Pergamon

Computers Math. Applic. Vol. 36, No. 7, pp. 131–140, 1998
© 1998 Elsevier Science Ltd. All rights reserved
Printed in Great Britain
0893-9659/98 $19.00 + 0.00

PII: S0898-1221(98)00177-1

Secret Sharing Schemes for Graph-Based Prohibited Structures

HUNG-MIN SUN*
Department of Information Management
Chaoyang Institute of Technology
168, Gifeng E. Rd., Wufeng, Taichung County
Taiwan 413, R.O.C.
hmsun@dscs2.csie.nctu.edu.tw

SHIUH-PYNG SHIEH
Department of Computer Science and Information Engineering
National Chiao Tung University
Hsinchu, Taiwan 30050, R.O.C.
ssp@csie.nctu.edu.tw

(Received October 1996; accepted June 1997)

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 prespecified 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. © 1998 Elsevier Science Ltd. All rights reserved.

Keywords—Cryptography, Data security, Information theory, Secret sharing scheme.

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 prespecified subsets of participants can recover the master key. Let $\mathbf{P}$ be the set of participants. The set of all subsets of $\mathbf{P}$, denoted by 2^P, is called the power set of $\mathbf{P}$. We use the notation $X \backslash Y = \{x \mid x \in X \text{ and } x \notin Y\}$ to denote the difference of two sets X and Y. 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,

$$\begin{aligned} &\text{if } \mathbf{A} \in \Gamma \text{ and } \mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{P}, && \text{then } \mathbf{B} \in \Gamma, && \text{and} \\ &\text{if } \mathbf{A} \in \Delta \text{ and } \mathbf{B} \subseteq \mathbf{A} \subseteq \mathbf{P}, && \text{then } \mathbf{B} \in \Delta. \end{aligned}$$

*Author to whom all correspondence should be sent.

This work was supported in part by the National Science Council, Taiwan, under contract NSC-87-2213-E-324-003.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

If $\Delta = 2^P \backslash \Gamma$, then we say the structure (Γ, Δ) is complete [2]. In the special case where $\Gamma = \{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P} \text{ and } |\mathbf{A}| \geq m\}$ and $\Delta = \{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P} \text{ and } |\mathbf{A}| \leq m-1\}$, the secret sharing scheme is called an (m,n)-threshold scheme [3,4], where $|\mathbf{P}| = n$. Let K be the master key space and S be the share space. The information rate of the secret sharing scheme is defined to be the ratio between the master key size and the maximum size of the shares [5]. Here we use the notation $\rho = \log_2 |\mathsf{K}| / \log_2 |\mathsf{S}|$ to denote the information rate. If a secret sharing scheme is to be practical, we do not want to have to distribute too much secret information as shares. Consequently, we want to make the information rate as high as possible. 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, $\Delta (= 2^P \backslash \Gamma)$ 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, $\Gamma (= 2^P \backslash \Delta)$ 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 $2^P \backslash (\Gamma \cup \Delta)$ can be ignored. Any subset of participants in $2^P \backslash (\Gamma \cup \Delta)$ may either recover the master key or not. Note that, here $\Gamma \cap \Delta = \varnothing$, and $\Gamma \cup \Delta \subset 2^P$.

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 exist graphs having maximum degree d such that the optimal information rate is at most $2/(d+1-\varepsilon)$, for all $d \geq 3$ and $\varepsilon > 0$. 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 nonedges. 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 $1/(n-1)$.

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 $\{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P} \text{ and } |\mathbf{A}| \geq 3\}$ and the pairs of participants corresponding to nonedges 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 applied to the reduction of storage and computation loads on the key distribution server in a secure network.

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 of graph-based prohibited structures. In Section 3, we propose a construction of perfect secret sharing schemes for graph-based prohibited structures. An example of a perfect secret sharing scheme for the graph-based prohibited structure is demonstrated in Section 4. In Section 5, we discuss the application of our construction. Finally, we conclude this paper in Section 6.

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 nonqualified 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 provides no information about the shared secret K [6,8]. It means that the prior probability $p(K = K_0)$ equals the conditional probability $p(K = K_0$ 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 Shimir [4] as follows.

We assume that the master key K is taken randomly from $GF(q)$. Therefore, $H(K) = \log q$. Let $f(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + K \pmod q$ be a polynomial of degree $m - 1$ over the finite field $GF(q)$. The n share S_i's are computed from $f(x)$ as follows:

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

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]:

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

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:

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

where

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

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

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

In this section, we give a construction of perfect secret sharing schemes for mixed structures (Γ, Δ), where $\Gamma = \{\mathbf{P}\}$ and $\Delta = \{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P} \text{ and } |\mathbf{A}| \leq |\mathbf{P}| - 2\}$. 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 $GF(q) \times GF(q)$. It is clear that $H(K) = 2 \log q$. Let $f(x) = a_{n-1}x^{n-1} + \cdots + a_2x^2 + K_1x + K_2 (\text{mod } q)$ be a polynomial of degree $n - 1$ over the finite field $GF(q)$. The n shares S_i's are computed from $f(x)$ as follows:

$$S_i = f(i) (\text{mod } q), \qquad i = 1, \ldots, n.$$

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

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

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

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

Because there are n unknown variables, $a_{n-1}, \ldots, a_2, K_1, K_2$, among these $n - 2$ equations, it is clear that the total number of possible solutions for $K = (K_1, K_2)$ is q^2. Hence, $H(K \mid S_{i_1}, \ldots, S_{i_{n-2}}) = H(K_1, K_2 \mid S_{i_1}, \ldots, S_{i_{n-2}}) = 2 \log q = H(K)$. 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 $\mathbf{P}$ be the set of participants, and G be a graph where a vertex denotes a participant in $\mathbf{P}$ and an edge denotes a pair of participants. In a *perfect* secret sharing scheme for the prohibited structure based of 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; $\mathbf{S}$ to denote the set of pairs of participants corresponding to edges in $E(G)$; $\mathbf{R}$ 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 $\Delta = \{\mathbf{A} \mid \mathbf{A} \subseteq$

$\mathbf{P}$ and $|\mathbf{A}| = 1\} \cup \{\mathbf{A} \mid \mathbf{A} \in \mathbf{S}\}$, and then the access structure is decided by $2^P \backslash \Delta = \{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P}$ and $|\mathbf{A}| \geq 3\} \cup \{\mathbf{A} \mid \mathbf{A} \in \mathbf{R}\}$.

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 $\mathbf{P} = \{p_1, p_2, \dots, p_n\}$ 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 submaster key and subshares, respectively. For each $(2,n) - TS_i$, let Sk_i be its submaster key and $s_{i,1}, s_{i,2}, \dots, s_{i,n}$ be its n subshares. Thus, given any two subshares, $s_{i,j}$ and $s_{i,k} (1 \leq j \leq k \leq n)$, the submaster key Sk_i can be recovered, but less than two subshares 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 submaster keys $Sk_1, Sk_2, \dots, Sk_n, Sk_{n+1}$ in such a way that all $n+1$ submaster 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 submaster 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 $1 \leq t \leq n+1$,

$$\begin{array}{ll}
a_{i,t} \text{ is empty} & \text{if } t = i, \\
a_{i,t} = s_{t,i} & \text{if } t = n+1 \text{ and } p_t \text{ is an isolated vertex,} \\
a_{i,t} = Sk_t & \text{if } t = n+1 \text{ and } p_t \text{ is not an isolated vertex,} \\
a_{i,t} = s_{t,i} & \text{if } t \neq i,\ t \neq n+1, \text{ and } \overline{p_i p_t} \text{ is an edge of } G, \\
a_{i,t} = Sk_t & \text{if } t \neq i,\ t \neq n+1, \text{ and } \overline{p_i p_t} \text{ is not an edge of } G.
\end{array}$$

Thus, the constructed secret sharing scheme satisfies:

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

THEOREM 1. *If $\mathbf{A} \in \mathbf{S}, \mathbf{A}$ 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 $\mathbf{A} = \{p_i, p_j\}$, 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 $\mathbf{A} \in \mathbf{S}$, $\overline{p_i p_j}$ 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) $a_{i,t} = Sk_t$ and $a_{j,t} = Sk_t$ if $t = n+1$,
(2) $a_{i,t} =$ empty and $a_{j,t} = s_{t,j}$ if $t = i$,
(3) $a_{i,t} = s_{t,i}$ and $a_{j,t} =$ empty if $t = j$,
(4) $a_{i,t} = s_{t,i}$ or Sk_t, and $a_{j,t} = s_{t,j}$ or Sk_t it $t \neq n+1, t \neq i$, and $t \neq j$.

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

THEOREM 2. *If* $\mathbf{A} \subseteq \mathbf{P}$ *and* $|\mathbf{A}| = 1, \mathbf{A}$ *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 $\mathbf{A} = \{p_i\}$ 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 $\overline{p_ip_j}$ is an edge of G. From Theorem 1, we know that $\{p_i, p_j\}$ obtains no information regarding the master key. Therefore, $\mathbf{A} = \{p_i\}$ obtains no information regarding the master key.

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

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

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

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

PROOF. We assume that $\mathbf{A} = \{p_i, p_j\}$, 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 $\mathbf{A} \in \mathbf{R}$, $\overline{p_ip_j}$ is an nonedge of G. We conclude that for any $t, 1 \le t \le n+1$, one of the following three cases holds.

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

In Cases (1)–(3), the submaster key k_t can be recovered. Thus, participant p_i and participant p_j can recover all $n+1$ submaster keys $Sk_1, Sk_2, \dots, Sk_{n+1}$, and hence, the master key K. ∎

THEOREM 4. *If* $\mathbf{A} \subseteq \mathbf{P}$ *and* $|\mathbf{A}| \ge 3, \mathbf{A}$ *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 $\mathbf{A} = \{p_i, p_j, p_k\}$, where i, j, and k are distinct. If there exists a pair of participants of $\mathbf{A}$ belongs to $\mathbf{R}$, then the master key can be recovered from Theorem 3. All we need to consider is the case that all $\overline{p_ip_j}, \overline{p_ip_k}$, and $\overline{p_jp_k}$ are edges of G. From Theorem 1, we know that p_i and p_j can recover all submaster keys except Sk_i and Sk_j. Similarly, p_i and p_k can recover all submaster keys except Sk_i and Sk_k. Also, p_j and p_k can recover all submaster keys except Sk_j and Sk_k. Therefore, p_i, p_j, and p_k can recover all submaster keys $Sk_1, Sk_2, \dots, Sk_{n+1}$, and hence, the master key K. ∎

The share of participant $p_i (= \langle a_{i,1}, \dots, a_{i,t}, \dots, a_{i,n}, a_{i,n+1}\rangle)$ 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 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, $E(G) = \{\overline{p_1p_3}, \overline{p_1p_5}, \overline{p_2p_5}, \overline{p_2p_6}, \overline{p_3p_5}, \overline{p_3p_6}\}$ and $E(\overline{G}) = \{\overline{p_1p_2}, \overline{p_1p_4}, \overline{p_1p_6}, \overline{p_2p_3}, \overline{p_2p_4}, \overline{p_3p_4}, \overline{p_4p_5}, \overline{p_4p_6}, \overline{p_5p_6}\}$. The secret sharing scheme for the prohibited structure based on the graph G is constructed as follows. Let $\mathbf{P} =$

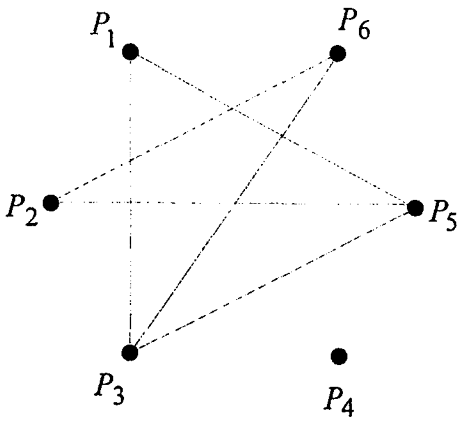

Figure 1. Graph G with six participants.

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

$$\mathbf{S} = \{\{p_1,p_3\},\{p_1,p_5\},\{p_2,p_5\},\{p_2,p_6\},\{p_3,p_5\},\{p_3,p_6\}\}, \qquad \text{and}$$
$$\mathbf{R} = \{\{p_1,p_2\},\{p_1,p_4\},\{p_1,p_6\},\{p_2,p_3\},\{p_2,p_4\},\{p_3,p_4\}\{p_4,p_5\}\{p_4,p_6\},\{p_5,p_6\}\}.$$

The prohibited structure

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

The access structure

$$\begin{aligned}\Gamma = \{&\{p_1,p_2\},\{p_1,p_4\},\{p_1,p_6\},\{p_2,p_3\},\{p_2,p_4\},\{p_3,p_4\},\{p_4,p_5\},\{p_4,p_6\}\{p_5,p_6\},\\ &\{p_1,p_2,p_3\},\{p_1,p_2,p_4\},\{p_1,p_2,p_5\},\{p_1,p_2,p_6\},\{p_1,p_3,p_4\},\{p_1,p_3,p_5\},\\ &\{p_1,p_3,p_6\},\{p_1,p_4,p_5\},\{p_1,p_4,p_6\},\{p_1,p_5,p_6\},\{p_2,p_3,p_4\},\{p_2,p_3,p_5\},\\ &\{p_2,p_3,p_6\},\{p_2,p_4,p_5\},\{p_2,p_4,p_6\},\{p_2,p_5,p_6\},\{p_3,p_4,p_5\},\{p_3,p_4,p_6\},\\ &\{p_3,p_5,p_6\},\{p_4,p_5,p_6\},\{p_1,p_2,p_3,p_4\},\{p_1,p_2,p_3,p_5\},\{p_1,p_2,p_3,p_6\},\\ &\{p_1,p_2,p_4,p_5\},\{p_1,p_2,p_4,p_6\},\{p_1,p_2,p_5,p_6\},\{p_1,p_3,p_4,p_5\},\{p_1,p_3,p_4,p_6\},\\ &\{p_1,p_3,p_5,p_6\},\{p_1,p_4,p_5,p_6\},\{p_2,p_3,p_4,p_5\},\{p_2,p_3,p_4,p_6\},\{p_2,p_3,p_5,p_6\},\\ &\{p_2,p_4,p_5,p_6\},\{p_3,p_4,p_5,p_6\},\{p_1,p_2,p_3,p_4,p_5\},\{p_1,p_2,p_3,p_4,p_6\},\\ &\{p_1,p_2,p_3,p_5,p_6\},\{p_1,p_2,p_4,p_5,p_6\},\{p_1,p_3,p_4,p_5,p_6\},\{p_2,p_3,p_4,p_5,p_6\},\\ &\{p_1,p_2,p_3,p_4,p_5,p_6\}\}.\end{aligned}$$

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

$$f_i(x) = r_i \cdot x + Sk_i (\bmod q)$$

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 six subshares $s_{i,1}, \ldots, s_{i,6}$ are computed from $f_i(x)$ as follows:

$$s_{i,j} = f_i(ID_j)(\bmod q), \qquad j = 1, \ldots, 6.$$

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

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

Thus, the submaster key $Sk_i(= f_i(0))$ can be obtained, but less than two subshares provide no information about the submaster key.

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

$$
\begin{aligned}
S_1 &= \langle —, Sk_2, s_{3,1}, Sk_4, s_{5,1}, Sk_6, Sk_7 \rangle, \\
S_2 &= \langle Sk_1, —, Sk_3, Sk_4, s_{5,2}, s_{6,2}, Sk_7 \rangle, \\
S_3 &= \langle s_{1,3}, Sk_2, —, Sk_4, s_{5,3}, s_{6,3}, Sk_7 \rangle, \\
S_4 &= \langle Sk_1, Sk_2, Sk_3, —, Sk_5, Sk_6, s_{7,4} \rangle, \\
S_5 &= \langle s_{1,5}, s_{2,5}, s_{3,5}, Sk_4, —, Sk_6, Sk_7 \rangle, \\
S_6 &= \langle Sk_1, s_{2,6}, s_{3,6}, Sk_4, Sk_5, —, Sk_7 \rangle, \text{ where '—', denotes empty entry.}
\end{aligned}
$$

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

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

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

If $A = \{p_4\} \in \Delta$, A cannot 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 $s_{5,1}$ of S_1 and $s_{5,2}$ of S_2.

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

5. APPLICATION

Our secret sharing scheme for graph-based prohibited structures can be employed in many applications in various areas, such as secure communication networks, and secure databases. It is particularly useful for access control (e.g., reading a file, or sending a message) in an environment where the number of participants is large, such as a large secure network. Consider a network system with n participants, where an access control policy is enforced by a Communication Granting Server (CGS) to restrict the communication between participants. A secure session key will be issued unless the sender requesting the key is allowed to communicate with the receiver. The access control matrix employed in conventional access control mechanisms can be used by the CGS to achieve the goal [17]. However, the CGS needs to store and search the large access control matrix of size $O(n^2)$. This size of information causes heavy storage and computation loads on the CGS when n is large. In the worst case, the storage and computation loads may make this design impractical.

In contrast, the secret sharing scheme for graph-based prohibited structures is more efficient. We can transform the communication relationships into a graph, where a vertex denotes a participant and an edge does an illegal communication. In the network system, each participant holds a secret (e.g., his password). The secret can be transformed into the corresponding share in the secret sharing scheme by the communication granting server. The transformation needs to be one-way so that it is computationally infeasible to compute the secret from the share. Two participants present their secrets to the CGS when attempting to communicate. If the two corresponding shares generated by the two secrets can successfully determine the master key, the CGS will return a session key to both participants. This session key will be used as both encryption and decryption keys for future communication between these two participants. In the scheme, the CGS need not maintain a large access control matrix, but only needs to keep a single master key.

6. CONCLUSIONS

In this paper, we give a construction of perfect secret sharing schemes for mixed structures (Γ, Δ), where $\Gamma = \{\mathbf{P}\}$ and $\Delta = \{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P} \text{ and } |\mathbf{A}| \leq |\mathbf{P}| - 2\}$. Based on the proposed perfect secret sharing schemes, we propose an efficient construction of a perfect secret sharing scheme for graph-based prohibited structures where a vertex denotes a participant and an edge denotes 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. We also present an application of our scheme to the reduction of storage and computation loads on the communication granting server in a secure network.

REFERENCES

1. M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, In *Proceeding of 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, Volume 773, pp. 126–135, Springer-Verlag, Berlin, (1994).
3. G.R. Blakley, Safeguarding cryptographic keys, In *Proceeding of AFIPs 1979 National Computer Conference*, New York, Volume 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*, Prentice-Hall, Englewood Cliffs, NJ, (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, Volume 403, pp. 27–35, Springer-Verlag, Berlin, (1990).
11. R.M. Capocelli, A. DeSantis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, In *Advances in Cryptology-Crypto'91 Proceeding*, Lecture Notes in Computer Science, pp. 101–113, Springer-Verlag, Berlin, (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 Computer Science, Volume 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 of 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, *Computers Math. Applic.* **31** (7), 129–135, (1996).
17. B.W. Lampson, Protection, In *Proceeding of the 5th Princeton Symp. of Info. Sci. and Syst.*, Princeton Univ., pp. 437–443, (March 1971); Reprinted in *ACM Oper. Syst. Rev.* **8** (1), 18–24, (January 1994).