Generalized Secret Sharing with Linear Hierarchical Secrets

Xi Chen[1], Yun Liu[1], Chin-Chen Chang[2,3], and Cheng Guo[4]
(Corresponding author: Chin-Chen Chang)

Key Laboratory of Communication and Information Systems[1]
Beijing Municipal Commission of Education, Beijing Jiaotong University
no. 3, Shang Yuan Cun, Hai Dian District, Beijing 100044, P. R. China
Department of Information Engineering and Computer Science[2]
Feng Chia University, Taichung 40724, Taiwan, R.O.C
Department of Computer Science and Information Engineering[3]
Asia University, Taichung 41354, Taiwan, R.O.C
Department of Computer Science, National Tsing-Hua University[4]
Hsinchu 30013, Taiwan, R.O.C
(Email: alan3c@gmail.com)

(Received Jan. 11, 2013; revised and accepted Mar. 4, 2013)

Abstract

Generalized secret sharing is a method of constructing secret sharing from the perspective of access structure. In this paper, we propose a novel solution for achieving generalized secret sharing with linear hierarchical secrets. We use a matrix to model the relationship related to the access structure and transfer the matrix to modular arithmetic, which is calculated by Chinese Remainder Theorem. The participants in the corresponding access structures can cooperate with each other to produce secrets in monotonous levels. We prove that shared secrets can be efficient and reconstructed only by the qualified subset of participants; unqualified participants cannot reconstruct the corresponding shared secret.
Keywords: Cryptography, generalized secret sharing, Chinese Remainder Theorem

1 Introduction

A secret sharing scheme is a method to distribute secret data among a set of participants. This distribution is done in such a way that some authorized subsets of the participants pool their information, allowing them to reconstruct the secret. Unauthorized subsets of participants cannot obtain any information about the secret [29].

In 1979, Blakley [4] and Shamir [22] independently proposed the concept of secret sharing for the first time. Their schemes are called (t,n)-threshold schemes [21], and they have been developed extensively by subsequent researchers, e.g., in key-management problems [9, 25, 28, 30] and key-distribution problems [11, 17]. As a result, they have been used in many practical applications. In such schemes, any set of at least out of participants can recover the secret. But, if there are less than participants, no information would be revealed. A more general case of secret sharing threshold schemes is the secret sharing scheme based on an access structure [18, 20]. In [15, 31], the authors showed how to develop a secret sharing scheme for any access structure that is a group of all the subsets of participants，who are authorized to reconstruct the secret [12]. The reader can consult the survey articles by Simmons [23] and Stinson [26], which provide a unified description of secret sharing schemes.

In addition to the research of secret sharing schemes, several authors studied this open issue from the perspective of access structures, forming a line of work that is categorized as generalized secret sharing schemes. In 1985, Kothari [16] introduced a generalized linear threshold scheme that can be used to provide a hierarchical threshold scheme. It allows multiple thresholds in a hierarchical environment, if necessary. In [14], Ito, Saito, and Nishizeki proposed a general method of secret sharing with access structures. The secret can be divided among a set of a qualified subset, the groups of which are called access structures. Any qualified subset of can reconstruct the secret, while the unqualified subsets cannot. Benaloh and Leichter [3] developed a secret sharing scheme for any monotone access structure. Several particular families of access structures, such as weighted threshold access structures, hierarchical threshold access structures [27], and multi-level access structures [5, 24] have been considered successively. The common ground of the above access structures is that they belong to multipartite access structures, in which the set of participants is divided into several parts, and the participants in the same group play an equivalent role.

According to a series of research projects on generalized secret sharing，any given access structure can be used for a secret sharing scheme [3, 14]. Some specific models for secret sharing with access structures have already been considered one after another, for example,

multi-level access structures, weighted-threshold access structures, hierarchical access structures, and generalized-threshold access structures. Among these generalizations of threshold secret sharing, hierarchical secret sharing has attracted a lot of interests. In [1], Akl and Taylor presented a scheme based on cryptography to solve the problem of access control in a hierarchy. Chang et al. [6] proposed a solution that combines secret sharing based on access structures with hierarchical key management. In Chang's scheme, the participant groups are classified into several levels, and higher-level groups can compute the secret keys of the lower-level groups. In addition, each group has its own access structures to share the group's secret key. In 2005, Lin et al. [19] proposed another scheme that improves Chang et al.'s efficiency with the usage of a one-way hash function to allow the shadows to be reused while achieving the property of hierarchical access control. In 2007, Tassa [27] proposed a hierarchical threshold secret sharing scheme by using Birkhoff interpolation, which generates fewer shares for participants of lower levels. Since the derivative orders are chosen properly, this allocation of shares dictates the threshold access requirements. As a consequence, when qualified subsets collaborate and attempt to recover the secret, it is necessary for them to solve the Birkhoff interpolation problem first. In 2010, O. Farràs and C. Padró [10] defined the family of hierarchical access structures and provided a full characterization of them.

The application of the Chinese Remainder Theorem to threshold secret sharing has already been proposed by many researchers. For example, Asmuth and Bloom [2] proposed a key safeguarding scheme based on the Chinese Remainder Theorem. In [26], Iftene and Boureanu achieved weighted threshold secret sharing by introducing the Chinese Remainder Theorem. Guo and Chang [8] proposed a group key distribution scheme, which was built on secret sharing. And the scheme greatly reduced computation and communication costs by using Chinese Remainder Theorem. Chang [7] designed a key-lock-pair mechanism and made use of Chinese Remainder Theorem to realize the faster operations and simpler constructions of keys and locks. Our idea is inspired from Chang's method.

In spite of the extensive application of secret sharing schemes, it was not known what access structures schemes solve such a problem. Let's consider the scene that occurs in the storage service, which is common in cloud computing or in large-scale, distributed systems. To reduce costs, we assumed one entrepreneurial team that rents some space for cloud storage to store the data and information of an incipient company. In the organization of this company, there is still no hierarchy among the team members, i.e., they are equal to each other. In this team, there are different levels of rights, such as executive power, financial control, and decision-making authority. Generally, we assume that decision-making authority is the highest right, with financial control and executive power following in that order. For mutual supervision, they use decentralized control, which implies that several members in one group share one right. At the same time, to reduce the labor cost, every person can join more than one group and cooperate with any member to produce keys with hierarchical rights in running the company. Therefore, special attention is required to determine how to distribute the right to every member and meet all the above demands. That also is our motivation for the proposed scheme.

This question can be simplified as a secret sharing problem. There are several participants without any hierarchy who have the same weight in the scheme, and they can take part in one or more subsets. Every group shares one secret, and these qualified subsets in the access structure can reconstruct them. We assume that there is a hierarchy on the shared secrets. The high level of secrets can produce the secrets of the lower levels. Figure 1 shows the groups of users in a generalized secret sharing scheme with linear hierarchical secrets. By comparison, Figure 2 shows the users' groups in a secret sharing scheme with hierarchical access structures. The set $\{U_1,U_2,...,U_6\}$ represents the collection of the users who share the secrets $\{S_1,S_2,S_3\}$.

Now, we analysis the similarities and differences between a generalized secret sharing scheme with linear hierarchical secrets and a secret sharing scheme with hierarchical access structures. From the perspective of shared secrets, these two schemes share one point, i.e., there is a hierarchy on the shared secrets, and the high level of secrets can produce the lower level of secrets. But as to the participants, there are two differences. The first one is that the participants in a generalized secret sharing scheme with linear hierarchical secrets and secret sharing are equivalent, i.e., they don't have a hierarchy on the access structures, but the weights of the participants in the latter scheme are unequal in the hierarchical access structures. The second difference is that the participants of the former can join one or more access structures, which is not allowed in the secret sharing scheme with hierarchical access structures.

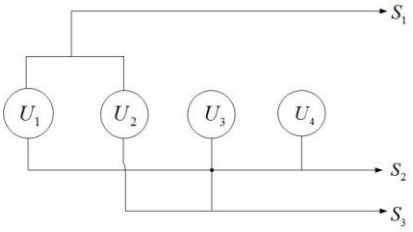

Figure 1: Users' groups in generalized secret sharing scheme with linear hierarchical secrets

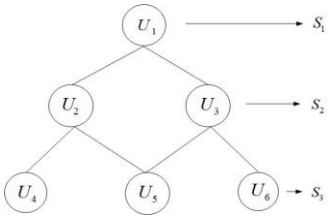

Figure 2: Users' groups in a secret sharing scheme with hierarchical access structures

In this paper, we propose a novel and simple solution for the above problem. In our scheme, we construct secret sharing with hierarchical access control by using a matrix and the Chinese Remainder Theorem，which is very little known in solving secret sharing with linear hierarchical secrets. We modeled the access structures of generalized secret sharing by using a matrix and determined the linear hierarchical secrets with the Chinese Remainder Theorem. Each subset of $t(t \le n)$ participants with their keys can recover secret keys at different levels. The reconstruction process is linear in that each secret key is computed as a fixed linear function of the secret. The levels of access control rights of secret keys are monotone ascending, in that the higher-level secret key can access the lower-level access structure, but not the other way around. The correctness and security of the proposed scheme were proven.

The generalized secret sharing scheme with linear hierarchical secrets is a simple scheme, but it still has some obvious advantages:

1. High efficiency. Every user is in more than one access structure, so it is efficient for one user to produce different level keys by cooperating with others.

2. Flexible to application. Even though there is no hierarchy on a team, it still can be applied to produce hierarchical secret keys.

3. High security. It implies two aspects, i.e., 1) the scheme satisfies the requirements of security and 2) it can reduce the possibility of information leakage for cooperators.

The rest of this paper is organized as follows. In Section 2, we give the basic definitions related to our scheme and briefly review the Chinese Remainder Theorem. In Section 3, we describe the proposed secret sharing scheme with linear hierarchical secrets. Section 4 addresses the correctness and security analysis of the proposed scheme. In Section 5, we compare the proposed scheme with other related schemes; and our conclusions are provided in Section 6.

2 Preliminary Grounds

In this section, we give definitions of access structures, generalized secret sharing, and the generalized secret sharing scheme with linear hierarchical secrets, and then we review the Chinese Remainder Theorem, which was used in our scheme.

2.1 Access Structures

Let U be the set of participants. An access structure, denoted by Γ, is a collection of subsets $A \subseteq 2^U$, and it also is a monotone ascending family, which means that any $A' \in \Gamma$, $A \subseteq 2^U$, $A' \subseteq A$ implies $A \in \Gamma$. Since it has the monotone property, any access structure can be considered as the minimum access structure $\Gamma_{\min} = \{A \in \Gamma \mid \forall B \subset A \Rightarrow B \notin \Gamma\}$.

2.2 Generalized Secret Sharing

In the secret sharing scheme, the secret is divided into several shares, and the shared secrets can reconstruct the secret only the number of shares reaches the threshold value. With different requirements, the generalized secret sharing scheme can realize the specific access structures based on the secret sharing scheme. We can construct a generalized secret sharing scheme satisfying with the following scene, according to the description in [27].

We assume that a dealer D wants to share a secret α with a set of participants U and that Γ is a monotone access structure on U. The dealer will give every participant one share α_i of secret α, which is distributed secretly. Then, a subset of participants can reconstruct the shared secret by pooling their secret shares together. A generalized secret sharing scheme with an access structure is such a scheme and it meets the following requirements:

1) Correctness requirement: any subset $A \subseteq \Gamma$ of participants, which means that the participants are in the qualified subset, is enabled to recover and compute α.

2) Security requirement: any subset $A \not\subset \Gamma$ of participants, which means that the participants are in the unqualified subset, is not enabled to recover α, even by pooling all of their shares.

2.3 Generalized Secret Sharing with Linear Hierarchical Secrets

Let $U=\{U_1,U_2,...,U_m\}$ be the set of participants. The set of access structures, denoted by $\Gamma' = \{\Gamma_1,\Gamma_2,...,\Gamma_n\}$, is a monotone ascending family. The access structures are the subsets of the participants U. The participants can join one or more access structures, which should be required to satisfy: $\Gamma_p,\Gamma_q \subseteq \Gamma', 1 \le p,q \le n, \Gamma_p \not\subset \Gamma_q$ and $\Gamma_q \not\subset \Gamma_p$.

Example 1. *Let* $U=\{U_1,U_2,U_3,U_4\}$ *and* $\Gamma' = \{\Gamma_1,\Gamma_2,\Gamma_3\} = \{\{U_1,U_2\}, \{U_1,U_3,U_4\}, \{U_2,U_3\}\}$ *; then, the secret data can be shared in such a set* $\Gamma'=\{\Gamma_1,\Gamma_2,\Gamma_3\}$. *Since the access structures satisfy the monotone ascending property, the access structures can be described as follows:*

$(\Gamma_1)_{\min} = \{\{U_1,U_2\}\}$, $(\Gamma_2)_{\min} = \{\{U_1,U_3,U_4\}\}$, $(\Gamma_3)_{\min} = \{\{U_2,U_3\}\}$

Suppose that $S=\{S_1,S_2,...,S_n\}$ is the collection of

secrets. Suppose a dealer D wants to share secrets S_j, for $1 \le j \le n$, among a set Γ' of access structures, and the participants in an access structure Γ_j, for $1 \le j \le n$, share one secret S_j. Then, each access structure corresponds to one level of secret key, and each participant is given a share. The shares should be distributed secretly, so no participant knows the share given to other participants. At a later time, a subset of participants in an access structure Γ_j will attempt to reconstruct the secret S_j from the shares they collectively hold. We divide all the secrets in S into n levels, namely, there is only one secret in one level. Here, we let the level for S_σ is greater than S_ω, if $1 \le \delta < \omega \le n$. $S_1 > S_2 ... > S_n$ means the level of S_1 is the highest; then, the level of S_2 takes the second level, and so on. A linear relationship exists among the elements of S. A generalized secret sharing scheme with linear hierarchical secrets is such a scheme and the following requirements are met:

1) Correctness requirement: any subset $A \subseteq \Gamma_j$ of participants, which means that the participants are in the qualified subset, is enabled to recover S_j and compute the secrets $S_j's$ in different levels also.

2) Security requirement: any subset $A \not\subset \Gamma_j$ of participants, which means that the participants are in the unqualified subset, is not enabled to recover S_j, even if they pool all of their shares. And they cannot reconstruct the secrets $S_j's$ in different levels either.

2.4 Chinese Remainder Theorem

Give two sets of integers $a=\{a_1,a_2,...,a_k\}$ and $b=\{b_1,b_2,...,b_k\}$, which satisfy the following conditions: a_i and a_j are coprime numbers, where $i \ne j$, $i=1,2,...,k$, and $j=1,2,...,k$; $0 \le b_i < a_i$, $i = 1, 2, ..., k$; $0 \le x < \prod_{i=1}^{k} a_i, i = 1, 2, ..., k$; and

$$\begin{cases} b_1 = x \bmod a_1, \\ b_2 = x \bmod a_2, \\ \vdots \\ b_k = x \bmod a_k, \end{cases}$$

where x is an integer variable. Then, x has one and only one solution.

3 Proposed Scheme

In this section, we first review the problem of generalized secret sharing, which we stated in Section 1 and provide additional details about it. Then, we propose the correctness and security requirements for the scheme. Finally, we propose a novel solution for achieving generalized secret sharing with linear hierarchical secrets.

3.1 Problem Reviewing

Without loss of generality, we assume that there are users $U=\{U_1,U_2,...,U_m\}$, sharing the secrets $S=\{S_1,S_2,...,S_n\}$, with the monotone access structures $\Gamma'=\{\Gamma_1,\Gamma_2,...,\Gamma_n\}$, Γ_j is composed of a given number of U_i, $1 \le j \le n$, $1 \le i \le m$ and every participant of the access structure Γ_j can share one secret S_j, $1 \le j \le n$. And each access structure Γ_j corresponds to one shared secret S_j. For the access structure Γ_j, there exists an integer L_j, $1 \le j \le n$, which is called the lock for the access structure Γ_j. Every user U_i, $1 \le i \le m$, is assigned to one key share K_i, $1 \le i \le m$; every key share can incorporate with each other in the same access structure to produce the corresponding secret S_j. There is a linear hierarchy of the different levels of secrets. The higher-level groups can compute the secret of the lower-level groups, but not vice versa. Besides the reconstruction by specific users (or secret shares), the secrets $S_j's$ can be generated by computing a function linearly.

Example 2. *(Following **Example 1**). There are four users in a company, U_1,U_2,U_3,U_4, and U_1 cooperates with U_2 to produce secret S_1; U_1,U_3, and U_4 can produce S_2. The levels of S_j, $1 \le j \le n$, are as follows: $S_1 > S_2 > ... > S_n$, where $S_1 = s$, $S_2 = h(S_1) = h(s)$, ..., $S_j = h(S_{j-1})$, ..., $S_n = h(S_{n-1})$. The inequality means the levels of S_j is in descending order, and the level of S_1 is the highest, while S_n is in the lowest level. Figure 3 shows more details. We take users U_1 and U_2 as examples. K_1 and K_2 are the keys held by users U_1 and U_2 in the access structure Γ_1. L_1 is the lock of access structure Γ_1, and S_1 is the corresponding secret .The users U_1 and U_2 can produce cooperatively S_1 by using K_1 and K_2. S_2 can be*

generated by the function of S_1, *which is in the higher level, but* S_1 *cannot be calculated through this function of* S_2.

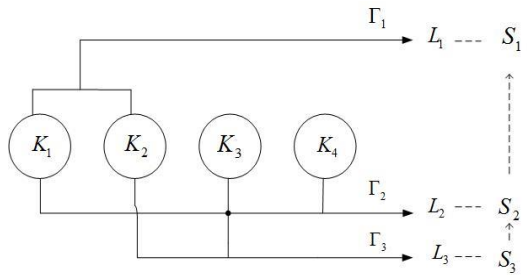

Figure 3: Model of a generalized secret sharing scheme with linear hierarchical secrets

3.2 Construction for Generalized Secret Sharing with Linear Hierarchical Secrets

In our scheme, we use a matrix to model the relationship between the secret keys of the users and the access structures of the generalized secret sharing scheme. The users in the corresponding access structures hold the keys cooperatively to produce the secrets. Then we transfer the matrix to modular arithmetic and calculate the keys with Chinese Remainder Theorem. Under the access structures, our scheme can realize the generation of the linear, hierarchical secrets. Given any access control structure matrix $A_{m\times n}$, the element a_{ij} of it represents the access value of user U_i for the access control structure Γ_j. The user U_i randomly selects numbers for a_{ij}, $1\le i\le m, 1\le j\le n$, satisfying the following constraints:

$$\begin{cases} a_{11}+a_{21}+a_{31}+\ldots+a_{m1}=S_1, \\ a_{12}+a_{22}+a_{32}+\cdots+a_{m2}=S_2, \\ \vdots \\ a_{1n}+a_{2n}+a_{3n}+\cdots+a_{mn}=S_n, \end{cases}$$

which means that the users in access structure Γ_j can incorporate the corresponding secret key S_j.

Example 3. (Following **Example 2)** *We assume users* U_1 *and* U_2 *can construct the secret* S_1*; users* U_1, U_3, *and* U_4 *are able to construct the secret* S_2*; and users* U_2 *and* U_3 *can produce the secret* S_3. *We can express their relationships, as follows:*

$$\begin{cases} a_{11}+a_{21}+0+0=S_1, \\ a_{12}+0+a_{32}+a_{42}=S_2, \\ 0+a_{23}+a_{33}+0=S_3. \end{cases}$$

The limits for S_i *are* $S_1>S_2>S_3$, *which means the level of* S_1 *is the highest, then* S_2, *and the level of* S_3 *is the lowest.* S_j *can be generated linearly, i.e.,* $S_1=s$, $S_2=h(S_1)=h(s)$, *and* $S_3=h(S_2)=h(h(s))$.

Assume that P_j *is the value of* L_j, $\gcd(P_i,P_j)=1$, $\forall\ i\ne j$, $1\le i\le m, 1\le j\le n$, *for the access control structure* Γ_j, $1\le j\le n$, *there exists integers* $L_j's$, $1\le j\le n$, *called locks for the access structures* $\Gamma_j's$, *and integers* $K_i's$, $1\le i\le m$, *called keys of the users* $U_i's$, *such that* $a_{ij}=K_i \bmod L_j$, $0<K_i<\prod_{k=1}^{n}L_k$, $1\le i\le m$, $1\le j\le n$. *The relationship can be expressed as the following matrix:*

	P_1	P_2	$\cdots$	P_n
K_1	a_{11}	a_{12}	$\cdots$	a_{1n}
K_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
K_m	a_{i1}	a_{i2}	$\cdots$	a_{mn}

Example 4. (Following **Example 3**) *We use the matrix to express the relationship between the locks of the access structures and the secret keys the users hold. Assume that* $\{P_1,P_2,P_3\}$ *are the values of the locks* $\{L_1,L_2,L_3\}$ *and that* $\{K_1,K_2,K_3,K_4\}$ *are the secret keys that users* U_1,U_2,U_3,U_4 *hold, respectively following* ***Example 3****, we can get the matrix:*

	P_1	P_2	P_3
K_1	a_{11}	a_{12}	0
K_2	a_{21}	0	a_{23}
K_3	0	a_{32}	a_{33}

$$K_4 \mid \quad 0 \qquad a_{42} \qquad 0$$

We can use congruent operation to express the couple of P_j and K_i and make a_{ij} as the value of the corresponding congruent operation. To the user U_i, all the equations form a system of equations that includes j equations and an unknown quantity K_i, as follows:

$$K_i \text{satisfies} \begin{cases} K_i \bmod P_1 = a_{i1}, \\ K_i \bmod P_2 = a_{i2}, \\ \vdots \\ K_i \bmod P_j = a_{ij}. \end{cases}$$

Example 5. (Following **Example 4**) *We assume that there are four users U_1, U_2, U_3 and U_4. Every element in the matrix of **Example 4** can be evaluated by using K_i and P_j. Every row of the matrix can be transferred to a system of equations.*

$$K_1 \text{ satisfies} \begin{cases} K_1 \bmod P_1 = a_{11}, \\ K_1 \bmod P_2 = a_{12}, \\ K_1 \bmod P_3 = 0; \end{cases}$$

$$K_2 \text{ satisfies} \begin{cases} K_2 \bmod P_1 = a_{21}, \\ K_2 \bmod P_2 = 0, \\ K_2 \bmod P_3 = a_{23}; \end{cases}$$

$$K_3 \text{ satisfies} \begin{cases} K_3 \bmod P_1 = 0, \\ K_3 \bmod P_2 = a_{32}, \\ K_3 \bmod P_3 = a_{33}; \end{cases}$$

$$K_4 \text{ satisfies} \begin{cases} K_4 \bmod P_1 = 0, \\ K_4 \bmod P_2 = a_{42}, \\ K_4 \bmod P_3 = 0. \end{cases}$$

According to the Chinese Remainder Theorem, we can calculate K_i as follows: Since $a_{ij} = K_i \bmod L_j, 1 \le i \le n$, $1 \le j \le m$, we assume that $Q = \prod_{i=1}^{n} P_i$, $Q_i = Q / P_i$, for $i \ne j$, given $C_i = Q_i \times (Q_i^{-1} \bmod P_i)$, then, $K_i \equiv (\sum_{i=1}^{k} a_{ij} C_i) \bmod Q$.

Example 6. (Following **Example 5**) *For the system of equations in **Example 5**, we can use the Chinese Remainder Theorem to get the value of K_i, as the unique solution of the system. We can calculate $\{K_1, K_2, K_3, K_4\}$ as follows:*

$Q = P_1 P_2 P_3$, $Q_1 = P_2 P_3$, $Q_2 = P_1 P_3$, $Q_3 = P_1 P_2$,

$$\begin{cases} C_1 = Q_1 \times [(Q_1)^{-1} \bmod P_1] \\ C_2 = Q_2 \times [(Q_2)^{-1} \bmod P_2]. \\ C_3 = Q_3 \times [(Q_3)^{-1} \bmod P_3] \end{cases}$$

We can obtain

$$\begin{cases} K_1 = [a_{11} C_1 + a_{12} C_2] \bmod Q \\ K_2 = [a_{21} C_1 + a_{23} C_3] \bmod Q \\ K_3 = [a_{32} C_2 + a_{33} C_3] \bmod Q \\ K_4 = (a_{42} C_2) \bmod Q \end{cases}.$$

K_1, K_2, K_3, and K_4 are the keys that are assigned to the users.

4 Analysis of Correctness and Security

We now prove that our scheme is a correct and secure secret sharing scheme. First, we give some definitions related to shared secrets. S is used to represent the shared secret, so $S_j, 1 \le j \le n$, is the shared secret that can be reconstructed by the participants in the access structure Γ_j, $1 \le j \le n$, and S' is a subset of S. We prove the following propositions.

Proposition 1. *The participants of the qualified subset Γ_j, $\Gamma_j \subseteq \Gamma'$, $1 \le j \le n$, can cooperate to reconstruct the corresponding shared secret $S_j, S_j \in S'$.*

Proof. As the above description indicated, matrix $A_{m \times n}$, in which the element a_{ij} represents the access value of user U_i, $1 \le i \le m$, can be constructed according to the shared secret S and the specific access structures. Given any access structure Γ_j in Γ', $1 \le e, f, ..., g \le m$, $1 \le j \le n$, we can set $S_j = a_{ej} + a_{fj} + ... + a_{gj}$. To every user U_i, there exists one and only one key K_i to recover the secret S_j, according to Chinese Remainder Theorem. Since every a_{ij} is randomly selected and bound to $S_j = a_{ej} + a_{fj} + ... + a_{gj}$. K_i will be calculated according to $a_{ij} = K_i \bmod L_j$. Therefore, any subset $\{U_e, U_f, ..., U_g\}$ of participants in $\Gamma' = \{\Gamma_1, \Gamma_2, ..., \Gamma_n\}$ can reconstruct the secret S_j by

computing a linear combination of their shares. Since the secrets $S_j's$ belonging to the set S' are linear and hierarchical, the higher-level groups can compute the secret keys of lower-level groups, and the rest of S can be calculated. □

Proposition 2. *Unqualified participants cannot reconstruct the corresponding shared secret* S_j, $S_j \in S'$, *even by pooling all of their shares together.*

Proof. According to Proposition 1, we can conclude that the shared secret can be reconstructed by any qualified subset of participants by computing $S_j = a_{ej} + a_{fj} + ... + a_{gj}$. Since these n row vectors $(K_1, K_2, ..., K_i)$ and a_{ij} are independent, there exists $\{L_1, L_2, ..., L_n\}$ that satisfies $a_{ij} = K_i \bmod L_j$. And then, since the entries a_{ij} of matrix A are selected randomly, just satisfying $S_j = \sum_{i=1}^{m} a_{ij}$, $1 \le j \le n$, unqualified participants also cannot guess the correct $a'_{ij}s$ that satisfy $S_j = \sum_{i=1}^{m} a_{ij}$, $1 \le j \le n$, even if they know some other secrets (i.e., they can obtain some other secrets by computing a linear combination of their shares). Moreover, there is a hierarchy on $S'_j s$, where $S_j \in S'$, and the higher-level groups can compute the secret keys of the lower-level groups, but not vice versa. Even though S_j can be obtained by the adversary, the rest of S cannot be derived from it. Hence, the proposed scheme is secure.

We now prove that our generalized secret sharing scheme can make the linear shared secrets having a hierarchical property. □

Proposition 3. *Let the secrets* $S'_j s$ *be linear and hierarchical so that the following properties are satisfied.*

1) *The participants in the monotone access structures* $\Gamma' = \{\Gamma_1, \Gamma_2, ..., \Gamma_n\}$ *,can reconstruct the shared secrets* $S'_j s$ *in corresponding levels.*

2) *The participants in the monotone access structures* $\Gamma' = \{\Gamma_1, \Gamma_2, ..., \Gamma_n\}$ *form several groups. And the groups corresponding to the higher level of the secret can compute the secret of the lower level, but not vice versa.*

Proof. The proof of the first property is straightforward from the proof of **Proposition 1**. Now, we prove the second property. Since for S_j, which has monotone ascending property, for example, $S_1 > S_2 > S_3$, we use a one-way hash function to represent the expression, $S_1 = s$, $S_2 = h(S_1) = h(s)$, $S_3 = h(S_2) = h(h(s))$. The shared secrets $S'_j s$ correspond to different access structures, so the participants of the higher-level groups can compute the secret keys of the lower-level groups. And we know it is difficult to get the original secret from the hash value, so the lower-level groups cannot compute the secret keys of the higher-level groups. Therefore, **Proposition 3** holds. □

5 Comparison

In this section, we first define some notations of computing overload related to the proposed scheme. Then we compare the scheme with Chang's scheme[6] and Lin's scheme[19] in term of computing overload.

Notations are introduced as follows. Suppose the runtime needed for exponent arithmetic (EXP) is T_e, the runtime needed for hash arithmetic (Hash) is T_h, the runtime needed for modular multiplication is T_m, and the runtime needed for inverse operation is T_i. Here, the runtime needed for exclusive-or operation T_x and addition T_a are not computed as in [19], since the computation cost are negligible.

We give a specific model based on our scheme to make a quantized analysis and comparison. We assume that there are n participants form m groups, which are considered as access structures. Every access structure shares one key S_j, and each participant in the corresponding access structure is assigned to one share of the key K_i. The computation overload produced in share generation is $n(T_m + T_i)$ and the computation cost of key generation is nT_h. Comparing to the computing overload of Chang's scheme[6] and Lin's scheme[19], the former is nT_e, and the later one is nT_h. Since the runtime of an exponentiation operation is longer than the one of one-way hash function, it is obvious that our scheme and Lin's scheme are more efficient than Chang's scheme. On the other hand, Lin's scheme needs more computing overload to produce related parameters besides the key generation, while our scheme doesn't need such computing costs. In this point, our scheme is the most efficient in the three schemes.

6 Conclusions

In this paper, we considered a novel, simple, efficient generalized secret sharing scheme with linear hierarchical secrets by using a matrix to express the relation between the secret keys of the users and the certain access structures

admit our secret sharing scheme. The users in the corresponding access structures produce the secrets with their secret keys together. Then, after transferring the matrix to modular arithmetic, we calculate the keys with Chinese Remainder Theorem. A set of users $U=\{U_1,U_2,...,U_m\}$ can join one or more groups, forming different access structures $\Gamma'=\{\Gamma_1,\Gamma_2,...,\Gamma_n\}$. The participants in one access structure Γ_j can share the corresponding secret S_j, which can be reconstructed by the cooperation of the participants. There is a hierarchy among the shared secrets. In addition, the secret also can be revealed by using a set of hash functions consecutively. The correctness and security of the proposed scheme imply that only authorized participants in an access structures can reconstruct the shared secret with different levels, and unauthorized sets of participants are not able to reconstruct the corresponding shared secret.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems*, vol. 1, pp. 239-248, 1983.

[2] C. Asmuth and J. Bloom, "A Modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 30, pp. 208-210, 1983.

[3] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," *Advances in Cryptology-Crypto '88*, pp. 27-35, Santa Barbara, California, USA,1990.

[4] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of the 1979 National Computer Conference*, pp. 313-317, New York, U.S.A., 1979.

[5] E. F. Brickell, "Some ideal secret sharing schemes," *Advances in Cryptology-Eurocrypt '89*, pp. 468-475, Houthalen, Belgian, 1990.

[6] C. C. Chang, C. H. Lin, W. Lee, and P. C. Hwang, "Secret sharing with access structures in a hierarchy," *International Conference on Advanced Information Networking and Applications 2004 (AINA)*, pp. 31-34, Fukuoka, Japan,2004.

[7] C. C. Chang, "On the design of a key-lock-pair mechanism in information protection systems," *BIT Numerical Mathematics*, vol. 26, pp. 410-417, 1986.

[8] G. Cheng and C. C. Chang, "An authenticated group key distribution protocol based on the generalized Chinese remainder theorem," *International Journal of Communication Systems 2012*; *In Press*, DOI: 10.1002/dac.2348.

[9] R. D'Souza, D. Jao, I. Mironov and O. Pandey, "Publicly verifiable secret sharing for cloud-based key management," *Advances in Cryptology - Indocrypt '11*, pp. 339-352, Chennai, India, 1995.

[10] O. Farràs and C. Padró, "Ideal hierarchical secret sharing schemes," *Theory of Cryptography*, LNCS 5978, pp. 219-236, Spriger-Verlag, 2010.

[11] L. Harn and C. L. Lin, "Authenticated group key transfer protocol based on secret sharing," *IEEE Transactions on Computers*, vol. 59, no. 6, pp. 842-846, 2010.

[12] C. F. Hsua, Q. Cheng, X. M. Tang and B. Zeng, "An ideal multi-secret sharing scheme based on MSP," *Information Sciences*, vol. 181, no.7, pp. 1403-1409, 2011.

[13] S. Iftene and I. Bourcanu, "Weighted threshold secret sharing based on the chinese remainder theorem," *Scientific Annals of Cuza University*, vol. 15, pp. 161-172, 2005.

[14] M. Ito, A. Saito and T. Nishizeki, "Secret sharing scheme realizing any access structure," *Proceedings of the IEEE Globecom '87*, pp. 99-102, Tokyo, Japan, 1987.

[15] W. A. Jackson, K. M. Martin and C. M. O'Keefe, "Ideal secret sharing schemes with multiple secrets," *Journal of Cryptology*, vol. 9, no. 4, pp. 233-250, 1996.

[16] S. C. Kothari, "Generalized linear threshold scheme," *Advances in Cryptology-Crypto '84,* pp. 231-241, Santa Barbara, USA,1985.

[17] C. Y. Lee, Z. H. Wang, L. Harn and C. C. Chang, "Secure key transfer protocol based on secret sharing for group communications," *IEICE Transactions on Information and Systems*, vol. 94, no.11, pp. 2069-2076, 2011.

[18] C. H. Lin, "Dynamic key management schemes for access control a hierarchy," *Computer Communications*, vol. 20, no.15, pp. 1381-1385, 1997.

[19] C. H. Lin, and W. Lee, "Efficient secret sharing with access structures in a hierarchy," *International Conference on Advanced Information Networking and Applications 2005 (AINA)*, pp. 123-126, Tamkang University, Taiwan, 2005.

[20] G. PremKumer, and P. Venkateram, "Security management architecture for access control to network resources," *IEEE Proceedings–Computers and Digital Techniques*, vol. 144, no. 6, pp. 362-370, 1997.

[21] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, pp. 59-61, N.Y., 1994.

[22] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no.11, pp. 612-613, 1979.

[23] G. J. Simmons, "An introduction to shared secret and/or shared control schemes and their applications," *Contemporary Cryptology*, pp. 441-497, IEEE Press, New York, 1991.

[24] G. J. Simmons, "How to (really) share a secret," *Advances in Cryptology-Crypto '88*, pp. 390-448, Santa Barbara, USA,1990.

[25] N. Sklavos and K. Odysseas, "Access control in networks hierarchy: implementation of key management protocol," *International Journal of Network Security*, vol. 1, pp. 103–109, 2005.

[26] D. R. Stinson, "An explication of secret sharing schemes," *Design, Codes, and Cryptography*, vol. 2, no. 4, pp. 357-390, 1992.

[27] T. Tassa, "Hierarchical threshold secret sharing," *Theory of Cryptography*, pp. 473-490, Cambridge, USA, 2004.

[28] S. F. Tzeng, C. C. Lee and T. C. Lin, "A novel key management scheme for dynamic access control in a hierarchy," *International Journal of Network Security*, vol.12, pp. 178-180, 2011.

[29] M. L. Wu and T.Y. Hwang, "Access control with single-key-lock," *IEEE Transactions on Software Engineering*, vol. SE-10, no. 2, pp. 185-191. 1984.

[30] Q. Zhang, Y. K. Wang and J. P. Jue, "A key management scheme for hierarchical access control in group communication," *International Journal of Network Security*, vol. 7, pp. 323-334, 2008.

[31] D. W. Zhao, H. P. Peng, C. Wang and Y.X. Yang, "A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure," *Computers and Mathematics with Applications*, vol. 64, no. 4, pp. 611-615, 2012.

Xi Chen is currently pursuing the PhD degree with Department of Information and Communication Engineering in Beijing Jiaotong University. Her research interests include cryptographic protocols and information security.

Yun Liu is a professor of Communication and Information Systems, Beijing Jiaotong University. Her current research interests include Computer Networks, Telecommunication, Network Security, Intelligent Transportation System, Social Dynamics, etc. Dr. Liu has edited many books and published over 200 papers and book chapters, as well as participated in many international academic activities, including the organization of several international conferences.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. His current research interests include database design, computer cryptography, image compression and data structures.

Cheng Guo received the B.S. degree in computer science from Xi'an University of Architecture and Technology in 2002. He received the M.S. degree in 2006 and his Ph.D in computer application and technology, in 2009, both from the Dalian University of Technology, Dalian, China. Now he is as a post doc in the National Tsing Hua University, Hsinchu, Taiwan. His current research interests include information security and cryptology.