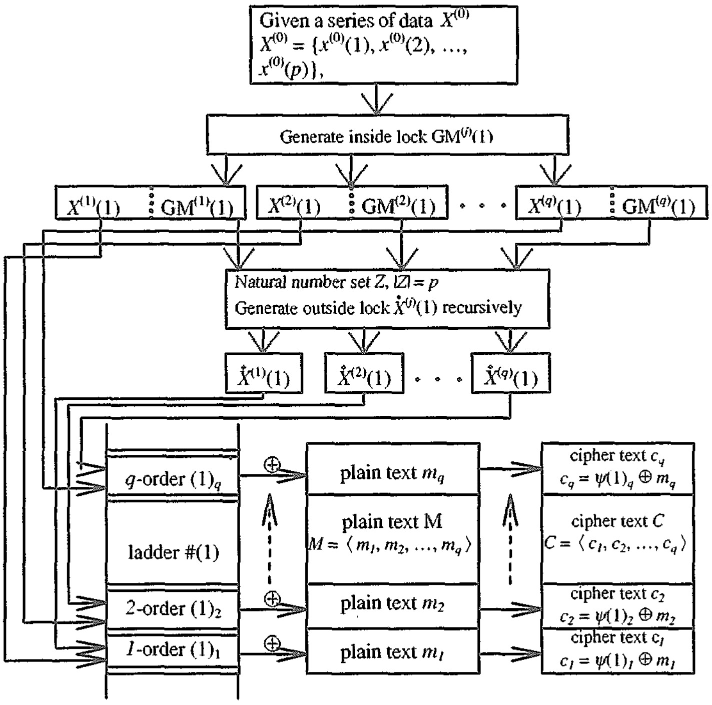
Given a series of data $X^{(0)}$
$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(p)\}$,
Generate inside lock $GM^{(i)}(1)$
$X^{(1)}(1)$ $GM^{(1)}(1)$
$X^{(2)}(1)$ $GM^{(2)}(1)$
$X^{(q)}(1)$ $GM^{(q)}(1)$
Natural number set Z, $|Z| = p$
Generate outside lock $\dot{X}^{(i)}(1)$ recursively
$\dot{X}^{(1)}(1)$
$\dot{X}^{(2)}(1)$
$\dot{X}^{(q)}(1)$
q-order $(1)_q$
ladder #(1)
2-order $(1)_2$
1-order $(1)_1$
⊕
plain text m_q
plain text M
$M = \langle m_1, m_2, \ldots, m_q \rangle$
plain text m_2
plain text m_1
cipher text c_q
$c_q = \psi(1)_q \oplus m_q$
cipher text C
$C = \langle c_1, c_2, \ldots, c_q \rangle$
cipher text c_2
$c_2 = \psi(1)_2 \oplus m_2$
cipher text c_1
$c_1 = \psi(1)_1 \oplus m_1$

Fig. 4 Flowchart of sequential full-encryption algorithm and encryption algorithm ladder.

$\psi(1)_i$ is the i-th-order in ladder #(1) , $M= \langle m_1,m_2,\cdots,m_q \rangle$ is a plaintext, and $C= \langle c_1,c_2, \cdots,c_q \rangle$ is a ciphertext.

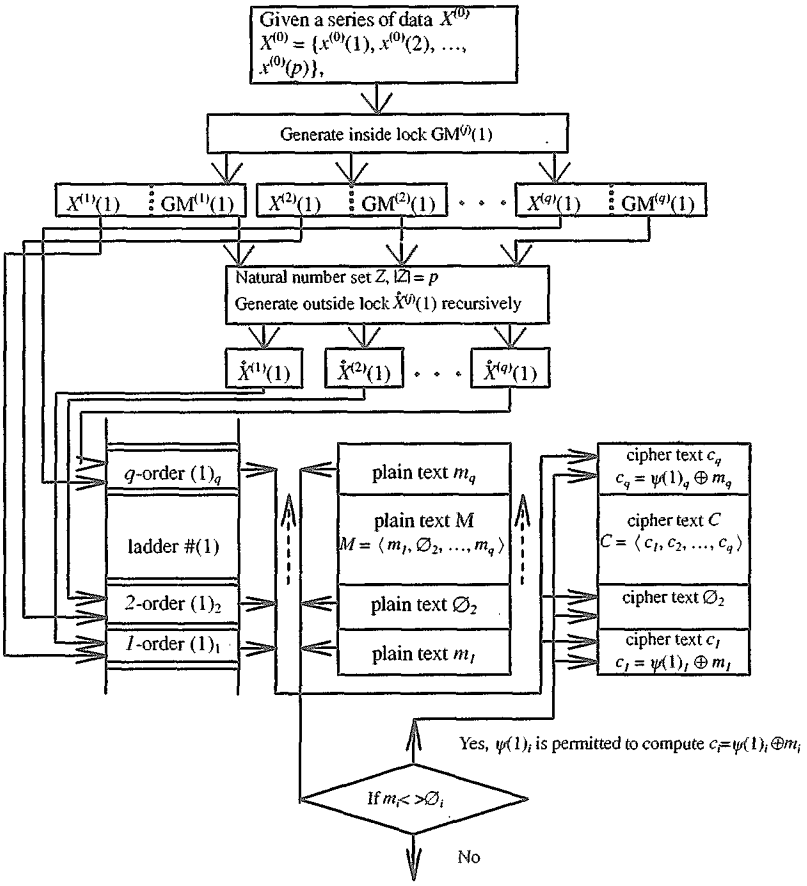
Given a series of data $X^{(0)}$
$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(p)\}$,
Generate inside lock $GM^{(i)}(1)$
$X^{(1)}(1)$ $GM^{(1)}(1)$
$X^{(2)}(1)$ $GM^{(2)}(1)$
$X^{(q)}(1)$ $GM^{(q)}(1)$
Natural number set Z, $|Z| = p$
Generate outside lock $\dot{X}^{(i)}(1)$ recursively
$\dot{X}^{(1)}(1)$
$\dot{X}^{(2)}(1)$
$\dot{X}^{(q)}(1)$
q-order $(1)_q$
ladder #(1)
2-order $(1)_2$
1-order $(1)_1$
plain text m_q
plain text M
$M = \langle m_1, \varnothing_2, \ldots, m_q \rangle$
plain text $\varnothing_2$
plain text m_1
cipher text c_q
$c_q = \psi(1)_q \oplus m_q$
cipher text C
$C = \langle c_1, c_2, \ldots, c_q \rangle$
cipher text $\varnothing_2$
cipher text c_1
$c_1 = \psi(1)_1 \oplus m_1$
Yes, $\psi(1)_i$ is permitted to compute $c_i=\psi(1)_i \oplus m_i$
If $m_i <> \varnothing_i$
No

Fig. 5 Flowchart of sequential half encryption algorithm and encryptionalgorithm ladder.

$\psi(1)_i$ is the i-th-order in ladder #(1); M_i is a plaintext needing to be encrypted; in contrast, $\varnothing_j$ is a plaintext not needing to be encrypted.