JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 15, 679-689 (1999)

Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structures

HUNG-MIN SUN AND SHIUH-PYNG SHIEH+
Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 701, R.O.C.
E-mail: hmsun@mail.ncku.edu.tw
+*Department of Computer Science and Information Engineering*
National Chiao Tung University
Hsinchu, Taiwan 300, R.O.C.
E-mail: ssp@csie.nctu.edu.tw

A perfect secret sharing scheme allows a secret K to be shared among a set of participants in such a way that only qualified subsets of participants can recover the secret, and unqualified subsets of participants obtain no information regarding the secret. In this paper, we propose a construction of perfect secret sharing schemes with uniform, generalized access structures of rank 3. Compared with other constructions, our construction has some improved lower bounds on the information rate. In addition, we also generalize the construction to perfect secret sharing schemes with uniform, generalized access structures of constant rank.

Keywords: cryptography, information security, secret sharing schemes, threshold schemes, information theory, access structures

1. INTRODUCTION

In a secret sharing scheme, a secret is broken into pieces, called shares, where each participant keeps a share. A secret sharing scheme allows the secret K to be shared among a set of participants $\boldsymbol{P}$ in such a way that only *qualified* subsets of participants can collaborate with their secret shares to recover the secret [1-4]. A special case of secret sharing schemes is the threshold scheme [5, 6], in which all groups of participants of at least some fixed size are qualified. Secret sharing schemes have many applications in different areas, such as access control, launching a missile, and opening a bank vault or a deposit box. For a more detailed description of secret sharing schemes and a wide discussion of their applications, we refer the reader to the excellent survey papers [3, 7]. A current and complete bibliography can also be found online [4]. The secret K is chosen by a special participant, called the dealer, who is responsible for computing and distributing the shares. The collection of subsets of participants that can reconstruct the secret in this way is called *access structure* Γ. Γ is usually monotone, that is, if $X \in \Gamma$ and $X \subseteq X' \subseteq \boldsymbol{P}$, then $X' \in \Gamma$. A minimal qualified subset $Y \in \Gamma$ is a subset of participants such that $Y' \notin \Gamma$ for all $Y' \subset Y$,

Received May 13, 1997; accepted March 10, 1998.
Communicated by Jean-Lien C. Wu.
*This work was supported in part by the National Science Council, Taiwan, R.O.C., under contract NSC-87-2213-E-324-003.

$Y' \neq Y$. The basis of Γ, denoted by Γ_0, is the family of all minimal qualified subsets. Let 2^P denote the collection of all subsets of $\boldsymbol{P}$. For any $\Gamma_0 \subseteq 2^P$, the *closure* of Γ_0 is defined as $cl(\Gamma_0) = \{X' : \exists X \in \Gamma_0, X \subseteq X' \subseteq \boldsymbol{P}\}$. Therefore, an access structure Γ is the same as the closure of its basis Γ_0, $cl(\Gamma_0)$. A secret sharing scheme is *perfect* if unqualified subsets of participants obtain no information regarding the secret [8, 9]. This means that the prior probability $p(K = K_0)$ is equal to the conditional probability $p(K = K_0 \mid$ given any or fewer secret shares of an unqualified set). With the entropy function H [10], we can state the requirements of a secret sharing scheme as follows:

(1) any qualified subset can reconstruct the secret:

$$\forall_{X \in \Gamma} H(K \mid X) = 0; \text{ and}$$

(2) any unqualified subset has no information on the secret:

$$\forall_{X \notin \Gamma} H(K \mid X) = H(K).$$

To efficiently implement a perfect secret sharing scheme, it is important to keep the length of the shares as small as possible. Let K be the secret space and S be the maximum share space. The information rate of a secret sharing scheme is defined as the ratio of the length of the secret to the maximum length of shares, that is, $\rho = \log_2 |K| / \log_2 |S|$ [2]. There are other, different approaches to measuring the efficiency of a secret sharing scheme, such as the average information rate [11] and the dealer's randomness approaches [12, 13]. The average information rate of a secret sharing scheme is the ratio between the length of the secret and the arithmetic mean of the length of all shares [11]. The dealer's randomness is the number of random bits required by the dealer to set up a secret sharing scheme [12, 13]. In this paper, we will only focus on the information rates of perfect secret sharing schemes.

Given any access structure Γ, Ito et al. [1, 14] showed that there exists a perfect secret sharing scheme to realize the structure. Benaloh and Leichter [15] 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. Since then, many researchers have studied the perfect secret sharing scheme for graph-based access structure Γ with basis Γ_0, where Γ_0 is the collection of pairs of participants corresponding to edges [8, 9, 16-18]. Stinson [18] 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 $2 / (d + 1)$. Dijk [9] 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 $\varepsilon > 0$.

The *rank* of an access structure Γ is the maximum cardinality of a minimal qualified subset. An access structure is *uniform* if every minimal qualified subset has the same cardinality. Therefore, a graph-based access structure is a uniform access structure with rank 2. Perfect secret sharing schemes with access structures of rank three were studied by Stinson [17]. He applied Steiner systems to construct perfect secret sharing schemes with access structures of rank three. The constructed secret sharing scheme has the information rate $\rho \geq \frac{6}{(n-1)(n-2)}$ if Γ is uniform and $n \equiv 2, 4 \pmod 6$, where n is the number of

participants. Note that if n doesn't satisfy the condition $n \equiv 2, 4 \pmod 6$, it is necessary to find an $n' > n$ such that $n' \equiv 2, 4 \pmod 6$. In this paper, we propose a construction of perfect secret sharing schemes with uniform access structures of rank three. The lower bound of the information rate of the proposed scheme is $\frac{6}{(n-1)^2+2}$. Compared with Stinson's construction, our construction has some improved lower bounds on the information rate. In addition, we also extend our idea which constructs perfect secret sharing schemes with uniform access structures of rank three to construct perfect secret sharing schemes with access structures of constant rank m.

This paper is organized as follows. In section 2, we first introduce the construction of secret sharing schemes for graph-based access structures. Section 3 gives the construction of perfect secret sharing schemes with uniform access structures of rank 3 and evaluates the information rate of the constructed scheme. In section 4, we propose an efficient decomposition construction of secret sharing schemes with uniform access structures of rank m. Finally, we conclude this paper in section 5.

2. CONSTRUCTION FOR GRAPH-BASED ACCESS STRUCTURES

A uniform access structure of rank m is the access structure in which the size of each element in Γ_0 is equal to m. Therefore, the graph-based access structure can be considered to be the case of rank 2. In this section, we first introduce the construction of secret sharing schemes for graph-based access structures [18]. An access structure based on a graph consists of the closure of a graph, where a vertex denotes a participant and an edge denotes a minimal qualified pair of participants. Suppose G is a graph with vertices $V(G)$, edges $E(G)$, and maximum degree d. Stinson [18] showed that there exists a perfect secret sharing scheme with information rate $\rho = 2 / (d + 1)$. In the following, we will propose a construction for graph-based access structures.

We assume that $\boldsymbol{P} = \{p_1, p_2, ..., p_n\}$ is the set of participants corresponding to the vertices of graph G, and that the secret $K = (K_1, K_2)$ is taken randomly from GF(q^2), where q is a prime and $q \geq n$. Let $f(x) = K_2x + K_1 \pmod q$. y_i is computed from $f(x)$ as follows:

$$y_i = f(i - 1) \pmod q, \text{ for } i = 1, ..., n.$$

It is clear that given y_i and y_j, for $i \neq j$, $f(x)$ can be determined uniquely. Therefore, if one can get two or more y_i's, he can recover the secret K. However, if one has no knowledge of any y_i, he can obtains no information about the secret. Note that if one can get one y_i, he can obtain some information about the secret.

The dealer selects n random numbers, $r_1, ..., r_n$, over GF(q). The share of participant p_i is given by

$$S_i = <a_{i,1}, ..., a_{i,t}, ..., a_{i,n}>,$$

where $1 \leq t \leq n$,

$$a_{i,t} = r_i \pmod q \qquad \text{if } t = i,$$

$$a_{i,t} = r_t + y_t \pmod q \qquad \text{if } \overline{p_i p_t} \text{ is an edge of } G, \text{ and}$$

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

Theorem 1: The constructed secret sharing scheme satisfies the dollowing conditions:

(1) any qualified subset can reconstruct the secret:

$\forall_{X \in \Gamma} H(K \mid X) = 0$; and

(2) any unqualified subset has no information about the secret:

$\forall_{X \notin \Gamma} H(K \mid X) = H(K)$.

***Proof*:**

(1) Let X be a subset of participants, and let $X \in \Gamma$. Then, there exists $p_i, p_j \in X (i \neq j)$ such that $\overline{p_i p_j}$ is an edge of G. Therefore, participant p_i owns $a_{i,i} = r_i$ and $a_{i,j} = r_j + y_j$, and participant p_j owns $a_{j,j} = r_j$ and $a_{j,i} = r_i + y_i$. Thus, participant p_i and participant p_j can recover y_i and y_j, and can then recover $f(x)$ and secret K.

(2) Let X be a subset of participants, and let $X \notin \Gamma$. Therefore, for any pair of participants $p_i, p_j \in X (i \neq j)$, $\overline{p_i p_j}$ is not an edge of G. We assume that X can recover y_i. Therefore there exists participant p_i who owns $a_{i,i} = r_i$ and participant p_j who owns $a_{j,i} = r_i + y_i$. Thus, $\overline{p_i p_j}$ is an edge of G. This is a contradiction of the condition that $\overline{p_i p_j}$ is not an edge of G. Hence, X cannot recover any y_i. That is, X obtains no information about secret K. □

The share of participant p_i is an n-dimensional vector. Except that $a_{i,j}$'s (for all j, $\overline{p_i p_j} \notin E(G)$) are empty, every $a_{i,j}$ is over GF(q). Therefore, the length of share S_i is $\log(q^{d_i+1})$, where d_i is the degree of vertex p_i of G. The maximal length of the shares is $\log(q^{d+1})$, where d is the maximum degree of G. The length of the secret is $\log(q^2)$. Thus, the information rate of the secret sharing scheme is $\rho = \frac{2 \cdot \log q}{(d+1) \cdot \log q} = \frac{2}{d+1}$.

Time Complexity: Here, we evaluate the time complexity for constructing the secret sharing scheme based on a graph G. It is clear that the computation of y_i's, for $i = 1, ..., n$, can be achieved in $O(n)$ time complexity. The dominant part is the assignment of the shares, S_i's. For these shares, S_i's, there are n^2 entries in total. Therefore, the construction can be achieved in $O(n^2)$ time complexity.

3. CONSTRUCTION FOR UNIFORM ACCESS STRUCTURES OF RANK THREE

In the section, we will propose the construction of perfect secret sharing schemes with uniform access structures of rank 3 and evaluate the information rate of the constructed scheme. Assume that $\boldsymbol{P} = \{p_1, p_2, ..., p_n\}$ is the set of participants, and that the secret $K = (K_1, K_2, K_3, K_4, K_5, K_6)$ is taken randomly from GF(q^6), where q is a prime and $q \geq 2n$. Let $f(x) = K_6x^5 + K_5x^4 + K_4x^3 + K_3x^2 + K_2x + K_1 (\text{mod } q)$. y_i be computed from $f(x)$ as follows:

$y_i = f(i-1) \pmod q$, for $i = 1, ..., 2n$.

Thus, if he can get six or more y_i's, he can recover $f(x)$ and then secret K. However, if he has no knowledge of any y_i, he can obtain no information about the secret.

We define G_i, for $1 \le i \le n$, as the graph with vertices $V(G_i)$ and edges $E(G_i)$, where $V(G_i) = \{p_j \mid \text{for all } p_j, \text{ where } \{p_i, p_j, p_k\} \in \Gamma_0\}$ and $E(G_i) = \{\overline{p_j p_k} \mid \text{for all } \overline{p_j p_k}, \text{ where } \{p_i, p_j, p_k\} \in \Gamma_0\}$. The dealer selects $2n$ random numbers, $r_1, ..., r_{2n}$, over GF(q). As in the construction presented in section 2, there exists a secret sharing scheme realizing G_i in which the secret is $(r_1 + y_i, r_{n+i} + y_{n+i})$ and the share of participant p_j is $S_j(G_i)$ for $p_j \in V(G_i)$.

The share of participant p_i is given by

$$S_i = < r_i, r_{n+i}, a_{i,1}, ..., a_{i,t}, ..., a_{i,n} >,$$

where $1 \le t \le n$,

$a_{i,t} = S_i(G_t)$ if $p_i \in V(G_t)$ and

$a_{i,t}$ is empty otherwise.

Theorem 2: The constructed secret sharing scheme satisfies the following conditions:
(1) any qualified subset can reconstruct the secret:

$$\forall_{X \in \Gamma} H(K \mid X) = 0; \text{ and}$$

(2) any unqualified subset has no information about the secret:

$$\forall_{X \notin \Gamma} H(K \mid X) = H(K).$$

***Proof*:**

(1) Let $X \in \Gamma$ be a subset of participants. Then, there exists $p_i, p_j, p_k \in X$ $(i \ne j \ne k)$ such that $\{p_i, p_j, p_k\} \in \Gamma_0$. Participant p_i owns r_i, r_{n+i}, $S_i(G_j)$, and $S_i(G_k)$. Participant p_j owns r_j, r_{n+j}, $S_j(G_i)$, and $S_j(G_k)$. Participant p_k owns r_k, r_{n+k}, $S_k(G_i)$, and $S_k(G_j)$. From $S_j(G_i)$ and $S_k(G_i)$, they can recover $r_i + y_i$, $r_{n+i} + y_{n+i}$ because $\overline{p_j p_k}$ is an edge of G_i. From $S_i(G_j)$ and $S_k(G_j)$, they can recover $r_j + y_j$, $r_{n+j} + y_{n+j}$ because $\overline{p_i p_k}$ is an edge of G_j. From $S_i(G_k)$ and $S_j(G_k)$, they can recover $r_k + y_k$, $r_{n+k} + y_{n+k}$ because $\overline{p_i p_j}$ is an edge of G_k. Thus, participants p_i, p_j and p_k can recover y_i, y_{n+i}, y_j, y_{n+j}, y_k and y_{n+k}, and can then recover $f(x)$ and secret K.

(2) Let $X \notin \Gamma$ be a subset of participants. Therefore, there does not exist any three participants p_i, p_j and p_k in X such that $\{p_i, p_j, p_k\} \in \Gamma_0$. We assume that X can recover y_i. Hence, there exists participant p_i who owns r_i, and participants p_j and p_k who can recover $r_i + y_i$. Thus, $\overline{p_j p_k}$ is an edge of G_i and $\{p_i, p_j, p_k\} \in \Gamma_0$. This is a contradiction of the condition that $\{p_i, p_j, p_k\} \notin \Gamma_0$. That is, X obtains no information about y_i, for $1 \le i \le 2n$, and, therefore, about secret K. □

The share of participant p_i is $S_i = < r_i, r_{n+i}, a_{i,1}, ..., a_{i,t}, ..., a_{i,n} >$. Because $a_{i,t} = S_i(G_t)$ for $p_i \in V(G_t)$, the length of $a_{i,t}$ is equal to $\log(p^{d_i(G_t)+1})$ if $p_i \in V(G_t)$, where $d_i(G_t)$ is the degree of vertex p_i in G_t. Hence, the length of share S_i is equal to $\log(q^{\sum_{t:p_i \in G_t}(d_i(G_t)+1)+2})$. Because the length of the secret is equal to $\log(q^6)$, the information rate of the secret sharing scheme is

$$\rho = \frac{6 \cdot \log q}{\underset{i}{Max}\{\sum_{t:p_i \in G_t}(d_i(G_t)+1)+2\} \cdot \log q}$$

$$= \frac{6}{\underset{t}{Max}\{\sum_{t:p_i \in G_t}(d_i(G_t)+1)\}+2}.$$

In the worst case when $p_i \in G_t$ (for $1 \le t \le n$ and $t \ne i$) and $d_i(G_t) = n - 2$, the information rate of the secret sharing scheme is $\rho = \frac{6}{(n-1)^2+2}$.

Table 1. Bounds on the information rate for uniform access structures of rank three on n participants for $n \ge 5$, where * denotes the method which has the better bound.

n	Stinson's Method	Our Method
$n \equiv$ (mod 6)	$\rho \ge \frac{6}{n(n+1)}$	$\rho \ge \frac{6}{(n-1)^2+2}$ *
$n \equiv$ 1,3 (mod 6)	$\rho \ge \frac{6}{n(n-1)}$	$\rho \ge \frac{6}{(n-1)^2+2}$ *
$n \equiv$ 2,4 (mod 6)	$\rho \ge \frac{6}{(n-1)(n-2)}$ *	$\rho \ge \frac{6}{(n-1)^2+2}$
$n \equiv$ 5 (mod 6)	$\rho \ge \frac{6}{(n+1)(n+2)}$	$\rho \ge \frac{6}{(n-1)^2+2}$ *

Compared with the lower bound studied by Stinson [17], our lower bound is better than Stinson's lower bound in some cases. The comparison can be seen in Table 1.

We demonstrate the use of our method in the following example.

Let $P = \{p_1, p_2, p_3, p_4, p_5\}$ and $\Gamma_0 = \{ \{p_1, p_2, p_3\}, \{p_1, p_2, p_5\}, \{p_1, p_3, p_4\}, \{p_2, p_4, p_5\}, \{p_3, p_4, p_5\} \}$. We construct

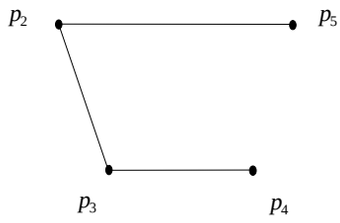
G_1 with $V(G_1) = \{p_2, p_3, p_4, p_5\}$ and $E(G_1) = \{\overline{p_2p_3}, \overline{p_2p_5}, \overline{p_3p_4}\}$,

G_2 with $V(G_2) = \{p_1, p_3, p_4, p_5\}$ and $E(G_2) = \{\overline{p_1p_3}, \overline{p_1p_5}, \overline{p_4p_5}\}$,

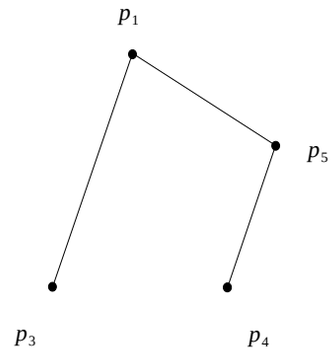
G_3 with $V(G_3) = \{p_1, p_2, p_4, p_5\}$ and $E(G_3) = \{\overline{p_1p_2}, \overline{p_1p_4}, \overline{p_4p_5}\}$,

G_4 with $V(G_4) = \{p_1, p_2, p_3, p_5\}$ and $E(G_4) = \{\overline{p_1p_3}, \overline{p_2p_5}, \overline{p_3p_5}\}$, and

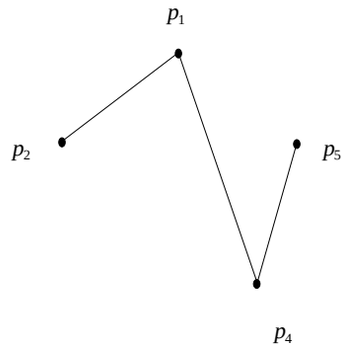
G_5 with $V(G_5) = \{p_1, p_2, p_3, p_4\}$ and $E(G_5) = \{\overline{p_1p_2}, \overline{p_2p_4}, \overline{p_3p_4}\}$ as follows.



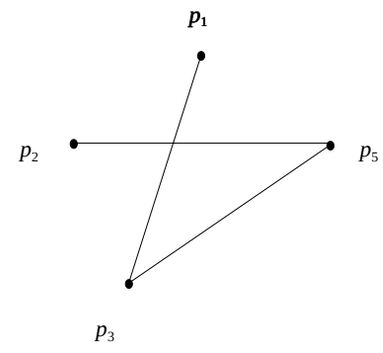
Graph G_1



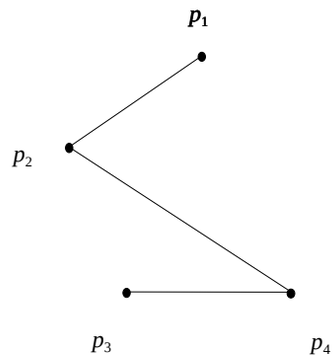
Graph G_2



Graph G_3



Graph G_4



Graph G_5

Graph G_1-G_5

Let the secret $K = (K_1, K_2, K_3, K_4, K_5, K_6)$ be taken randomly from GF(q^6), where q is a prime and $q \geq 10$.

Let $f(x) = K_6x^5 + K_5x^4 + K_4x^3 + K_3x^2 + K_2x + K_1 \pmod q$ and $y_i = f(i-1) \pmod q$, for $i = 1, ..., 10$. The dealer selects 10 random numbers r_i's ($1 \leq i \leq 10$) from GF(q). Each pair of $(r_i + y_i, r_{n+i} + y_{n+i})$ is shared by the secret sharing scheme with access structure G_i, and the share of participant p_j is $S_j(G_i)$ for $p_j \in V(G_i)$.

The share of participant p_i is given by

$S_1 = < r_1, r_6, -, S_1(G_2), S_1(G_3), S_1(G_4), S_1(G_5) >,$
$S_2 = < r_2, r_7, S_2(G_1), -, S_2(G_3), S_2(G_4), S_2(G_5) >,$
$S_3 = < r_3, r_8, S_3(G_1), S_3(G_2), -, S_3(G_4), S_3(G_5) >,$
$S_4 = < r_4, r_9, S_4(G_1), S_4(G_2), S_4(G_3), -, S_4(G_5) >,$
$S_5 = < r_5, r_{10}, S_5(G_1), S_5(G_2), S_5(G_3), S_5(G_4), - >.$

Obviously, $\{p_1, p_2, p_5\}$ can recover y_1, y_2, y_5, y_6, y_7, and y_{10}, and can then recover K. The lengths of $S_i(G_j)$'s can be tabulated as follows.

	j=2	j=3	j=4	j=5	
i=1	–	$\log(q^3)$	$\log(q^3)$	$\log(q^2)$	$\log(q^2)$
i=2	$\log(q^3)$	–	$\log(q^2)$	$\log(q^2)$	$\log(q^3)$
i=3	$\log(q^3)$	$\log(q^2)$	–	$\log(q^3)$	$\log(q^2)$
i=4	$\log(q^2)$	$\log(q^2)$	$\log(q^3)$	–	$\log(q^3)$
i=5	$\log(q^2)$	$\log(q^3)$	$\log(q^2)$	$\log(q^3)$	–

Therefore, the length of each share S_i is equal to $\log(q^{12})$, and the information rate of the secret sharing scheme is $\rho = \frac{6 \cdot \log q}{12 \cdot \log q} = \frac{1}{2}$.

Time Complexity: Here, we evaluate the time complexity for constructing a secret sharing scheme with a uniform access structure of rank three. First, it is clear that the computation of y_i's, for $i = 1, ..., n$, can be achieved in $O(n)$ time complexity. On the other hand, to construct a secret sharing scheme with a uniform access structure of rank three on n participants, we need to construct n secret sharing schemes for n graphs (each n -1 vertices). From section 2, we know that the time complexity for constructing a secret sharing scheme for a graph with n -1 vertices is $O((n-1)^2)$. Because the complexity $O(n(n-1)^2)$ is equivalent to the complexity $O(n^3)$, the construction of a secret sharing scheme with a uniform access structure of rank three can be achieved in $O(n^3)$ time complexity.

4. CONSTRUCTION FOR UNIFORM ACCESS STRUCTURES OF RANK *m*

In this section, based on the same concept used in the construction of the secret sharing schemes with uniform access structures of rank 3, we propose an efficient decomposition construction of secret sharing schemes with uniform access structures of rank m. Let Γ be a uniform access structure of rank m on n participants. Assume that $\boldsymbol{P} = \{p_1, p_2, ..., p_n\}$ is the set of participants, and that the basis of Γ is Γ_0. We can decompose Γ_0 into the union

of Γ_i's, for $1 \le i \le n$, where $\Gamma_i = \{X : X \in \Gamma_0$ and X contains participant $p_i\}$. Thus, $\Gamma = cl(\Gamma_0) = cl(\Gamma_1) \cup ... \cup cl(\Gamma_n)$. We define $\Gamma_i^* = \{X : X \cup \{p_i\} \in \Gamma_i\}$. Therefore, each $cl(\Gamma_i^*)$ is a uniform access structure of rank $m - 1$. We assume that secret $K = (K_1, K_2, ..., K_m)$, where each K_i, for $1 \le i \le m$, is taken randomly from GF($q^{h(m-1)}$), which is the secret space of the secret sharing schemes with uniform access structures of rank $m - 1$. Note that $h(i)$ is a function which indicates that the secret space of the secret sharing schemes with uniform access structures of rank i is GF($q^{h(i)}$). The dealer selects a polynomial $f(x)$ of degree $m \cdot h(m - 1) - 1$ with coefficients K and computes y_i as follows: $y_i = f(i - 1) \pmod q$, for $i = 1, ..., n \cdot h(m - 1)$.

Thus, if one can get $m \cdot h(m - 1)$ or more y_i's, he can recover $f(x)$ and then secret K. However, if one has no knowledge of any y_i, he can obtain no information about the secret. We use $Y_1, Y_2, ..., Y_n$ over GF($q^{h(m-1)}$) to denote these $n \cdot h(m - 1)$ y_i's. The dealer selects n random numbers $R_1, R_2, ..., R_n$ over GF($q^{h(m-1)}$). We assume that there exists a secret sharing scheme realizing $cl(\Gamma_i^*)$, in which the secret is $R_i + Y_i$ and the share of participant p_j is $S_j(\Gamma_i^*)$.

The share of participant p_i is given by

$$S_i = < R_i, S_i(\Gamma_1^*), ..., S_i(\Gamma_{i-1}^*), S_i(\Gamma_{i+1}^*), ..., S_i(\Gamma_n^*) >.$$

Thus, the constructed secret sharing scheme is a perfect secret sharing scheme with access structure Γ. Summarizing, we have the following theorem.

Theorem 3: The constructed secret sharing scheme satisfies the following conditions:
(1) any qualified subset can reconstruct the secret:

$$\forall_{X \in \Gamma} H(K \mid X) = 0; \text{ and}$$

(2) any unqualified subset has no information on the secret:

$$\forall_{X \notin \Gamma} H(K \mid X) = H(K).$$

Time Complexity: Here, we will evaluate the time complexity for constructing a secret sharing scheme with a uniform access structure of rank m. First, it is clear that we can use a polynomial of degree $m! - 1$ to compute all y_i's, for $i = 1, ..., n$. Thus, the computation of y_i's can be achieved in $O(n \cdot m!)$, which is smaller than the time complexity of the following part. On the other hand, to construct a secret sharing scheme with an access structure of rank m on n participants, we need to construct n secret sharing schemes with access structures of rank $m - 1$ on $n - 1$ participants. Let $O(T(m, n))$ be the time complexity for constructing a secret sharing scheme with an access structure of rank m on n participants. Then, $O(T(m, n)) = O(m \cdot T(m - 1, n - 1))$. Thus, $O(T(m, n)) = O(m \cdots 3 \cdot T(2, n - m + 2))$. Because $O(T(2, n - m + 2)) = O((n - m + 2)^2)$, it is clear that $O(T(m, n)) = O(\frac{m!}{2} \cdot (n - m + 2)^2)$.

5. CONCLUSIONS

Based on the secret sharing schemes with graph-based access structures, we have proposed an efficient construction to realize the perfect secret sharing schemes with uniform access structures of rank 3. Given any uniform access structure of rank 3, with basis

Γ_0, the information rate of the constructed secret sharing scheme is equal to $\frac{6}{\underset{i}{Max}\{\sum_{t:p_i \in G_t}(d_i(G_t)+1)\}+2}$, where G_i is the graph with vertices $V(G_i) = \{p_j \mid \text{for all } p_j, \text{ where } \{p_i, p_j, p_k\} \in \Gamma_0\}$ and edges $E(G_i) = \{\overline{p_j p_k} \mid \text{for all } \overline{p_j p_k}, \text{ where } \{p_i, p_j, p_k\} \in \Gamma_0\}$. In the worst case, the lower bound $\frac{6}{(n-1)^2+2}$ can be achieved, where n is the number of participants. Compared with Stinson's construction, our construction has some improved lower bounds on the information rate. In addition, we have also proposed a construction of perfect secret sharing schemes for uniform access structures of rank m.

REFERENCES

1. M. Ito, A. Saito and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Proceedings of IEEE Globecom'87*, Tokyo, 1987, pp. 99-102.
2. D. R. Stinson, "An explication of secret sharing schemes," *Designs, Codes and Cryptography* Vol. 2, No. 4, 1992, pp. 357-390.
3. G. J. Simmons, ed., "An introduction to shared secret and/or shared control schemes and their application," in *Contemporary Cryptology, The Science of Information Integrity*, IEEE Press, 1992, pp. 441-497.
4. D.R. Stinson, "Bibliography on secret sharing schemes," Available online, http://bibd.unl.edu/~stinson/ssbib.html
5. A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, No. 11, 1979, pp. 612-613.
6. G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of American Federation of Information Processing Societies 1979 National Computer Conference*, Vol. 48, 1979, pp. 313-317.
7. G. J. Simmons, W. A. Jackson and K. M. Martin, "The geometry of shared secret schemes, " *Bulletin of the Institute of Combinatorial Applications*, Vol. 1, 1991, pp. 71-88.
8. E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *Journal of Cryptology*, Vol. 5, No. 3, 1992, pp. 153-166.
9. M. van Dijk, "On the information rate of perfect secret sharing schemes," *Designs, Codes and Cryptography*, Vol. 6, No. 2, 1995, pp. 143-169.
10. R. W. Hamming, *Coding and Information Theory*, Englewood Cliffs, Reading, NJ: Prentice-Hall, 1986.
11. K. M. Martin, "New secret sharing schemes from old," *Journal of Combinational Mathematics and Combinatorial Computing,* Vol. 14, 1993, pp. 65-77.
12. C. Blundo, A. De Santis and U. Vaccaro, "Randomness in distribution protocols," *Information and Computation,* Vol. 131, No. 2, 1996, pp. 111-139. [A preliminary version appeared in "Automata, Languages and Programming, 21st International Colloquium", S. Abiteboul and E. Shamir, eds., Lecture Notes in Computer Science Vol. 820, 1994, pp. 568-579.]
13. C. Blundo, A. Giorgia Gaggia and D. R. Stinson, "On the dealer's randomness required in secret sharing schemes," *Designs, Codes and Cryptography*, Vol. 11, No. 2, 1997, pp. 107-122. [A preliminary version appeared in "Advances in Cryptology – EUROCRYPT

'94", A. De Santis, ed., Lecture Notes in Computer Science Vol. 950, 1995, pp. 35-46.]
14. M. Ito, A. Saito and T. Nishizeki, "Multiple assignment scheme for sharing secret," *Journal of Cryptology*, Vol. 6, No. 1, 1993, pp. 15-20.
15. 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, 1990, pp. 27-35.
16. C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, "Graph decompositions and secret sharing schemes," *Journal of Cryptology*, Vol. 8, 1995, pp. 39-63.
17. 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*, Springer-Verlag, Vol. 740, 1993, pp. 168-182.
18. D. R. Stinson, "Decomposition constructions for secret sharing schemes," *IEEE Transactions Information Theory*, Vol. IT-40, No. 1, 1994, pp. 118-125.

Hung-Min Sun (孫宏民) received his B.S. degree in applied mathematics from National Chung-Hsing University in 1988, his M.S. degree in applied mathematics from National Cheng Kung University in 1990, and his Ph.D. degree in computer science and information engineering from National Chiao Tung University in 1995, respectively. He was an associate professor with the Department of Information Management, Chaoyang University of Technology from 1995 to 1999. Currently he is teaching at the Department of Computer Science and Information Engineering, National Cheng Kung University. His research interests include reliability theory, computer security, cryptography, and information theory.

Shiuh-Pyng Shieh (謝續平) received the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1986 and 1991, respectively. He is currently a professor with the Department of Computer Science and Information Engineering, National Chiao Tung University. From 1988 to 1991, he participated in the design and implementation of the B2 Secure XENIX for IBM, Federal Sector Division, Gaithersburg, Maryland, USA. He is also the designer of the SNP (Secure Network Protocols). Since 1994, he has been a consultant for the Computer and Communications Laboratory, Industrial Technology Research Institute, Taiwan, in the area of network security and distributed operating systems. He is also a consultant for the National Security Bureau, Taiwan. Dr. Shieh has been on the organizing committees of a number of conferences, such as the International Computer Symposium, and the International Conference on Parallel and Distributed Systems. Recently, he is the general chair of 1998 Network Security Technology Workshop, the program chair of 1999 Mobile Computing Conference and 1997 Information Security Conference (INFOSEC '97). His research interests include internetworking distributed operating systems, and network security.