# A Multi-Level Secret Sharing Scheme Based on Semigroup Structures*

HE Ming-xing[1,2], FAN Ping-zhi[1]

[1](*Southwest Jiaotong University, Chengdu* 610031, *China*);

[2](*Sichuan University of Science and Technology, Chengdu* 610039, *China*)

E-mail: hemingxing@mail.scit.edu.cn; p.fan@ieee.org

Received February 13, 2001; accepted June 15, 2001

**Abstract:** How to securely distribute a company's secret key to its *n* authorized departments is of much importance in information management system of E-commerce. In many cases, every authorized department in a company needs a partial or sub-secret key, and each person in the corresponding authorized department has an access level to the sub-secret key. Upon the sub-secret key of a department being cooperatively reconstructed, the company's secret key can be securely and completely reconstructed from all sub-secret keys of the departments. This paper presents such a novel multi-level secret sharing scheme. Instead of traditional method, this scheme is mainly based on the complexity of semigroup structures in which each department's sub-secret key is related to a group and each person's access level in the corresponding department is characterized by an order of an element in the group. The proposed scheme can also be employed to other scenarios where multi-level secret sharing is needed.

**Key words:** semigroup; group; multi-level secret sharing; information system; E-commerce

With the recent explosive growth of the Internet and mobile systems, more and more business is conducted over the open communication network and a huge amount of sensitive information is managed within these open systems. As a result, the increase of information transmitted electronically has led to an increased need for security. Since the access control services of traditional file systems are insufficient to meet the file-protection security requirements coming along with the open and cooperative environments, cryptographic techniques are applied to solve the problem. Consider such a scenario that how to securely distribute a company's secret information to its *n* authorized departments. In many cases, each authorized department in a company need a partial or sub-secret key and each person in the authorized department has an different access level to this sub-secret key. When a group of members in each department gets the department's sub-secret key cooperatively according to their access levels, the company's secret key can be reconstructed completely from all sub-secret keys in each department. So a multi-level secret sharing scheme is needed in such a situation.

On the other hand, semigroup theory is an enormously diffuse subject and has advanced on a very broad front. The most coherent part of semigroup theory related to key sharing scheme is the part concerned with the structure of

* Supported by the National Natural Science Foundation of China under Grant No. 69825102 (国家自然科学基金)

**HE Ming-xing** was born in 1964. He received the M.S. degree in Applied Mathematics of the Chongqing University in 1990. He is an associate professor of the Sichuan University of Science and Technology and is a Ph.D. candidate at the school of Computer and Communications Engineering, Southwest Jiaotong University. His current research areas include computer networks, information security and its applications in mobile communications. **FAN Ping-zhi** received the Ph.D. degree in Electrical Engineering from the Hull University, U.K. in 1994. He is a professor and doctoral supervisor of the School of Computer and Communications Engineering, Southwest Jiaotong University. His research interests include wireless mobile and personal communications, wireless multimedia systems, computer networks, information security and signal design & processing.

various kinds of semigroups[1~6]. The authors ponder over how to connect the structure complexity of semigroups with the security of secret sharing scheme. As far as authors are aware, secret sharing schemes based on field and ring theory have been investigated by many researchers[3,5~8,10], but no semigroup-based secret sharing scheme is known except for Ref.[1]. However, the work presented in Ref.[1] is limited by its strict conditions. Therefore, we attempt to propose a new method to implement multi-level secret key sharing that can be based on the complexity of semigroup structure. Mathematically, the proposed scheme is related to a collection of semigroups which are generated by some kinds of finite groups by using a given method, and each person's secret access level to the sub-secret key is characterized by an order of one element in a group. To be specific, the more the order of element, the higher his/her access level. In short, the proposed scheme has two features: (1) The secret sharing access structure is more general than the scheme in Ref.[1], in this scheme each person has his own access level not being necessarily the same as that of others; (2) The scheme is more secure than that of Ref.[1]. We expect that an extensive study on semigroup may unveil more practical and secure methods in secret key distribution and reconstruction.

The rest of the paper is organized as follows. Section 1 gives preliminary concepts and semigroup basics. Section 2 discusses the security issues of a previous work. Section 3 presents the new multi-level secret sharing scheme based on semigroup structure. Section 4 addresses the security and implementation issue of the proposed scheme. Section 5 presents some illustrative application examples. Finally, Section 6 concludes the paper.

## 1 Preliminary

In this section, some related concepts and theorem[1,2,9] are presented.

**Definition 1 (Semigroup and Group)**. Given a non-empty set $S$ on which a binary operation $\mu: S\times S\to S$ is defined, we shall say that $(S,\mu)$ is a semigroup if $\mu$ is associative, i.e.,

$$\forall x,y,z\in S,\ ((x,y)\mu,z)\mu=(x,(y,z)\mu)\mu \tag{1}$$

Following the usual practice in algebra, we shall write $(x,y)\mu$ simply as $x\ y$ and usually refer to the semigroup operation as multiplication. The formula (1) then becomes $(x\ y)z=x(y\ z)$. We shall write a multiplicative semigroup as $(S, .)$ or simply as $S$. The cardinal number $|S|$ will be called the order of the semigroup $S$.

If a semigroup has the property:

$$\forall a\in S, a\ S=S \ \text{ and } \ S\ a=S \tag{2}$$

we call it a group.

**Definition 2 (Subsemigroup).** If $(S, .)$ is a semigroup, then a non-empty subset $T$ of $S$ is called a subsemigroup of $S$ if it is closed with respect to multiplication, i.e.,

$$\forall x,y\in T,\ \ xy\in T \tag{3}$$

**Definition 3 (Generating Set).** If $\{U_i: i\in I\}$ is a non-empty family of subsemigroups of a semigroup $S$, then it is easy to see that $\bigcap\{U_i: i\in I\}$ is either empty or is itself a subsemigroup of $S$. If $A$ is an arbitrary non-empty subset of $S$, then the family of subsemigroups of $S$ containing $A$ is non-empty. Hence the intersection of the family is a subsemigroup of $S$ containing $A$. We denote it by $\langle A\rangle$, the semigroup $\langle A\rangle$ consists of all elements of $S$ that can be expressed as finite products of elements in $A$. If $\langle A\rangle= S$ we shall say that $A$ is set of generators for $S$ or a generating set of $S$.

**Definition 4 (Monogenic Semigroups).** If $A$ is a finite set $\{a_1,a_2,\ldots,a_n\}$, we shall write $\langle A\rangle$ as $\langle a_1,a_2,\ldots,a_n\rangle$. Especially interesting is the case where $A=\{a\}$, when $\langle a\rangle=\langle a^1,a^2,a^3,\ldots\rangle$. We refer to $\langle a\rangle$ as the monogenic subsemigroup of $S$ generated by the element $a$. The order of $a$ is defined as the order of the subsemigroup $\langle a\rangle$. If a semigroup $S$ has the property that $S=\langle a\rangle$ for some $a$ in $S$, we say that $S$ is monogenic semigroup.

**Definition 5 (Index and Period).** Let $a$ be an element of a semigroup $S$ and consider the monogenic

subsemigroup $\langle a\rangle=\langle a^1,a^2,a^3,\ldots\rangle$ of $S$ generated by $a$. If there are no repetitions in the list $a^1,a^2,\ldots$, i.e. if $a^m = a^n \Rightarrow m = n$, then the element has infinite order. If repetitions do occur among the power of $a$, then the set $\{x \in N : \exists y \in N, s.t.\ ax = ay, x \neq y\}$ is non-empty and so has a least element $m$ and we call it the index of $a$. Then the set $\{x \in N :\ a^{m+x} = a^m\}$ is non-empty and so it too has a least element $r$ which we call it the period of $a$.

**Definition 6 (Homomorphism Mapping).** If $\phi$ is a mapping from a semigroup ($S$, .) into a semigroup ($T$, .) we say that $\phi$ is a homomorphism if

$$\forall x, y \in S, \quad (xy)\phi = (x\phi)(y\phi) \tag{4}$$

If $\phi$ is one-one mapping we call it a monomorphism; and if it is both one-one and onto mapping we call it an isomorphism.

**Lemma 1.** If $a$ is an element of a finite group $G$, then the period of $a$ divide $|G|$.

**Lemma 2.** Given a semigroup $S=\langle a_1,a_2,\ldots,a_n\rangle$, if the order of $\langle a_i\rangle$ is a prime $q_i$ ($i$=1,2,…,$n$), the same as the period of $a_i$, then for all $x_i \in \langle a_i\rangle$ satisfying $x_i \neq a_i^{q_i}$, the relation $\langle x_i\rangle = \langle a_i\rangle$ and $S=\langle x_1,x_2,\ldots,x_n\rangle$ hold.

**Lemma 3.** If $\phi: G \to G'$ is a homomorphism from group $G$ to group $G'$, $a \in G$, the period of $a$ is $r$, the period of $\phi(a)$ is $k$, then $k$ divide $r$.

**Lemma 4.** If $G=\langle a\rangle$ and $G'=\langle b\rangle$ are cyclic groups of order $n$ and $m$ respectively, then there exists a homomorphism $\phi$ from $G$ to $G'$ such that $a\phi = b^k$ if and only if $m$ divide $n$ $k$.

**Lemma 5.** If $G=\langle a\rangle$ and $G'=\langle b\rangle$ are cyclic groups of order $n$ and $m$ respectively, then $G$ and $G'$ are onto homomorphic if and only if $m$ divide $n$.

**Theorem 1.** Let $Y$ be a semilattice and $S = \{G_\alpha : \alpha \in Y\}$ be a family of disjoint groups, indexed by $Y$. For each pair $\alpha, \beta$ of elements of $Y$ such that $\alpha \geq \beta$, let $\phi_{\alpha,\beta} : G_\alpha \to G_\beta$ be a homomorphism and suppose that

$\phi_{\alpha,\beta}$ is the identical automorphism of $G_\alpha$ for each $\alpha \in Y$,

$\phi_{\alpha,\beta}\phi_{\beta,\gamma} = \phi_{\alpha,\gamma}$, for ever $\alpha, \beta, \gamma$ in $Y$ such that $\alpha \geq \beta \geq \gamma$.

Let $S = \bigcup\{G_\alpha : \alpha \in Y\}$ and define a multiplication $*$ on $S$ by the rule that if $a_\alpha \in G_\alpha$ and $b_\beta \in G_\beta, a_\alpha * b_\beta = (a_\alpha\phi_{\alpha,\alpha\beta}) * (b_\beta\phi_{\beta,\alpha\beta})$, then $(S,*)$ is a semigroup.

**Notations** Let $C_i$ stand for cyclic group with order $i$, $K_4$ stand for Klein group with 4 elements, $P_i$ stand for permutation group of order $i$. $D_i$ stand for Department $i$ in a company.

## 2 A Previous Scheme and Its Security

This section introduces an interesting secret key distribution scheme based on semigroup theory[1].

Firstly, let us pay attention to the main steps of which the scheme in Ref.[1] consists.

Step 1. Choose $n$ pair wise disjoint finite cyclic groups $G_i=\langle x_i\rangle$, $i$=1,2,…,$n$, such that $|G_i| = q_i$, $q_i$ is a prime; distribute $G_i$ to department $D_i$ as its sub-secret key; each one in department $D_i$ is assigned to an element $x_i^l \in \langle x_i\rangle$ ($x_i^l \neq a_i^{qi}$) as ones secret sharing key.

Step 2. Let $Y$ be {1,2,…,$n$}, $S = \bigcup\{G_\alpha : \alpha \in Y\}$ and define a multiplication $*$ on $S$: for $a_\alpha \in G_\alpha$ and $b_\beta \in G\beta$, $a_\alpha * b_\beta = (a_\alpha\phi_{\alpha,\alpha\beta}) * (b_\beta\phi_{\beta,\alpha\beta})$. Choose a total ordered semilattice $Y$, such that $|Y|= n$, and for each pair $\alpha, \beta \in Y$, it is held that either $\alpha \leq \beta$ or $\beta \leq \alpha$. where $\phi : S \to Y$ be an onto homomorphism, and suppose that $\phi_{\alpha,\beta} : G_\alpha \to G_\beta$ be a homomorphism satisfying:

$\phi_{\alpha,\alpha}$ is the identical automorphism of $G_\alpha$ for each $\alpha \in Y$,

$\phi_{\alpha,\beta}\phi_{\beta,\gamma} = \phi_{\alpha,\gamma}$, for ever $\alpha,\beta,\gamma$ in $Y$ such that $\alpha \geq \beta \geq \gamma$,

Step 3. Let semigroup $(S,*)$ be the company's main secret key.

Secondly, we notice that there are some restrictions in this scheme which make the scheme less practical and less secure: A) the scheme requires that $q_i$ be a prime, so there exist only two kinds of homomorphism mappings $\phi_{\alpha,\beta}: G_\alpha \to G_\beta$ in this case by Lemma 1 and Lemma 3. One is monomorphism and the other is identity homomorphism. In case of $q_\alpha \neq q_\beta$, for example, $|G_\alpha|=3$ and $|G_\beta|=5$, by lemma 1 and lemma 3, there exists only one trivial homomorphism mappings $\phi_{\alpha,\beta}: G_\alpha \to G_\beta$ from $G_\alpha$ into $G_\beta$, i.e. identity homomorphism: $\forall a \in G_\alpha$, $a\phi_{\alpha,\beta}=e$ ($e$ is identity element of $G_\beta$). If $q_\alpha = q_\beta$, for example, $|G_\alpha|=|G_\beta|=3$, and $G_\alpha=\{e,a,a^2\}$, $G_\beta=\{e,b,b^2\}$, it is obvious that there is only one kind of non-trivial homomorphism: $\phi_{\alpha,\beta}: a^i \to b^i$ ($i$=1,2,3) is such a non-trivial homomorphisms from $G_\alpha$ to $G_\beta$. Hence the security of the scheme is weakened. B) by Lemma 2 and Step 1 the scheme does not distinguish the access levels of members in a department, in other words, each member has the same access authority to the sub-secret key of his department, i.e., $\langle x_i^l\rangle=\langle x_i\rangle$, that means every one by itself can access the department's sub-secret key. This restriction has narrowed its application areas.

## 3 The Proposed Scheme

The proposed secret key sharing scheme is based on Theorem 1 and depends on the following main parameters: authorized department $D_\alpha$ ($\alpha \in Y$), access level of member in $D_\alpha$ and secret key $K=\{Y;\ \{G_\alpha : \alpha \in Y\};\{\phi_{\alpha,\beta}: \alpha,\beta \in Y, \alpha \geq \beta\}\}$. It is assumed that a key management server is available in this scheme.

The secret key distribution process is as follows:

(1) The server assigns a finite group $G_\alpha$ to each department $D_\alpha$ as the department's partial secret key. (Note that $|G_\alpha|$ is not necessarily a prime). Different $G_\alpha$ is distributed to a different $D_\alpha$ and $G_\alpha \cap G_\beta = \Phi$ if $\alpha \neq \beta$.

(2) Each member in $D_\alpha$ receives a non-identity element of $G_\alpha$ as his/her characteristic of access level, which is decided by the order of the element of which the member possess; generally speaking, the greater the order of element, the higher his/her access level.

(3) The server creates a set of homomorphisms $\phi_{\alpha,\beta}: G_\alpha \to G_\beta$ from arbitrary $G_\alpha$ to $G_\beta$ provided that $\alpha,\beta \in Y$ and $\alpha \geq \beta$, where $Y$ is a well-ordered semilattice. It is required that $\phi_{\alpha,\beta}\phi_{\beta,\gamma}=\phi_{\alpha,\gamma}$ for $\alpha,\beta,\gamma$ in $Y$ such that $\alpha \geq \beta \geq \gamma$.

(4) The server keeps $K=\{Y;\ \{G_\alpha : \alpha \in Y\};\{\phi_{\alpha,\beta}: \alpha,\beta \in Y, \alpha \geq \beta\}\}$ as the company's secret key.

Then the secret key reconstruction process is realized as follows:

(1) Each department $D_\alpha$ chooses appropriate persons to reconstruct the department's partial secret key $G_\alpha$;

(2) All departments' representatives present together to produce $S=\bigcup_{\alpha \in Y}(G_\alpha)$;

(3) With the help of the server, specifically, when the server presents the corresponding set of homomorphisms $\{\phi_{\alpha,\beta}: \alpha,\beta \in Y, \alpha \geq \beta\}$, secret key $K=(S,*)$ is reconstructed. Where a multiplication $*$ on $S$ is defined by the rule: $a_\alpha \in G_\alpha, {}_\beta \in G_\beta, a_\alpha * b_\beta = (a_\alpha\phi_{\alpha,\alpha\beta}) * (b_\beta\phi_{\beta,\alpha\beta})$. In fact, $(S,*)$ is a semigroup.

(4) The server can verify the validity of this key by comparing $(S,*)$ with $K=\{Y;\ \{G_\alpha : \alpha \in Y\};\{\phi_{\alpha,\beta}: \alpha,\beta \in Y, \alpha \geq \beta\}\}$ kept before.

## 4 Security and Implementation Issue

Security of the proposed scheme is mainly based on the complexity of the structures of semigroups, which are determined by elements and multiplication of these semigroups. Imagine a set of $n$ elements, we can define $n^{n^2}$ kinds of multiplication if no other restrictions are required for the multiplication (numbers of all possible multiplications). Even if a semigroup structure is embedded in this set, the number of possible multiplications is still very large. Moreover, our scheme is with a few of parameters. The following context presents an extensive analysis for these parameters.

(1) Well ordered semilattice $Y$

In short, a well ordered semilattice is employed to order departments, for example, {1,2,…,$n$} is a well ordered semilattice under the relation ">" (more than) or "<"(less than). Diversities of semilattice-selection make diversities of homomorphisms set $\{\phi_{\alpha,\beta}: G_\alpha \to G_\beta, \alpha,\beta \in Y, \alpha \geq \beta\}$, which result in stronger security of the proposed sharing scheme.

(2) Groups $G_\alpha : \alpha \in Y$

How to choose a finite group for each department $D_\alpha$? It is determined by the number and access level of each member in the department $D_\alpha$. We list a few classification results on the Abelian group of orders 1 to 14 in Table 1 for illustration.

**Table 1** Abelian groups of orders 1 to 14

| Order | Number | Type | Order | Number | Type |
|---|---|---|---|---|---|
| 1 | 1 | $C_1$ | 8 | 3 | $C_8$, $C_2\times C_4$, $C_2\times C_2\times C_2$ |
| 2 | 1 | $C_2$ | 9 | 2 | $C_9$, $C_3\times C_3$ |
| 3 | 1 | $C_3$ | 10 | 1 | $C_{10}= C_2\times C_5$ |
| 4 | 2 | $C_4$ , $K_4$ | 11 | 1 | $C_{11}$ |
| 5 | 1 | $C_5$ | 12 | 2 | $C_{12}= C_3\times C_4$, $C_2\times C_2\times C_3$ |
| 6 | 1 | $C_6= C_2\times C_3$ | 13 | 1 | $C_{13}$ |
| 7 | 1 | $C_7$ | 14 | 1 | $C_{14}= C_2\times C_7$ |

A general method for constructing all finite groups can be broken down into two problems: the group extension problem and the discovery of all finite simple groups. These had been major preoccupations of workers in the field of finite groups until 1980 when an excellent theorem of the classification of simple groups was given. A good introduction to this theory is on Refs.[11,13]. Algebra software such as GAP[13] can be employed to present groups as GAP knows how to construct a number of well-known groups such as symmetric and classical groups. Hence the appropriate group can be chosen for each department $D_\alpha$ and this option results in stronger security of the proposed sharing scheme than that of the scheme in Ref.[1].

(3) Set of homomorphisms $\{\phi_{\alpha,\beta}: G_\alpha \to G_\beta, \alpha,\beta \in Y, \alpha \geq \beta\}$

Once the well ordered semilattice Y and the group family is determined, homomorphisms can be constructed by various methods provided that $\phi_{\alpha,\beta}$ satisfy the condition of Lemma 3, Lemma 4 and Lemma 5 (Refer to Tables3, 4, 5, 6).

(4) Multi-Access levels

Each member in department $D_\alpha$ is assigned to a different element of group $G_\alpha$ according to his/her access level. For illustration, Table 2 lists all possible orders of elements in a finite group $G$ with order $2pq^2$. Then we can make decision on which element is assigned to a member in a department according to his/her access level. This property is a characteristic which the scheme in Ref.[1] does not possess. From the view of secret sharing access structure[14], the proposed scheme is more practical than Ref.[1].

**Table 2**

| order | 2 | $q$ | $p$ | $2q$ | $2p$ | $Pq$ |
|---|---|---|---|---|---|---|
| number | 1 | $q$-1 | $p$-1 | $q$-1 | $p$-1 | ($p$-1)($q$-1) |
| order | $q^2$ | $2pq$ | $2q^2$ | $pq^2$ | $2pq^2$ | |
| number | $q$($q$-1) | ($p$-1)($q$-1) | $q$($q$-1) | $q$($p$-1)($q$-1) | $q$($p$-1)($q$-1) | |

## 5 Illustrative Examples

Let $G_1$, $G_2$, $G_3$, $G_4$ denote four finite groups, which satisfy $|G_1|=12$, $|G_2|=10$, $|G_3|=8$, $|G_4|=6$, then $G_1$ can be classed into 3 cases: $G_1=C_{12}$, $G_1=C_3 \times C_4$, $G_1= C_3 \times K_4$; $G_2$ can be classed into 2 cases: $G_2=C_{10}$, $G_1=C_2 \times C_5$; $G_3$ can be classed into 5 cases: $G_3= C_2 \times C_2 \times C_2$, $G_3=C_2 \times C_4$, $G_3=C_8$, $G_3=S_4$, $G_3$=8 elements group; $G_4$ can be classed into 2 cases: $G_4=C_6$, $G_4=P_3$.

Case 1: Unequal access levels

For simplicity of illustration, assume there are 3 authorized departments in a company, there are 11, 9, 7 members in department $D_1$, $D_2$, $D_3$ respectively (Fig.1). The boss is out for a conference, but staff needs some documents in case of emergency. Then the boss can distribute the access secret keys according to our scheme.

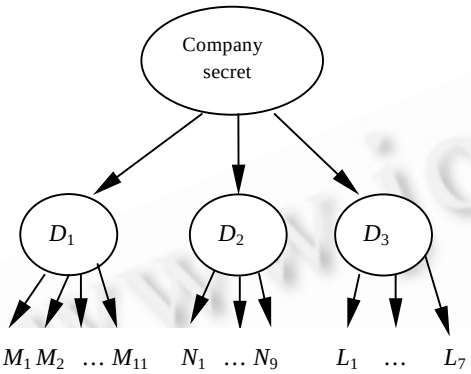


Fig.1 Company structure 1

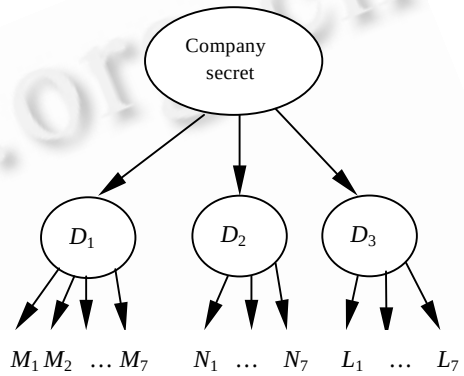


Fig.2 Company structure 2

(1) According to the secret distribution process described in Section 3, suppose department $D_1$ received $G_1=C_{12}=\{e,a,a^2,a^3,\ldots,a^{11}\}$, department $D_2$ received $G_2=C_{10}=\{e,b,b^2,b^3,\ldots,b^9\}$ and department $D_3$ received $G_3=C_8=\{e,c,c^2,c^3,\ldots,c^7\}$. Each member in a department received an access level. For example, some members in department $D_1$ are assigned to generators $a$, $a^5$, $a^7$, $a^{11}$ of $G_1$ and received the highest level, some members are assigned to $a^2$, $a^4$, $a^8$, $a^{10}$ and received lower level, …, and a member $e$ received the lowest level (Note that the member is equivalently considered to be the element he/she received in the rest of this paper without declaration).

In $D_1$, member received $a^4$ (order=3) and member $a^3$ (order=4) together can represent $D_1$;

In $D_2$, member $b^3$ (order=10) alone or member $b^2$ and member $b^5$ (orders=5,2) together can represent $D_2$;

In $D_3$, member $c^7$ (order=8) alone can represent $D_3$.

(2) Choose a well ordered semilattice, for example, $Y=\{1,2,3\}$ where $1 \geq 2 \geq 3$, such that $G_1 \to 1$, $G_2 \to 2$, $G_3 \to 3$, establish the following homomorphisms: $\phi_{1,2}$: $G_1 \to G_2$, $\phi_{2,3}$: $G_2 \to G_3$, then $\phi_{1,3}= \phi_{1,2}\phi_{2,3}$: $G_1 \to G_3$.

**Table 3** Homomorphism $\phi_{1,2}$

| $\alpha \in G_1$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha\phi_{1,2} \in G_2$ | $e$ | $b^5$ | $e$ | $b^5$ | $e$ | $b^5$ | $e$ | $b^5$ | $e$ | $b^5$ | $e$ | $b^5$ |

**Table 4** Homomorphism $\phi_{2,3}$

| $\beta \in G_2$ | $e$ | $b$ | $b^2$ | $b^3$ | $b^4$ | $b^5$ | $b^6$ | $b^7$ | $b^8$ | $b^9$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $\beta\phi_{2,3} \in G_3$ | $e$ | $c^4$ | $e$ | $c^4$ | $e$ | $c^4$ | $e$ | $c^4$ | $e$ | $c^4$ |

(3) Let $S=\cup\{G_i : 1 \leq i \leq 3\}$, $\forall a_\alpha \in G_\alpha, \forall b_\beta \in G_\beta$, abiding with the rule $a_\alpha * b_\beta = (a_\alpha \phi_{\alpha,\alpha\beta}) * (b_\beta \phi_{\beta,\alpha\beta})$ we can calculate products in $S$, for example, $a^2 * b^3 = (a^2 \phi_{1,2})(b^3 \phi_{2,2}) = eb^3=b^3, b^4 * c^2=(b^4 \phi_{2,3})(c^2 \phi_{3,3})= c^2$, $a^9 * c^3=$

$(a^9\phi_{1,3})(c^3\phi_{3,3}) = c^4c^3 = c^7$. We can verify that $(a^2 * b^3) * c^5 = b^3 * c^5 = c^9 = c$ equals to $a^2 * (b^3 * c^5) = a^2 * c = e * c = c$. Then $(S, *)$ is a semigroup (multiplication table is omitted here), and $K = \{Y; \{G_\alpha : \alpha \in Y\}; \{\phi_{\alpha,\beta} : \alpha, \beta \in Y, \alpha \geq \beta\}\} = \{\{1, 2, 3\}; \{G_1, G_2, G_3\}; \{\phi_{1,2}, \phi_{1,3}, \phi_{2,3}\}$ is just the secret key shared by $G_1, G_2, G_3$.

Case 2: Equal access levels

Assume there are 3 authorized departments in a company (Fig.2), and the access priority of each member in a department is of equality.

(1) Without loss of generality, assume department 1 received $G_1 = C_7 = \{e, a, a^2, a^3, \ldots, a^6\}$, department 2 received $G_2 = C_7 = \{e, b, b^2, b^3, \ldots, b^6\}$, department 3 received $G_3 = C_7 = \{e, c, c^2, c^3, \ldots, c^6\}$. Each member in a department received an equal access level. For example, in department 1 members are assigned generators $a, a^2, a^3, \ldots, a^6$ of $G_1$ and received the same level, in other words, each member can represent his/her department to access the secret key of the company.

(2) Choose a well ordered semilattice, for example, $Y = \{1,2,3\}$ where $1 \geq 2 \geq 3$, such that $G_1 \to 1$, $G_2 \to 2$, $G_3 \to 3$, establish the following homomorphisms: $\phi_{1,2}: G_1 \to G_2$, $\phi_{2,3}: G_2 \to G_3$, then $\phi_{1,3} = \phi_{1,2}\phi_{2,3}: G_1 \to G_3$

**Table 5** Homomorphism $\phi_{1,2}$

| $\alpha \in G_1$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
|---|---|---|---|---|---|---|---|
| $\alpha\phi_{1,2} \in G_2$ | $e$ | $b^3$ | $b^6$ | $b^2$ | $b^5$ | $b$ | $b^4$ |

**Table 6** Homomorphism $\phi_{2,3}$

| $\beta \in G_2$ | $e$ | $b$ | $b^2$ | $b^3$ | $b^4$ | $b^5$ | $b^6$ |
|---|---|---|---|---|---|---|---|
| $\beta\phi_{2,3} \in G_3$ | $e$ | $c^2$ | $c^4$ | $c^6$ | $c$ | $c^3$ | $c^5$ |

(3) Let $S = \cup\{G_i : 1 \leq i \leq 3\}$, $\forall a_\alpha \in G_\alpha, \forall b_\beta \in G_\beta$, by the rule $a_\alpha * b_\beta = (a_\alpha \phi_{\alpha,\alpha\beta}) * (b_\beta \phi_{\beta,\alpha\beta})$ we can calculate products in $S$, for example, $a^2 * b^3 = (a^2\phi_{1,2})(b^3\phi_{2,2}) = b^6b^3 = b^2$, $b^3 * c^5 = (b^3\phi_{2,3})(c^5\phi_{3,3}) = c^6c^5 = c^4$. We can verify that $(a^2 * b^3) * c^5 = b^2 * c^5 = c^2$ equals to $a^2 * (b^3 * c^5) = a^2 * c^4 = c^5 * c^4 = c^2$. Then $(S, *)$ is a semigroup (multiplication table is omitted here), and $K = \{Y; \{G_\alpha : \alpha \in Y\}; \{\phi_{\alpha,\beta} : \alpha, \beta \in Y, \alpha \geq \beta\}\} = \{\{1,2,3\}; \{G_1, G_2, G_3\}; \{\phi_{1,2}, \phi_{1,3}, \phi_{2,3}\}$ is just the sharing secret key of $G_1$, $G_2$, $G_3$.

## 6 Conclusions

This paper presents a multi-level secret sharing scheme that is mainly based on semigroup theory. Compared with the scheme in Ref.[1], the proposed scheme has the following two advantages: (1) the secret sharing access structure is more general. In this scheme each person has his own access level not being necessarily the same as that of others, i.e., the so-called multi-level key sharing scheme. (2) The scheme is more secure. The security depends on the complexity of group selection, homomorphisms construction, semigroup multiplication, etc. This multi-secret sharing scheme can be used to distribute and reconstruct secret key in a company consisting of a number of departments whose members are classified and allocated with different secret-access-levels. In addition, several simple illustrative examples are provided to demonstrate the applicability of the new scheme. It is also expected that the scheme can be applied to other situations where multi-level secret sharing is needed.

**Acknowledgement** The authors would like to thank the anonymous referees for their valuable comments on the previous version of this paper.

**References:**

[1] Wang, Yong-chuan, Li, Zi-cheng, Yang, Yi-xian. A secret key distributions schemes based on the theory of algebraic semigroups. Journal of Eletronics, 2000,22(3):509~512 (in Chinese).

[2] Howie, J.M. An Introdution to Semigroup Theory. New York: Academic Press, 1976. 89~124.

[3] Ecker, A. Finite semigroup and RSA cryptosystem. In: Advances in Cryptology-EuroCrypt'82. Berlin: Springer-Verlag, 1983. 353~369.

[4] Warne, R.J. On the structure of certain classes of semigroups which are unions of groups. Mathmatics Journal, 1973,4:21~26.

[5] Jackson, D.C. Direct products of cyclic semigroups and unions of groups. Semigroup Forum, 1995,50(2):223~231.

[6] Zhu, Wen, He Ming-xing. On the congruences lattice of G inverse semigroups. Journal of Mathematics, 1999,19(4):411~415 (in Chinese).

[7] Koga, H., Hirosuke H. Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Transactions on Fundamentals, 1998,E81-A(6):1262~1269.

[8] Naor, M., Shamir, A. Visual cryptography: improving the contrast via the cover base. http://theory.lcs.mit.edu/tcryptol/1996/96-07.html.

[9] Zhu, Wen, He, Ming-xing. On the automorphism groups of finite groups. Journal of UEST, 2000,29(5):269~271 (in Chinese).

[10] He, M.X., Fan, P.Z. Multiple secrets sharing schemes for mobile Internet environment. In: Proceedings of the Mobile Internet Workshop. Beijing, 2000. 82~86.

[11] Solomon, R. On finite simple groups and their classification. Notices America Mathatics Society, 1995,42(2):231~239.

[12] Xu, Ming-yao. Introduction to Finite Groups. Beijing: Science Press, 1999 (in Chinese).

[13] GAP Research Group. Introduction of GAP. 2000. http://www-groups.dcs.st-and.ac.uk/.

[14] Brickell, E.F., Daveport, D.M. On the classification of idea secret sharing scheme. Journal of Cryptology, 1991,4(2):123~134.

附中文参考文献:

[1] 王永传,李子臣,杨义先.基于代数半群理论的密钥分享方案.电子科学学刊,2000,22(3):509~512.

[6] 朱雯,何明星.G-逆半群的同余格.数学杂志,1999,19(4):411~415.

[9] 朱雯,何明星.有限群的自同构群.电子科技大学学报,2000,29(5):269~271.

[12] 徐明耀.有限群导引.北京:科学出版社,1999.

# 基于半群结构的多等级密钥分享方案

何明星[1,2], 范平志[1]

[1](西南交通大学 计算机与通信工程学院,四川 成都 610031);

[2](四川工业学院 计算机科学与工程系,四川 成都 610039)

摘要: 在信息管理与电子商务应用中,如何安全地将一个合法实体(比如一个公司)的密钥分配给其属下的若干部门具有非常重要的意义.通常在这类应用中各部门都需拥有自己的子密钥,而每个部门的每个人(或科室)都有不同的子密钥授权等级,即一个部门只要其中一部分被授权人根据他们的密钥授权等级适当联合就能获得所在部门的子密钥,而一旦得到每个部门的子密钥就能够恢复出公司完整的密钥.基于此,建立了一个满足这种要求的安全的密钥分享体制.与传统方法不同,利用代数中群与半群的结构理论,通过使个人的密钥授权等级对应于相应群的特定元素的阶从而给出了一种能实现这种多等级密钥分享的方案.该方案可用于需要多等级密钥分享的其它场合.

关键词: 半群;群;多等级密钥分享;信息系统;电子商务

中图法分类号: TP309 文献标识码: A