Pergamon

Computers Math. Applic. Vol. 31, No. 7, pp. 129–135, 1996

0898-1221/96 $15.00 + 0.00

S0898-1221(96)00022-3

An Efficient Construction of Perfect Secret Sharing Schemes for Graph-Based Structures

HUNG-MIN SUN
Department of Information Management, Chaoyang Institute of Technology
Wufeng, Taichung County, Taiwan, R.O.C.

SHIUH-PYNG SHIEH
Department of Computer Science and Information Engineering
National Chiao Tung University, Hsinchu, Taiwan, R.O.C.

(Received October 1993; revised and accepted May 1995)

Abstract—In this paper, we propose an efficient construction of perfect secret sharing schemes for graph-based access structures where a vertex denotes a participant and an edge does a qualified pair of participants. The secret sharing scheme is based on the assumptions that the pairs of participants corresponding to edges in the graph can compute the master key but the pairs of participants corresponding to nonedges in the graph cannot. The information rate of our scheme is $1/(n-1)$, 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.

Keywords—Secret sharing scheme, Data security, Cryptography, Access structure.

1. INTRODUCTION

In 1987, Ito *et al.* 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 [1]. Let $\mathbf{P}$ be the set of participants. The collection of subsets of participants that can reconstruct the secret in this way is called the *access structure* (denoted by Γ). The collection of subsets of participants that cannot obtain any information about the secret is called the *prohibited structure* (denoted by Δ) [2]. The natural restriction is that Γ is monotone increasing and Δ is monotone decreasing; that is,

- if $\mathbf{A} \in \Gamma$ and $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{P}$, then $\mathbf{B} \in \Gamma$, and
- if $\mathbf{A} \in \Delta$ and $\mathbf{B} \subseteq \mathbf{A} \subseteq \mathbf{P}$, then $\mathbf{B} \in \Delta$.

If $\Delta = 2^P \setminus \Gamma$, then we say the structure (Γ, Δ) is *complete* [2]. Let $\mathcal{K}$ be the master key space and $\mathcal{S}$ be the share space. The information rate for the secret sharing scheme is defined to be $\log_2 |\mathcal{K}| / \log_2 |\mathcal{S}|$ (see [3]). A *construction* for a secret sharing scheme is some concrete realization of the scheme. The concept of an (m, n)-threshold scheme, $m \leq n$, is to transform a master key, top secret, into n shares in such a way that the master key cannot be reclaimed unless m or more shares are collected [4,5]. It is clear that the threshold scheme is a way of constructing secret sharing schemes. A secret sharing scheme is called *perfect* if any set of participants in the prohibited structure Δ obtains no information regarding the master key [2,6,7]. Given any complete structure (Γ, Δ) (i.e., $\Delta = 2^P \setminus \Gamma$), Ito *et al.* showed that there exists a perfect secret sharing

This research was supported by the National Science Council of Republic of China under Grant No. NSC-84-2213-E-009-081.

scheme to realize the structure [1,8]. Benaloh and Leichter proposed a different algorithm to realize secret sharing schemes for any given monotone access structure [9]. 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 [1,10]. Their goal is to maximize the information rate of a secret sharing scheme. Brickell and Stinson studied a perfect secret sharing scheme for a graph-based structure where the monotone-increasing access structure Γ contains the pairs of participants corresponding to edges, and the prohibited structure Δ is the collection of subsets of participants corresponding to any independent set of the graph [1]. They proved that, for any graph G with n vertices having maximum degree d, there exists a perfect secret sharing scheme realizing G in which the information rate is at least $2/(d+3)$. In the worst case when $d = n-1$, the information rate is $2/(n+2)$. The structure of their secret sharing scheme is complete. However, their construction is difficult to use because it needs to maintain a large access check matrix with at least $|\mathcal{K}| \cdot d$ rows. It is also time-consuming to recover the master key by looking up the large access check matrix.

In this paper, we propose an efficient construction of a perfect secret sharing scheme for access/prohibited structures based on a graph where the monotone-increasing access structure Γ contains the pairs of participants corresponding to edges, and the monotone-decreasing prohibited structure Δ contains the pairs of participants corresponding to nonedges. The information rate of our scheme is $1/(n-1)$, where n is the number of participants. Our scheme does not need to maintain a large access check matrix, and thus is more efficient than the Brickell and Stinson's method. 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.

This paper is organized as follows. In Section 2, we propose a construction of perfect secret sharing schemes for graph-based access/prohibited structures. In Section 3, we discuss the application of our construction. Finally, we conclude the paper in Section 4.

2. CONSTRUCTION OF PERFECT MONOTONE SSS FOR GRAPH-BASED ACCESS/PROHIBITED STRUCTURES

It is difficult to efficiently construct a secret sharing scheme for any access structure due to its irregular nature. In this paper, we focus only on the graph-based access/prohibited structures that have interesting features. For convenience, we abbreviate the secret sharing scheme for graph G to SSS(G). 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 does a pair of participants. In a *perfect* secret sharing scheme for access/prohibited structures based on G, a pair of participants corresponding to an edge of G can compute the master key, while a pair of participants corresponding to a nonedge of G cannot obtain any information regarding the master key. We use $\mathbf{E}$ to denote the set of edges of G; $\mathbf{NE}$ to denote the set of nonedges of G; $\mathbf{S}$ to denote the set of pairs of participants corresponding to edges of G; $\mathbf{R}$ to denote the set of pairs of participants corresponding to nonedges of G. It is reasonable to restrict that the access structure and prohibited structure are monotone. That is,

- if $\mathbf{A} \in \mathbf{S}$ and $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{P}$, $\mathbf{B}$ can compute the master key, and
- if $\mathbf{A} \in \mathbf{R}$ and $\mathbf{B} \subseteq \mathbf{A} \subseteq \mathbf{P}$, $\mathbf{B}$ can obtain no information regarding the master key.

Thus, the access structure $\Gamma = \{\mathbf{B} \mid \mathbf{A} \in \mathbf{S} \text{ and } \mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{P}\}$, and the prohibited structure $\Delta = \{\mathbf{B} \mid \mathbf{A} \in \mathbf{R} \text{ and } \mathbf{B} \subseteq \mathbf{A} \subseteq \mathbf{P}\}$.

Here, we only consider the case of an access graph G which is connected. If graph G is not connected, we can divide G into two or more connected components. Each component is realized by a perfect secret sharing scheme, respectively. Our access graph is based on the assumptions as Brickell and Stinson's schemes [3] that graphs do not have loops or multiple edges.

In the following, we will use the conventional threshold schemes [4,5] to construct the perfect secret sharing schemes for graph-based access structures. We assume that all computations are over $GF(q)$ where q is a prime which is larger than the size of the master key space.

Given a connected graph G without loops, a secret sharing scheme for the access structure based on the graph G is constructed as follows. Assume that $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ is the set of participants corresponding to the vertices of the graph G. We first construct n conventional $(2, n)$-threshold schemes [4,5], named $\mathrm{TS}_1, \mathrm{TS}_2, \ldots$, and TS_n. 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 k_i be its submaster key and $s_{i,1}, s_{i,2}, \ldots, s_{i,n}$ be its n subshares. Thus, given any two subshares, $s_{i,j}$ and $s_{i,k}$ $(1 \leq j < k \leq n)$, the submaster key k_i can be recovered, but less than two subshares provide no information about k_i.

The master key of the secret sharing scheme for the access structure based on the graph G is given by $K = k_1 + k_2 + \cdots + k_n \pmod{q}$, where k_i is randomly selected over $GF(q)$, for $1 \leq i \leq n$.

The share of participant p_i is given by $S_i = \langle a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n} \rangle$, where $1 \leq t \leq n$,

$a_{i,t} = k_t$ if $\overline{p_i p_t}$ is an edge of G,
$a_{i,t} = s_{t,i}$ if $\overline{p_i p_t}$ is not an edge of G and $t \neq i$, and
$a_{i,t}$ is empty if $t = i$.

Thus, the constructed secret sharing scheme satisfies:

(1) if $\mathbf{A} \in \mathbf{S}$ and $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{P}$, $\mathbf{B}$ can compute the master key;
(2) if $\mathbf{A} \in \mathbf{R}$ and $\mathbf{B} \subseteq \mathbf{A} \subseteq \mathbf{P}$, $\mathbf{B}$ can obtain no information regarding the master key.

THEOREM 1. *If $\mathbf{A} \in \mathbf{S}$ and $\mathbf{A} \subseteq \mathbf{B} \subseteq \mathbf{P}$, $\mathbf{B}$ can compute the master key of the constructed secret sharing scheme for the access structure based on the graph G.*

PROOF. Because $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{A} \in \mathbf{S}$, there exists $p_i, p_j \in \mathbf{B}$ $(i \neq j)$ such that $\overline{p_i p_j} \in \mathbf{E}$. The share of p_i is $S_i = \langle a_{i,1}, a_{i,2}, \ldots, a_{i,n} \rangle$ and the share of p_j is $S_j = \langle a_{j,1}, a_{j,2}, \ldots, a_{j,n} \rangle$.

Because $\overline{p_i p_j}$ is an edge of G, we can conclude that for any t, $1 \leq t \leq n$, one of the following three cases holds:

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

In all these cases (1), (2), and (3), the submaster key k_t can be recovered. Thus, participant p_i and participant p_j can recover the submaster keys $k_1, k_2, \ldots, k_n$ and hence the master key K. ∎

THEOREM 2. *If $\mathbf{A} \in \mathbf{R}$ and $\mathbf{B} \subseteq \mathbf{A} \subseteq \mathbf{P}$, then $\mathbf{B}$ can obtain no information regarding the master key of the constructed secret sharing scheme for the access structure based on the graph G.*

PROOF. Because $|\mathbf{A}| = 2$ and $\mathbf{B} \subseteq \mathbf{A}$, $|\mathbf{B}| \leq 2$. Without loss of generality, we assume that $\mathbf{B} = \{p_i, p_j\}$, where $i \neq j$. Because $\mathbf{B} \subseteq \mathbf{A}$ and $\mathbf{A} \in \mathbf{R}$, $\overline{p_i p_j} \in \mathbf{NE}$.

The share of p_i is $S_i = \langle a_{i,1}, a_{i,2}, \ldots, a_{i,n} \rangle$ and the share of p_j is $S_j = \langle a_{j,1}, a_{j,2}, \ldots, a_{j,n} \rangle$. Because $\overline{p_i p_j}$ is not an edge of G, we can conclude that for any t, $1 \leq t \leq n$, one of the following three cases holds:

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

In case (1), the submaster key k_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 k_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 k_j.

Because $K = k_1 + k_2 + \cdots + k_n \pmod{q}$, p_i and p_j get no information about the master key K. ∎

The share of participant p_i, $\langle a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n} \rangle$, is an n-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-1}, and the size of the master key space is q. It is clear that the information rate of our secret sharing

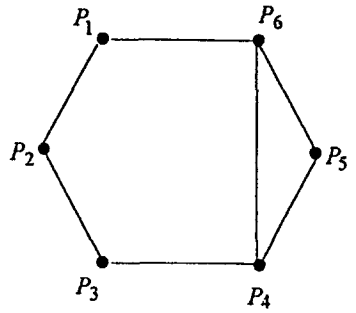

Figure 1. Graph G with six participants.

scheme for graph-based access structure is $\log_2 q / \log_2 q^{n-1} = 1/(n-1)$, where n is the number of participants.

We demonstrate the use of our method in the following example. In Figure 1, the graph G denotes the access/prohibited structures with six participants. The graph G has a set of edges $\mathbf{E}$ and a set of nonedges $\mathbf{NE}$, where

$$\mathbf{E} = \{\overline{p_1p_2}, \overline{p_1p_6}, \overline{p_2p_3}, \overline{p_3p_4}, \overline{p_4p_5}, \overline{p_4p_6}, \overline{p_5p_6}\}, \quad \text{and}$$
$$\mathbf{NE} = \{\overline{p_1p_3}, \overline{p_1p_4}, \overline{p_1p_5}, \overline{p_2p_4}, \overline{p_2p_5}, \overline{p_2p_6}, \overline{p_3p_5}, \overline{p_3p_6}\}.$$

The secret sharing scheme for the access/prohibited structures based on the graph G is constructed as follows.

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

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

The access structure

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

The prohibited structure

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

Let $\mathrm{TS}_1, \mathrm{TS}_2, \ldots,$ and TS_6 be six (2,6)-threshold schemes. We assume that k_i is the submaster key of TS_i and $s_{i,1}, s_{i,2}, \ldots,$ and $s_{i,n}$ are the subshares of TS_i. Here we use Shamir's method [5] to construct these threshold schemes. For each $(2,6)$-TS_i, let

$$f_i(x) = r_i \cdot x + k_i \pmod q$$

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

$$s_{i,j} = f_i(\mathrm{ID}_j) \pmod{q}, \quad j = 1, \ldots, 6.$$

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 [11]:

$$f_i(x) = s_{i,j}\frac{(x - \mathrm{ID}_k)}{(\mathrm{ID}_j - \mathrm{ID}_k)} + s_{i,k}\frac{(x - \mathrm{ID}_j)}{(\mathrm{ID}_k - \mathrm{ID}_j)} \pmod{q}.$$

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

The master key of the SSS(G) is given by $K = k_1 + k_2 + \cdots + k_6 \pmod{q}$. The shares of participants are given by

$$\begin{aligned}
S_1 &= \langle -, k_2, s_{3,1}, s_{4,1}, s_{5,1}, k_6 \rangle, \\
S_2 &= \langle k_1, -, k_3, s_{4,2}, s_{5,2}, s_{6,2} \rangle, \\
S_3 &= \langle s_{1,3}, k_2, -, k_4, s_{5,3}, s_{6,3} \rangle, \\
S_4 &= \langle s_{1,4}, s_{2,4}, k_3, -, k_5, k_6 \rangle, \\
S_5 &= \langle s_{1,5}, s_{2,5}, s_{3,5}, k_4, -, k_6 \rangle, \\
S_6 &= \langle k_1, s_{2,6}, s_{3,6}, k_4, k_5, - \rangle, \qquad \text{where '–' denotes empty entry.}
\end{aligned}$$

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

(1) Participant p_1 can obtain k_2 and k_6 because he owns his share S_1.
(2) Participant p_2 can obtain k_1 and k_3 because he owns his share S_2.
(3) Participants p_1 and p_2 can recover k_4 from $s_{4,1}$ of S_1 and $s_{4,2}$ of S_2.
(4) Participants p_1 and p_2 can recover k_5 from $s_{5,1}$ of S_1 and $s_{5,2}$ of S_2.

Therefore, participants p_1 and p_2 can compute $K = k_1 + k_2 + \cdots + k_6 \pmod{q}$. On the other hand, if $B = \{p_1, p_3\} \in \Delta$, B cannot recover either k_1 or k_3. Therefore, B can obtain no information about the master key K.

3. APPLICATION

Our secret sharing scheme for graph-based access 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 not 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 [12]. However, the CGS need 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 perfect secret sharing scheme for graph-based access structures is more efficient. We can transform the communication relationships into a graph where a vertex denotes a participant and an edge does a legal communication. In the network system, each participant holds a secret (which can be regarded as his private secret key). The secret can be transformed into the corresponding share in the secret sharing scheme by the communication granting server.

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.

In the following, we state the communication granting protocol for the support of the legal communication in detail. It is clear that any access matrix (communication relationships) for legal communication can be transformed into a graph where a vertex denotes a participant and an edge denotes a legal communication. Let graph G denote the access graph, S_i $(1 \leq i \leq n)$ be the share of the participant p_i in a secret sharing scheme based on the access graph G, and K be the master key of the secret sharing scheme. We assume the communication granting server has the secret key K_{CGS}. Each participant p_i holds a T_i in secret, where $T_i = \{S_i\}K_{\text{CGS}}$ (S_i is encrypted with CGS's secret key K_{CGS}).

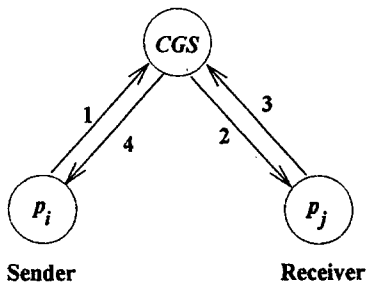

Figure 2. Communication granting protocol.

Figure 2 illustrates the communication granting protocol. The following abbreviations are used in the protocol.

s	$\rightarrow$ sender
r	$\rightarrow$ receiver
$K_{x,y}$	$\rightarrow$ session key for x and y
$\{M\}K_{x,y}$	$\rightarrow$ message M encrypted with the session key shared by x and y

The steps of the protocol are listed in the following.

STEP 1. $P_i \xrightarrow{\{s,r,T_i\}K_{P_i,\text{CGS}}} \text{CGS}$.

STEP 2. $\text{CGS} \xrightarrow{\{s,r,K_{P_i,P_j}\}K_{P_j,\text{CGS}}} P_j$.

STEP 3. $P_j \xrightarrow{\{s,r,T_j\}K_{P_j,\text{CGS}}} \text{CGS}$.

Then, CGS checks whether S_i and S_j, derived from T_i and T_j, respectively, can recover the master key K or not. If not, the request for communication is illegal.

STEP 4. $\text{CGS} \xrightarrow{\{s,r,K_{P_i,P_j}\}K_{P_i,\text{CGS}}} P_i$.

It is clear that if the request of communication between a pair of participants is illegal, then the CGS will not return a session key to the sender. Thus, the communication between the pair of participants will not be processed. Note that no subset of participants can recover the master key without the help of CGS.

4. CONCLUSIONS

In this paper, we propose an efficient construction of perfect secret sharing schemes for graph-based access structures. The information rate of our scheme is $1/(n-1)$. Our scheme does not

need to maintain a large access check matrix, and thus is more efficient. Our efficient scheme can be applied to access control in an environment where the number of participants is large. The CGS based on our scheme does not need to maintain a large $n \times n$ access control matrix, but instead only needs to keep a single master key. Thus, the storage and computation loads on the CGS are greatly reduced.

REFERENCES

1. M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, *Proc. IEEE Globecom '87*, 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, pp. 126–135, Springer-Verlag, Berlin, (1994).
3. 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).
4. G.R. Blakley, Safeguarding cryptographic keys, In *Proc. AFIPs 1979 National Computer Conference*, New York, Vol. 48, pp. 313–317, (1979).
5. A. Shamir, How to share a secret, *Commun. of the ACM* **22** (11), 612–613 (1979).
6. R.W. Hamming, *Coding and Information Theory*, Prentice-Hall, Englewood Cliffs, NJ, (1986).
7. C.E. Shannon, Communication theory of secrecy systems, *Computer Security Journal* **VI** (2), 7–66 (1990).
8. M. Ito, A. Saito and T. Nishizeki, Multiple assignment scheme for sharing secret, *Journal of Cryptology* **6**, 15–20 (1993).
9. 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, pp. 27–35, Springer-Verlag, Berlin, (1990).
10. 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*, pp. 101–113, Springer-Verlag, Berlin, (1992).
11. D.E.R. Denning, *Cryptology and Data Security*, Addison-Wesley, Reading, MA, (1983).
12. B.W. Lampson, Protection, *Proc. 5th Princeton Symp. of Info. Sci. and Syst.*, Princeton Univ., 437–443, (March 1971); Reprinted in *ACM Oper. Syst. Rev.* **8** (1), 18–24 (January 1974).