

Secret Sharing in Graph-Based Prohibited Structures

Hung-Min Sun
Department of Information Management
Chaoyang Institute of Technology
Wufeng, Taichung County, Taiwan 413
Email: hmsun@dscs2.csie.nctu.edu.tw

Shiuh-Pyng Shieh
Department of Computer Science
and Information Engineering
National Chiao Tung University
Hsinchu, Taiwan 30050
Email: ssp@csie.nctu.edu.tw

Abstract

A secret sharing scheme for the prohibited structure is a method of sharing a master key among a finite set of participants in such a way that only certain pre-specified subsets of participants cannot recover the master key. A secret sharing scheme is called perfect if any subset of participants who cannot recover the master key obtains no information regarding the master key. In this paper, we propose an efficient construction of perfect secret sharing schemes for graph-based prohibited structures where a vertex denotes a participant and an edge does a pair of participants who cannot recover the master key. The information rate of our scheme is $2/n$, where n is the number of participants.

1: Introduction

In 1987, Ito et al. [1] described a general method of secret sharing called *secret sharing scheme* (SSS) which allows a master key to be shared among a finite set of participants in such a way that only certain pre-specified subsets of participants can recover the master key. Let P be the set of participants. The collection of subsets of participants that can reconstruct the master key in this way is called *access structure* (denoted by Γ). The collection of subsets of participants that cannot reconstruct the master key is called *prohibited structure* (denoted by Δ) [2]. The natural restriction is that Γ is monotone increasing and Δ is monotone decreasing, that is,

if $A \in \Gamma$ and $A \subseteq B \subseteq P$, then $B \in \Gamma$, and

This research was supported by the National Science Council, Taiwan under grant number NSC-85-2213-E-009-032 and NSC-86-2213-E-324-002.

if $A \in \Delta$ and $B \subseteq A \subseteq P$, then $B \in \Delta$.

If $\Delta = 2^P \setminus \Gamma$, then we say the structure (Γ, Δ) is *complete* [2]. In the special case where $\Gamma = \{ A \mid A \subseteq P \text{ and } |A| \geq m \}$ and $\Delta = \{ A \mid A \subseteq P \text{ and } |A| \leq m-1 \}$, the secret sharing scheme is called an (m, n) -threshold scheme [3,4], where $|P| = n$. Let \mathbf{K} be the master key space and \mathbf{S} be the share space. The information rate of the secret sharing scheme is defined as $\log_2 |\mathbf{K}| / \log_2 |\mathbf{S}|$ [5]. A secret sharing scheme is *perfect* if any set of participants in the prohibited structure Δ obtains no information regarding the master key [6-9]. Secret sharing schemes are classified into the following types:

Type I: A secret sharing scheme for the *access structure* Γ is a method of sharing a master key among a finite set of participants in such a way that only subsets of participants in Γ can recover the master key while other subsets cannot. That is, $\Delta (= 2^P \setminus \Gamma)$ is implied.

Type II: A secret sharing scheme for the *prohibited structure* Δ is a method of sharing a master key among a finite set of participants in such a way that only subsets of participants in Δ cannot recover the master key while other subsets can. That is, $\Gamma (= 2^P \setminus \Delta)$ is implied.

Type III: A secret sharing scheme for the *mixed structure* (Γ, Δ) is a method of sharing a master key among a finite set of participants in such a way that subsets of participants in Γ can recover the master key but subsets of participants in Δ cannot recover the master key. That is, the privileges of subsets in $2^P \setminus (\Gamma \cup \Delta)$ are not cared. Any subset of participants in $2^P \setminus (\Gamma \cup \Delta)$ may either recover the master key or not. Note that here $\Gamma \cap \Delta = \emptyset$, and $\Gamma \cup \Delta \subseteq 2^P$.

Given any access structure Γ , Ito et al. [1,8] showed that there exists a perfect secret sharing scheme to realize the structure. Benaloh and Leichter [10] proposed a different algorithm to realize secret sharing schemes for any given monotone access structure. In both constructions, the information rate decreases exponentially as a function of n , the number of participants.

There are several performance and efficiency measures proposed for analyzing secret sharing schemes [5,11-14]. Their goal is to maximize the information rate of a secret sharing scheme. Brickell and Stinson [5] studied a perfect secret sharing scheme for graph-based access structure Γ where the monotone-increasing access structure Γ contains the pairs of participants corresponding to edges (the prohibited structure is implied to be the collection of subsets of participants corresponding to any independent set of the graph). They proved that, for any graph G with n vertices having maximum degree d , there exists a perfect secret sharing scheme for the access structure based on G in which the information rate is at least $2/(d+3)$. Stinson [14] improved the general result that there exists a perfect secret sharing scheme realizing access structure based on G in which the information rate is at least $2/(d+1)$. After that, van Dijk [12] showed that Stinson's lower bound is tight because he proved that there exists graphs having maximum degree d such that the optimal information rate is at most $2/(d+1-\epsilon)$ for all $d \geq 3$ and $\epsilon > 0$. Secret sharing schemes for mixed structures (Γ, Δ) proposed by Shieh and Sun in 1994 [15] were based on the graph where Γ contains the pairs of participants corresponding to edges and Δ contains the pairs of participants corresponding to non-edges. The information rate of their scheme is $1/(2n)$, where n is the number of participants. In 1996, Sun and Shieh [16] improved the information rate of the secret sharing scheme to be $1/(n-1)$. They also presented an application of the secret sharing scheme for a graph-based structure to reduce storage and computation load on the key distribution server in a secure network [16].

In this paper, we study the perfect secret sharing scheme for a prohibited structure based on the graph where the monotone-decreasing prohibited structure Δ contains all participants and the pairs of participants corresponding to edges (the access structure is implied to be the union of $\{A \mid A \subseteq P \text{ and } |A| \geq 3\}$ and the pairs of participants corresponding to non-edges of the graph). We propose an efficient perfect secret sharing scheme for the graph-based prohibited structure. The information rate of our scheme is $2/n$, where n is the number of participants. Our scheme can be also applied to the reduction of storage and computation loads on the key

distribution server in a secure network and can obtain better efficiency than the scheme proposed in [16].

This paper is organized as follows. In section 2, we give some preliminaries which will be used later on to construct the perfect secret sharing schemes for graph-based prohibited structures. In section 3, we propose a construction of perfect secret sharing schemes for graph-based prohibited structures. An example of perfect secret sharing scheme for the graph-based prohibited structure is demonstrated in section 4. Finally, we conclude the paper in section 5.

2: Preliminaries

2.1: Perfect (m, n) Threshold Schemes

The (m, n) threshold schemes were introduced by Blakley and Shamir in 1979 [3,4]. The main idea underlying an (m, n) threshold scheme is to divide the master key K into n shares S_i 's corresponding to n participants ($1 \leq i \leq n$) in such a way that the master key K cannot be reclaimed unless m shares are collected. Apparently, the (m, n) threshold scheme is the special case of secret sharing schemes when the qualified subsets of participants are all subsets whose order are larger than or equal to m and the non-qualified subsets of participants are all subsets whose order are less than or equal to $m-1$.

A secret sharing scheme is *perfect* if any unqualified subset of participants provide no information about the shared secret K [6,8]. It means that the prior probability $p(K = K_0)$ equals the conditional probability $p(K = K_0 \mid \text{given any or less secret shares of an unqualified set})$. By using the entropy function H from [6,7,9], we can state the requirements for an (m, n) threshold scheme as follows:

$$(1) H(K \mid S_{i_1}, \dots, S_{i_m}) = 0$$

$$(2) H(K \mid S_{i_1}, \dots, S_{i_{m-1}}) = H(K)$$

for an arbitrary set of m indices $\{i_1, \dots, i_m\}$ from $\{1, \dots, n\}$.

As an example, we review the (m, n) threshold scheme proposed by Shamir [4] as follows.

We assume that the master key K is taken randomly from $\text{GF}(q)$. Therefore, $H(K) = \log q$.

Let $f(x) = a_{m-1}x^{m-1} + \dots + a_1x + K \pmod{q}$ be a polynomial of degree $m-1$ over the finite field $\text{GF}(q)$. The n shares S_i 's are computed from $f(x)$ as follows,

$$S_i = f(i) \pmod{q}, i = 1, \dots, n.$$

Obviously, given any m secret shares S_{i_1}, \dots, S_{i_m} , $\{i_1, \dots, i_m\} \subset \{1, \dots, n\}$, $f(x)$ can be reconstructed from the Lagrange interpolating polynomial as follows [6],

$$f(x) = \sum_{k=1}^m (S_{i_k} \cdot \prod_{j=1, j \neq k}^m \frac{(x-i_j)}{(i_k-i_j)}) \pmod{q}.$$

Thus, the master key K can be obtained by $f(0)$. On the other hand, given any $m-1$ secret shares $S_{i_1}, \dots, S_{i_{m-1}}$, $\{i_1, \dots, i_{m-1}\} \subset \{1, \dots, n\}$, $f(0)$ can be written as follows.

$$f(0) = a + S_{i_m} \cdot b \pmod{q}, \text{ where}$$

$$a = \sum_{k=1}^{m-1} (S_{i_k} \cdot \prod_{j=1, j \neq k}^{m-1} \frac{(0-i_j)}{(i_k-i_j)}) \text{ and } b = \prod_{j=1}^{m-1} \frac{(0-i_j)}{(i_m-i_j)}.$$

Because S_{i_m} is uniformly distributed over $\text{GF}(q)$, $H(K | S_{i_1}, \dots, S_{i_{m-1}}) = H(f(0) | S_{i_1}, \dots, S_{i_{m-1}}) = H(a + S_{i_m} \cdot b) = H(S_{i_m}) = \log q = H(K)$. Therefore, the (m, n) threshold scheme is perfect.

2.2: Perfect Secret Sharing Schemes for Mixed Structures (Γ, Δ)

In the section, we give a construction of perfect secret sharing schemes for mixed structures (Γ, Δ) , where $\Gamma = \{P\}$ and $\Delta = \{A | A \subseteq P \text{ and } |A| \leq |P| - 2\}$. The secret sharing scheme will be used later on to construct the perfect secret sharing schemes for graph-based prohibited structures.

We assume that the master key $K = (K_1, K_2)$ is taken randomly from $\text{GF}(q) \times \text{GF}(q)$. It is clear that $H(K) = 2 \log q$.

Let $f(x) = a_{n-1}x^{n-1} + \dots + a_2x^2 + K_1x + K_2 \pmod{q}$ be a polynomial of degree $n-1$ over the finite field $\text{GF}(q)$. The n shares S_i 's are computed from $f(x)$ as follows, $S_i = f(i) \pmod{q}$, $i = 1, \dots, n$.

Obviously, given n secret shares S_i , $i = 1, \dots, n$, $f(x)$ can be reconstructed from the Lagrange interpolating polynomial as follows [6],

$$f(x) = \sum_{k=1}^n (S_k \cdot \prod_{j=1, j \neq k}^n \frac{(x-j)}{(k-j)}) \pmod{q}.$$

Thus, the master key K can be obtained from $f(x)$. On the other hand, given any $n-2$ secret shares $S_{i_1}, \dots, S_{i_{n-2}}$, $\{i_1, \dots, i_{n-2}\} \subset \{1, \dots, n\}$, we can get the following relations:

$$\begin{bmatrix} i_1^{n-1} & \dots & i_1 & 1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ i_{n-4}^{n-1} & \dots & i_{n-4} & 1 \\ i_{n-3}^{n-1} & \dots & i_{n-3} & 1 \\ i_{n-2}^{n-1} & \dots & i_{n-2} & 1 \end{bmatrix} \begin{bmatrix} a_{n-1} \\ \cdot \\ \cdot \\ a_2 \\ K_1 \\ K_2 \end{bmatrix} = \begin{bmatrix} S_{i_1} \\ \cdot \\ \cdot \\ S_{i_{n-4}} \\ S_{i_{n-3}} \\ S_{i_{n-2}} \end{bmatrix} \pmod{q}.$$

Because there are n unknown variables, $a_{n-1}, \dots, a_2, K_1, K_2$, among these $n-2$ equations, it is clear that the total number of possible solutions for $K = (K_1, K_2)$ is q^2 . Note that once the secret (K_1, K_2) is chosen, the system has a unique solution over the field $\text{GF}(q)$. Hence, $H(K | S_{i_1}, \dots, S_{i_{n-2}}) = H(K_1, K_2 | S_{i_1}, \dots, S_{i_{n-2}}) = 2 \log q = H(K)$. Therefore, the secret sharing scheme for the mixed structure (Γ, Δ) is perfect.

3: Construction of Perfect SSS for Prohibited Structures Based on Graphs

Let P be the set of participants, and G be a graph where a vertex denotes a participant in P and an edge does a pair of participants. In a *perfect* secret sharing scheme for the prohibited structure based on G , a pair of participants corresponding to an edge of G cannot obtain any information regarding the master key. In addition, we also assume that each participant corresponding to a vertex of G cannot obtain any information regarding the master key. This is because that if one participant is allowed to recover the master key by himself, we can assign the master key as his share and remove him from the graph G . The graph we consider here may include disconnected graphs and isolated vertices. A participant corresponding to an isolated vertex can be interpreted as that he can recover the master key in cooperation with any participant in the graph except himself. We use $E(G)$ to denote the set of edges of G ; $E(\overline{G})$ to denote the set of edges of \overline{G} , where \overline{G} is the complement of G ; S to denote the set of pairs of participants corresponding to edges in $E(G)$; R to denote the set of pairs of participants corresponding to edges in $E(\overline{G})$. It is reasonable to restrict that the prohibited structure and the access structure are monotone. Thus, given a graph G , the prohibited structure is denoted by $\Delta = \{A | A \subseteq P \text{ and } |A| = 1\} \cup \{A | A \in S\}$, and then the access structure is decided by $2^P \setminus \Delta = \{A | A \subseteq P \text{ and } |A| \geq 3\} \cup \{A | A \in R\}$.

In the following, we will use the conventional threshold schemes [3,4] to construct the perfect secret sharing schemes for graph-based prohibited structures.

We assume that all computations are over $GF(q)$ where q is a prime.

Given a graph G for the prohibited structure, a perfect secret sharing scheme is constructed as follows. Assume that $P = \{ p_1, p_2, \dots, p_n \}$ is the set of participants corresponding to the vertices of the graph G . We first construct $n+1$ conventional $(2, n)$ -threshold schemes [3,4], named $TS_1, TS_2, \dots,$ and TS_{n+1} . To avoid ambiguity, we call the master key and the shares of each TS_i sub-master key and sub-shares, respectively. For each $(2, n)$ - TS_i , let Sk_i be its sub-master key and $s_{i,1}, s_{i,2}, \dots, s_{i,n}$ be its n sub-shares. Thus, given any two sub-shares, $s_{i,j}$ and $s_{i,k}$ ($1 \leq j < k \leq n$), the sub-master key Sk_i can be recovered, but less than two sub-shares provide no information about Sk_i .

The master key of the secret sharing scheme for the prohibited structure based on the graph G is given by $K = (K_1, K_2)$, which is protected by these sub-master keys $Sk_1, Sk_2, \dots, Sk_n, Sk_{n+1}$ in such a way that all $n+1$ sub-master keys $Sk_1, Sk_2, \dots, Sk_n, Sk_{n+1}$ collected together, the master key K can be recovered, but any $n-1$ or less sub-master keys provide no information regarding the master key. It is easy to construct such protection mechanism following the method proposed in section 2.2.

The share of participant p_i is given by

$$S_i = \langle a_{i,1}, \dots, a_{i,t}, \dots, a_{i,n}, a_{i,n+1} \rangle,$$

where $1 \leq t \leq n+1$,

$$a_{i,t} \text{ is empty if } t = i,$$

$$a_{i,t} = s_{i,i} \text{ if } t = n+1 \text{ and } p_i \text{ is an isolated vertex,}$$

$$a_{i,t} = Sk_i \text{ if } t = n+1 \text{ and } p_i \text{ is not an isolated vertex,}$$

$$a_{i,t} = s_{i,i} \text{ if } t \neq i, t \neq n+1, \text{ and } \overline{p_i p_t} \text{ is an edge of } G,$$

$$a_{i,t} = Sk_i \text{ if } t \neq i, t \neq n+1, \text{ and } \overline{p_i p_t} \text{ is not an edge of } G.$$

Thus, the constructed secret sharing scheme satisfies:

- (1) if $A \in \mathcal{S}$, A obtains no information regarding the master key,
- (2) if $A \subseteq P$ and $|A| = 1$, A obtains no information regarding the master key,
- (3) if $A \in \mathcal{R}$, A can recover the master key,
- (4) if $A \subseteq P$ and $|A| \geq 3$, A can recover the master key.

THEOREM 1. If $A \in \mathcal{S}$, A obtains no information regarding the master key of the constructed secret sharing scheme for the prohibited structure based on the graph G .

PROOF. We assume that $A = \{ p_i, p_j \}$, where $i \neq j$. The share of p_i is $S_i = \langle a_{i,1}, a_{i,2}, \dots, a_{i,n+1} \rangle$ and the share of p_j is $S_j = \langle a_{j,1}, a_{j,2}, \dots, a_{j,n+1} \rangle$. Because $A \in \mathcal{S}$, $\overline{p_i p_j}$ is an edge of G . We conclude that for any t , $1 \leq t \leq n+1$, one of the following four cases holds.

- (1) $a_{i,t} = Sk_i$ and $a_{j,t} = Sk_i$ if $t = n+1$,
- (2) $a_{i,t}$ is empty and $a_{j,t} = s_{i,j}$ if $t = i$,
- (3) $a_{i,t} = s_{i,i}$ and $a_{j,t}$ is empty if $t = j$,
- (4) $a_{i,t} = s_{i,i}$ or Sk_i , and $a_{j,t} = s_{i,j}$ or Sk_i if $t \neq n+1, t \neq i$, and $t \neq j$.

In case (1) and (4), the sub-master key Sk_i can be recovered. In case (2), $a_{i,i}$ and $a_{j,i}$ can obtain only one sub-share $s_{i,j}$ of the $(2, n)$ - TS_i . Therefore, p_i and p_j get no information about the sub-master key Sk_i . In case (3), $a_{i,j}$ and $a_{j,j}$ can obtain only one sub-share $s_{j,i}$ of the $(2, n)$ - TS_j . Therefore, p_i and p_j get no information about the sub-master key Sk_j . Hence, p_i and p_j can obtain only $n-1$ sub-master keys which provide no information regarding the master key K .

(Q.E.D.)

THEOREM 2. If $A \subseteq P$ and $|A| = 1$, A obtains no information regarding the master key of the constructed secret sharing scheme for the prohibited structure based on the graph G .

PROOF. This means the case that each participant obtains no information regarding the master key. We assume that $A = \{ p_i \}$ and the share of p_i is $S_i = \langle a_{i,1}, a_{i,2}, \dots, a_{i,n+1} \rangle$. If p_i is not an isolated vertex, then there exists a vertex p_j such that $\overline{p_i p_j}$ is an edge of G . From Theorem 1, we know that $\{ p_i, p_j \}$ obtains no information regarding the master key. Therefore, $A = \{ p_i \}$ obtains no information regarding the master key.

If p_i is not an isolated vertex, we conclude that for any t , $1 \leq t \leq n+1$, one of the following three cases holds.

- (1) $a_{i,t} = s_{i,i}$ if $t = n+1$,
- (2) $a_{i,t}$ is empty if $t = i$,
- (3) $a_{i,t} = Sk_i$ if $t \neq n+1, t \neq i$.

In case (1) and case (2), p_i gets no information about the sub-master key Sk_{n+1} and Sk_i . Hence, p_i can obtain only $n-1$ sub-master keys which provide no information regarding the master key K . (Q.E.D.)

THEOREM 3. If $A \in R$, A can recover the master key of the constructed secret sharing scheme for the prohibited structure based on the graph G .

PROOF. We assume that $A = \{ p_i, p_j \}$, where $i \neq j$. The share of p_i is $S_i = \langle a_{i,1}, a_{i,2}, \dots, a_{i,n+1} \rangle$ and the share of p_j is $S_j = \langle a_{j,1}, a_{j,2}, \dots, a_{j,n+1} \rangle$. Because $A \in R$, $\overline{p_i p_j}$ is a non-edge of G . We conclude that for any t , $1 \leq t \leq n+1$, one of the following three cases holds.

- (1) $a_{i,t} = \text{empty}$ and $a_{j,t} = Sk_t$ if $t = i$,
- (2) $a_{i,t} = Sk_t$ and $a_{j,t} = \text{empty}$ if $t = j$,
- (3) $a_{i,t} = s_{i,j}$ or Sk_t , and $a_{j,t} = s_{i,j}$ or Sk_t if $t \neq i$, and $t \neq j$.

In all these cases (1),(2), and (3), the sub-master key k_i can be recovered. Thus, participant p_i and participant p_j can recover all $n+1$ sub-master keys $Sk_1, Sk_2, \dots, Sk_{n+1}$ and hence the master key K . (Q.E.D.)

THEOREM 4. If $A \subseteq P$ and $|A| \geq 3$, A can recover the master key of the constructed secret sharing scheme for the prohibited structure based on the graph G .

PROOF. Without loss of generality, we assume that $A = \{ p_i, p_j, p_k \}$, where i, j , and k are distinct. If there exists a pair of participants of A belongs to R , then the master key can be recovered from Theorem 3. All we need to consider is the case that all $\overline{p_i p_j}$, $\overline{p_i p_k}$, and $\overline{p_j p_k}$ are edges of G . From Theorem 1, we know that p_i and p_j can recover all sub-master keys except Sk_i and Sk_j . Similarly, p_i and p_k can recover all sub-master keys except Sk_i and Sk_k . Also, p_j and p_k can recover all sub-master keys except Sk_j and Sk_k . Therefore, p_i, p_j , and p_k can recover all sub-master keys $Sk_1, Sk_2, \dots, Sk_{n+1}$ and hence the master key K .

(Q.E.D.)

The share of participant p_i ($= \langle a_{i,1}, \dots, a_{i,i}, \dots, a_{i,n}, a_{i,n+1} \rangle$) is an $(n+1)$ -dimensional vector. Except that $a_{i,i}$ is empty, every $a_{i,j}$ is over $GF(q)$. Therefore, the size of the share space is q^n . Because the master key K is equal to (K_1, K_2) , the size of the master key space is q^2 . It is clear that the information rate of our secret sharing scheme for the graph-based prohibited structure is $\log q^2 / \log q^n = 2/n$, where n is the number of participants.

4: An Example of Perfect SSS for a Prohibited Structure

We demonstrate the use of our method in the following example. In Figure 1, the graph G denotes the prohibited structure with six participants. Therefore, $E(G) = \{ \overline{p_1 p_3}, \overline{p_1 p_5}, \overline{p_2 p_5}, \overline{p_2 p_6}, \overline{p_3 p_5}, \overline{p_3 p_6} \}$ and $E(\overline{G}) = \{ \overline{p_1 p_2}, \overline{p_1 p_4}, \overline{p_1 p_6}, \overline{p_2 p_3}, \overline{p_2 p_4}, \overline{p_3 p_4}, \overline{p_4 p_5}, \overline{p_4 p_6}, \overline{p_5 p_6} \}$. The secret sharing scheme for the prohibited structure based on the graph G is constructed as follows.

Let $P = \{ p_1, p_2, p_3, p_4, p_5, p_6 \}$. Thus,

$S =$
 $\{ \{ p_1, p_3 \}, \{ p_1, p_5 \}, \{ p_2, p_5 \}, \{ p_2, p_6 \}, \{ p_3, p_5 \}, \{ p_3, p_6 \} \}$ and

$R =$
 $\{ \{ p_1, p_2 \}, \{ p_1, p_4 \}, \{ p_1, p_6 \}, \{ p_2, p_3 \}, \{ p_2, p_4 \}, \{ p_3, p_4 \}, \{ p_4, p_5 \}, \{ p_4, p_6 \}, \{ p_5, p_6 \} \}$.

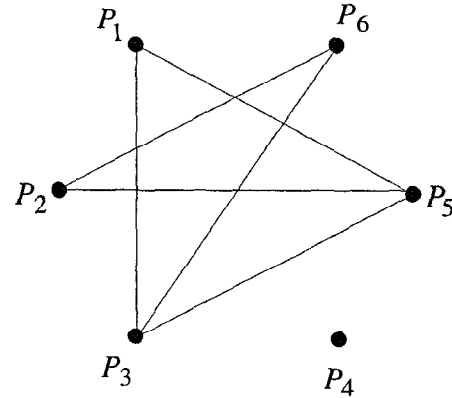


Figure 1: Graph G with six participants

The prohibited structure

$\Delta =$
 $\{ \emptyset, \{ p_1 \}, \{ p_2 \}, \{ p_3 \}, \{ p_4 \}, \{ p_5 \}, \{ p_6 \}, \{ p_1, p_3 \}, \{ p_1, p_5 \}, \{ p_2, p_5 \}, \{ p_2, p_6 \}, \{ p_3, p_5 \}, \{ p_3, p_6 \} \}$.

The access structure

$\Gamma =$
 $\{ \{ p_1, p_2 \}, \{ p_1, p_4 \}, \{ p_1, p_6 \}, \{ p_2, p_3 \}, \{ p_2, p_4 \}, \{ p_3, p_4 \}, \{ p_4, p_5 \}, \{ p_4, p_6 \}, \{ p_5, p_6 \}, \{ p_1, p_2, p_3 \}, \{ p_1, p_2, p_4 \}, \{ p_1, p_2, p_5 \}, \{ p_1, p_2, p_6 \}, \{ p_1, p_3, p_4 \}, \{ p_1, p_3, p_6 \}, \{ p_1, p_4, p_5 \}, \{ p_1, p_4, p_6 \}, \{ p_1, p_5, p_6 \}, \{ p_2, p_3, p_4 \}, \{ p_2, p_3, p_5 \}, \{ p_2, p_3, p_6 \} \}$.

$\{ p_2, p_4, p_5 \}, \{ p_2, p_4, p_6 \}, \{ p_2, p_5, p_6 \},$
 $\{ p_3, p_4, p_5 \}, \{ p_3, p_4, p_6 \}, \{ p_3, p_5, p_6 \},$
 $\{ p_4, p_5, p_6 \}, \{ p_1, p_2, p_3, p_4 \}, \{ p_1, p_2, p_3, p_5 \},$
 $\{ p_1, p_2, p_3, p_6 \}, \{ p_1, p_2, p_4, p_5 \}, \{ p_1, p_2, p_4, p_6 \},$
 $\{ p_1, p_2, p_5, p_6 \}, \{ p_1, p_3, p_4, p_5 \}, \{ p_1, p_3, p_4, p_6 \},$
 $\{ p_1, p_3, p_5, p_6 \}, \{ p_1, p_4, p_5, p_6 \}, \{ p_2, p_3, p_4, p_5 \},$
 $\{ p_2, p_3, p_4, p_6 \}, \{ p_2, p_3, p_5, p_6 \}, \{ p_2, p_4, p_5, p_6 \},$
 $\{ p_3, p_4, p_5, p_6 \}, \{ p_1, p_2, p_3, p_4, p_5 \},$
 $\{ p_1, p_2, p_3, p_4, p_6 \}, \{ p_1, p_2, p_3, p_5, p_6 \},$
 $\{ p_1, p_2, p_4, p_5, p_6 \}, \{ p_1, p_3, p_4, p_5, p_6 \},$
 $\{ p_2, p_3, p_4, p_5, p_6 \}, \{ p_1, p_2, p_3, p_4, p_5, p_6 \} \}.$

Let $TS_1, TS_2, \dots,$ and TS_7 be seven (2, 6)-threshold schemes. We assume that Sk_i is the sub-master key of TS_i and $s_{i,1}, s_{i,2}, \dots,$ and $s_{i,6}$ are the sub-shares of TS_i , for $1 \leq i \leq 7$. Here we use Shamir's method [4] to construct these threshold schemes. For each (2,6)- TS_i , let

$$f_i(x) = r_i \cdot x + Sk_i \pmod{q}$$

be a secret polynomial of degree 1 over the finite field $GF(q)$, where q is a prime. Let ID_j denote the identity of the participant p_j . The 6 sub-shares $s_{i,1}, \dots, s_{i,6}$ are computed from $f_i(x)$ as follows:

$$s_{i,j} = f_i(ID_j) \pmod{q}, j = 1, \dots, 6.$$

Obviously, given any two sub-shares, $s_{i,j}$ and $s_{i,k}$, $f_i(x)$ can be reconstructed from the Lagrange interpolating polynomial as follows [6]:

$$f_i(x) = s_{i,j} \cdot \frac{(x - ID_k)}{(ID_j - ID_k)} + s_{i,k} \cdot \frac{(x - ID_j)}{(ID_k - ID_j)} \pmod{q}.$$

Thus, the sub-master key Sk_i ($= f_i(0)$) can be obtained, but less than two sub-shares provide no information about the sub-master key.

The master key of the secret sharing scheme is given by $K = (K_1, K_2)$ which is protected by these sub-master keys Sk_1, Sk_2, \dots, Sk_7 in such a way that all seven sub-master keys collected together, the master key K can be recovered, but any five or less sub-master keys provide no information regarding the master key (See section 2.2). The shares of participants are given by:

$$\begin{aligned}
S_1 &= \langle -, Sk_2, s_{3,1}, Sk_4, s_{5,1}, Sk_6, Sk_7 \rangle, \\
S_2 &= \langle Sk_1, -, Sk_3, Sk_4, s_{5,2}, s_{6,2}, Sk_7 \rangle, \\
S_3 &= \langle s_{1,3}, Sk_2, -, Sk_4, s_{5,3}, s_{6,3}, Sk_7 \rangle, \\
S_4 &= \langle Sk_1, Sk_2, Sk_3, -, Sk_5, Sk_6, s_{7,4} \rangle,
\end{aligned}$$

$$S_5 = \langle s_{1,5}, s_{2,5}, s_{3,5}, Sk_4, -, Sk_6, Sk_7 \rangle,$$

$$S_6 = \langle Sk_1, s_{2,6}, s_{3,6}, Sk_4, Sk_5, -, Sk_7 \rangle, \text{ where}$$

'-' denotes empty entry.

In the following, we demonstrate the constructed secret sharing scheme satisfies:

- (1) if $A \in S$, A obtains no information regarding the master key,
- (2) if $A \subseteq P$ and $|A|=1$, A obtains no information regarding the master key,
- (3) if $A \in R$, A can recover the master key,
- (4) if $A \subseteq P$ and $|A| \geq 3$, A can recover the master key.

If $A = \{ p_1, p_3 \} \in \Delta$, A can not recover Sk_1 and Sk_3 . Therefore, A obtains no information about the master key K .

If $A = \{ p_4 \} \in \Delta$, A can not recover Sk_4 and Sk_7 . Therefore, A obtains no information about the master key K .

If $A = \{ p_1, p_2 \} \in \Gamma$, A can recover the master key K as follows.

- (1) Participant p_1 can obtain $Sk_2, Sk_4, Sk_6,$ and Sk_7 because he owns his share S_1 .
- (2) Participant p_2 can obtain $Sk_1, Sk_3, Sk_4,$ and Sk_7 because he owns his share S_2 .
- (3) Participants p_1 and p_2 can recover Sk_5 from $s_{3,1}$ of S_1 and $s_{5,2}$ of S_2 .

Therefore, participants p_1 and p_2 can recover all seven sub-master keys and hence the master key K .

If $A = \{ p_1, p_3, p_5 \} \in \Gamma$, A can recover the master key K as follows.

- (1) Participant p_1 can obtain $Sk_2, Sk_4, Sk_6,$ and Sk_7 because he owns his share S_1 .
- (2) Participants p_3 and p_5 can recover Sk_1 from $s_{1,3}$ of S_3 and $s_{1,5}$ of S_5 .
- (3) Participants p_1 and p_5 can recover Sk_3 from $s_{3,1}$ of S_1 and $s_{3,5}$ of S_5 .
- (4) Participants p_1 and p_3 can recover Sk_5 from $s_{5,1}$ of S_1 and $s_{5,3}$ of S_3 .

Therefore, participants $p_1, p_3,$ and p_5 can recover all seven sub-master keys and hence the master key K .

5: Conclusions

In this paper, we give a construction of perfect secret sharing schemes for mixed structures (Γ, Δ) , where $\Gamma = \{P\}$ and $\Delta = \{A \mid A \subseteq P \text{ and } |A| \leq |P| - 2\}$. Based on

the proposed perfect secret sharing schemes, we propose an efficient construction of perfect secret sharing schemes for graph-based prohibited structures where a vertex denotes a participant and an edge does a pair of participants who cannot recover the master key. The information rate of our scheme is $2/n$, where n is the number of participants.

References

- [1] M. Ito, A. Saito and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Proc. IEEE Globecom'87*, Tokyo, pp. 99-102 (1987).
- [2] W.A. Jackson, K.M. Martin and C. M. O'Keefe, "Multisecret threshold schemes," in *Advances in Cryptology-Crypto'93 Proceedings*, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, Berlin, pp. 126-135 (1994).
- [3] G.R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPs 1979 National Computer Conference*, New York, Vol. 48, pp. 313-317 (1979).
- [4] A. Shamir, "How to share a secret," *Commun. of the ACM* **22** (11) 612-613 (1979).
- [5] E.F. Brickell and D.R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *Journal of Cryptology* **5** 153-166 (1992).
- [6] D.E.R. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, MA (1983).
- [7] R.W. Hamming, *Coding and Information Theory*, Englewood Cliffs, Reading, NJ:Prentice-Hall (1986).
- [8] M. Ito, A. Saito and T. Nishizeki, "Multiple assignment scheme for sharing secret," *Journal of Cryptology* **6** 15-20 (1993).
- [9] C.E. Shannon, "Communication theory of secrecy systems," *Computer Security Journal*, **VI**(2) 7-66 (1990).
- [10] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Advances in Cryptology-Crypto'88 Proceedings*, Lecture Notes in Computer Science, Vol. 403, Springer-Verlag, Berlin, pp. 27-35 (1990).
- [11] R.M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, "On the size of shares for secret sharing schemes," in *Advances in Cryptology-Crypto'91 Proceedings*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 101-113 (1992).
- [12] M. van Dijk, "On the information rate of perfect secret sharing schemes," *Designs, Codes and Cryptography* **6** 143-169 (1995).
- [13] D.R. Stinson, "New general lower bounds on the information rate of secret sharing schemes," in *Advance in Cryptology-CRYPTO'92, Lecture Notes in Comput. Sci.*, Vol. 740, pp. 168-182 (1993).
- [14] D.R. Stinson, "Decomposition constructions for secret sharing schemes," *IEEE Trans. Inform. Theory* **40**(1) 118-125 (1994).
- [15] S.P. Shieh and H.M. Sun, "On constructing secret sharing schemes," in *Proceedings of the 1994 IEEE International Conference on Computer Communications, Networking for Global Communications (INFOCOM '94)*, pp. 1288-1292 (1994).
- [16] H.M. Sun and S.P. Shieh, "An efficient construction of perfect secret sharing schemes for graph-based structures," *Journal of Computers and Mathematics with Applications* **31**(7) 129-135 (1996).