PERGAMON Computers and Mathematics with Applications 37 (1999) 87–96

An International Journal
computers & mathematics
with applications

Recursive Constructions for Perfect Secret Sharing Schemes

HUNG-MIN SUN
Department of Information Management
Chaoyang University of Technology
Wufeng, Taichung County
Taiwan 413, R.O.C.
hmsun@mail.cyut.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 May 1997; revised and accepted March 1998)

Abstract—A secret sharing scheme is a method which allows a secret to be shared among a set of participants in such a way that only qualified subsets of participants can recover the secret. A secret sharing scheme is called perfect if unqualified subsets of participants obtain no information regarding the secret. The information rate of a secret sharing scheme is defined to be the ratio between the size of secret and the maximum size of the shares. In this paper, we propose some recursive constructions for perfect secret sharing schemes with access structures of constant rank. Compared with the best previous constructions, our constructions have some improved lower bounds on the information rate.

Keywords—Cryptography, Secret sharing scheme, Information theory, Access structures.

1. INTRODUCTION

A secret sharing scheme is a method which allows a secret K to be shared among a set of participants $\mathbf{P}$ in such a way that only qualified subsets of participants can recover the secret [1,2]. The information kept by each participant is called share. The collection of subsets of participants that can reconstruct the secret in this way is called access structure, denoted by Γ. It is natural to require Γ to be monotone, that is, if $X \in \Gamma$ and $X \subseteq X' \subseteq \mathbf{P}$, then $X' \in \Gamma$. A minimal qualified subset $Y \in \Gamma$ is a subset of participants such that $Y' \notin \Gamma$, for all $Y' \subset Y$. The basis of Γ, denoted by Γ_0, is the family of all minimal qualified subsets. For any $\Gamma_0 \subseteq 2^P$, the closure of Γ_0 is defined to be $\mathrm{cl}(\Gamma_0) = \{X' : \exists X \in \Gamma_0, X \subseteq X' \subseteq \mathbf{P}\}$. Therefore, an access structure Γ is the same as the closure of its basis $\Gamma_0, \mathrm{cl}(\Gamma_0)$. In the special case where $\Gamma = \{\mathbf{A} \mid \mathbf{A} \subseteq \mathbf{P} \text{ and } |\mathbf{A}| \geq m\}$, the secret sharing scheme is called an (m,n)-threshold scheme [3,4], where $|\mathbf{P}| = n$. A secret sharing scheme is called perfect if unqualified subsets of participants obtain no information regarding the

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

0898-1221/99/$ - see front matter Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX
PII: S0898-1221(99)00049-8

secret [5,6]. It means that the prior probability $p(K = K_0)$ equals the conditional probability $p(K = K_0 \mid$ given any shares of an unqualified set). The information theoretic models for threshold schemes and secret sharing schemes were defined by Karnin *et al.* [7] and Capocelli *et al.* [8], respectively. We refer to Gallager [9] and Hamming [10] for a treatment of information theory. Following the approach of [8], we can state the requirements for a secret sharing scheme by using the entropy function H as follows:

(1) any qualified subset can reconstruct the secret

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

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

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

An important issue in the implementation of perfect secret sharing schemes is the size of shares. Let $\mathbf{K}$ be the secret space and $\mathbf{S}$ be the maximum share space. The information rate for a secret sharing scheme is defined as $\rho = \log_2 |\mathbf{K}| / \log_2 |\mathbf{S}|$ (see [5]). The information rate for share S_i is defined as $\rho_i = \log_2 |\mathbf{K}| / \log_2 |\mathbf{S}_i|$, where $\mathbf{S}_i$ is the share space for S_i. We will use the notation $PS(\Gamma, \rho, q)$ to denote a perfect secret sharing scheme with access structure Γ and information rate ρ for a set of q keys. Given any access structure Γ, Ito *et al.* [2,11] showed that there exists a perfect secret sharing scheme to realize the structure. Benaloh and Leichter [1] proposed a different algorithm to realize secret sharing schemes for any given monotone access structures. In both constructions, the information rate decreases exponentially as a function of n, the number of participants. After that, many researchers focused on studying the perfect secret sharing scheme for graph-based access structure Γ having basis Γ_0, where Γ_0 is the collection of the pairs of participants corresponding to edges [5,6,8,12–16]. Among these constructions, Stinson [16] proposed the idea of decomposition construction which is more general than previous constructions [5,8,12–15]. In addition, he 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 $2/(d+1)$. Recently, Blundo *et al.* [17] showed that Stinson's lower bound is tight.

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, the graph-based access structure is the case of access structure with rank two. Perfect secret sharing schemes with access structures of constant rank were studied by Stinson [15]. 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

$$\rho \geq \frac{4}{(n-1)(n-2)},$$

if Γ is nonuniform and $n \equiv 2, 4 \pmod 6$ or

$$\rho \geq \frac{6}{(n-1)(n-2)},$$

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 $n' \equiv 2, 4 \pmod 6$. The degree of a participant in a secret sharing scheme with access structure $\mathrm{cl}(\Gamma_0)$ is defined to be the number of subsets in Γ_0 which contain the participant. Based on the edge-colourings of bipartite graphs, Stinson [15] also studied the construction of secret sharing schemes with access structures of rank m. The constructed secret sharing schemes have the information rate

$$\rho \geq \frac{m}{(2m-1) \cdot \binom{n-1}{m-2} + d},$$

where n is the number of participants and d is the maximum degree of any participant.

In this paper, we propose some recursive constructions for perfect secret sharing schemes with access structures of constant rank. If Γ is an access structure (either uniform or nonuniform) of rank three on n participants, we show that there exists a secret sharing scheme with information rate

$$\rho \geq \frac{6}{(n-1)^2+2},$$

for $n \geq 5$. If Γ is a uniform access structure of rank m on n participants, we show that there exists a secret sharing scheme with information rate

$$\rho \geq \frac{n-m+1}{\binom{n}{m}}.$$

Compared with the best previous constructions [15], our constructions have some improved lower bounds on the information rate.

2. PRELIMINARIES

Suppose Γ is an access structure having basis Γ_0. A λ-decomposition of Γ_0 consists of a collection $\{\Gamma_1, \ldots, \Gamma_t\}$ such that the following requirements are satisfied.

(1) $\Gamma_h \subseteq \Gamma_0$ for $1 \leq h \leq t$.
(2) For each $X \in \Gamma_0$, there exist at least λ indices $i_1 < \cdots < i_\lambda$ such that $X \in \Gamma_{i_j}$ for $1 \leq j \leq \lambda$.

Let $\mathbf{P}_h$ be the set of participants in a scheme with access structure $\mathrm{cl}(\Gamma_h)$. Stinson [16] proposed the Decomposition Construction (DC) for secret sharing schemes. The proposed construction is more general than other well-known constructions [5,8,12–14].

THEOREM 2.1. DECOMPOSITION CONSTRUCTION, DC. *(See [16].) Let Γ be an access structure on n participants, having basis Γ_0, and suppose that $\{\Gamma_1, \ldots, \Gamma_t\}$ is a λ-decomposition of Γ_0. Assume that for each access structure $\mathrm{cl}(\Gamma_h)$, there exists a perfect secret sharing scheme with information rate ρ_{ih} for each $p_i \in \mathbf{P}_h$, and a set of q keys. Then there exists a $PS(\Gamma, \rho, q^\lambda)$, where*

$$\rho = \min\left\{ \frac{\lambda}{\sum_{\{h: p_i \in P_h\}} (1/\rho_{ih})} : 1 \leq i \leq n \right\}.$$

Let's consider the case when the basis of an access structure is a graph and Γ_i's are complete multipartite graphs. Because there exists a $PS(\mathrm{cl}(G), \rho = 1, q)$ for any complete multipartite graph [5], we can obtain the following theorem.

THEOREM 2.2. *(See [6,16].) Suppose access structure G is a graph with vertex set V and edge set E for which a complete multipartite covering exists, say $\prod = \{G_1, \ldots, G_t\}$. For each vertex $v \in V$ define $R_v = |\{i : v \in V_i\}|$, where V_i denotes the vertex set of G_i. For each edge $e \in E$ define $T_e = |\{i : e \in E_i\}|$, where E_i denotes the edge set of G_i. Let $R = \max\{R_v : v \in V\}$ and $T = \min\{T_e : e \in E\}$. Then there exists a $PS(\mathrm{cl}(G), \rho, q^T)$, where q is a prime power and $\rho \geq T/R$.*

By decomposing graph into stars, Stinson [16] showed that for any graph G with n vertices having maximum degree d, there exists a perfect secret sharing scheme for the access structure in which the information rate is at least $2/(d+1)$. In the following, we propose a construction which is similar to the one proposed by Stinson [16].

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

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

Obviously, given y_i and y_j, for $i \neq j$, $f(x)$ can be determined uniquely. Therefore, one who gets two or more y_i's can recover the secret K. However, one without knowledge of any y_i obtains no information on the secret. Note that one who gets one y_i can obtain partial information on the secret.

The dealer selects n random numbers, $r_1, \ldots, r_n$ over $GF(q)$. 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 $1 \leq t \leq n$,

$$\begin{aligned} &a_{i,t} = r_i (\mathrm{mod}\, q), && \text{if } t = i, \\ &a_{i,t} = r_t + y_t (\mathrm{mod}\, q), && \text{if } \overline{p_i p_t} \text{ is an edge of } G, \quad \text{and} \\ &a_{i,t} \text{ is empty}, && \text{if } t \neq i \text{ and } \overline{p_i p_t} \text{ is not an edge of } G. \end{aligned}$$

Thus the constructed secret sharing scheme is a perfect secret sharing scheme with access structure G and information rate $2/(d+1)$.

THEOREM 2.3. *If Γ is a uniform access structure of rank two and degree d, then there exists a $PS(\Gamma, \rho, q^2)$, where $\rho \geq 2/(d+1)$.*

PROOF.

(I) First, we show that the above constructed secret sharing scheme for graph G is perfect.
   (a) Let X be a subset of participants and $X \in \Gamma$. So, 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 then recover the $f(x)$ and the secret K.
   (b) Let X be a subset of participants and $X \notin \Gamma$. 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 to 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 on the secret K.

(II) Second, we show that the above constructed secret sharing scheme has information rate $2/(d+1)$.

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 size of share S_i is $\log(q^{d_i+1})$, where d_i is the degree of vertex p_i of G. The maximal size of the shares is $\log(q^{d+1})$, where d is the maximum degree of G. The size of the secret is $\log(q^2)$. Thus, the information rate of the secret sharing scheme is

$$\rho = \frac{2 \cdot \log q}{(d+1) \cdot \log q} = \frac{2}{d+1}.$$

∎

3. SECRET SHARING SCHEMES WITH ACCESS STRUCTURES OF RANK THREE

In this section, we propose a decomposition construction of perfect secret sharing schemes with access structures of rank three, and evaluate the information rate of the constructed scheme. For an access structure of rank three, with basis Γ_0, we can decompose Γ_0 into $\{\Gamma_1, \Gamma_2\}$ such that $\Gamma_0 = \Gamma_1 \cup \Gamma_2$ where $\mathrm{cl}(\Gamma_1)$ is a uniform access structure of rank two and $\mathrm{cl}(\Gamma_2)$ is a uniform access structure of rank three.

Assume that $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ is the set of participants and 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 $q > 2n + 2$. Let $f(x) = K_6 x^5 + K_5 x^4 + K_4 x^3 + K_3 x^2 + K_2 x^1 + K_1 \ (\mathrm{mod}\, q)$. y_i is computed from $f(x)$ as follows:

$$y_i = f(i) (\mathrm{mod}\, q), \qquad \text{for } i = 1, \ldots, 2n + 2.$$

Thus one who gets six or more y_i's can recover $f(x)$ and then the secret K. However, one without knowledge of any y_i obtains no information on the secret.

We use G to denote the access structure $\mathrm{cl}(\Gamma_1)$ whose rank is two. From Section 2, we know that there exists a graph-based secret sharing scheme realizing $\mathrm{cl}(\Gamma_1)$ in which the secret is (y_{2n+1}, y_{2n+2}) and the share of participant p_i is $S_i(G)$.

In addition, we define G_i, for $1 \le i \le n$, is the graph with vertices $V(G_i)$ and edges $E(G_i)$, where

$$V(G_i) = \{p_j \mid \text{for all } p_j, \text{where } \{p_i, p_j, p_k\} \in \Gamma_2\}$$

and

$$E(G_i) = \{\overline{p_j p_k} \mid \text{for all } \overline{p_j p_k}, \text{where } \{p_i, p_j, p_k\} \in \Gamma_2\}.$$

The dealer selects $2n$ random numbers, $r_1, \ldots, r_{2n}$, over $GF(q)$. As the construction in Section 2, there exists a secret sharing scheme realizing G_i in which the secret is $(r_i + y_i, r_{n+i} + y_{n+i})$ 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

$$S_i = \langle r_i, r_{n+i}, a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n}, S_i(G) \rangle,$$

where $1 \le t \le n$,

$$\begin{array}{lll} a_{i,t} = S_i(G_t), & \text{if } p_i \in V(G_t), & \\ a_{i,t} = (r_t + y_t, r_{n+t} + y_{n+t}), & \text{if } \overline{p_i p_t} \in E(G), & \text{and} \\ a_{i,t} \text{ is empty}, & \text{otherwise}. & \end{array}$$

Thus the constructed secret sharing scheme is a perfect secret sharing scheme realizing the access structure with basis Γ_0.

THEOREM 3.1. *If Γ is an access structure (either uniform or nonuniform) of rank three on n participants, then there exists a $PS(\Gamma, \rho, q^6)$, where*

$$\rho \ge \frac{6}{(n-1)^2 + 2}.$$

PROOF.

PART I. First, we show that the above constructed secret sharing scheme is perfect.

(a) Let $X \in \mathrm{cl}(\Gamma_2)$ be a subset of participants. So, there exists $p_i, p_j, p_k \in X (i \ne j \ne k)$ such that $\{p_i, p_j, p_k\} \in \Gamma_2$. 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 then recover the $f(x)$ and the secret K.

Now, we consider the case of $X \notin \mathrm{cl}(\Gamma_2)$ but $X \in \mathrm{cl}(\Gamma_1)$. Let X be a subset of participants which satisfies $X \notin \mathrm{cl}(\Gamma_2)$ but $X \in \mathrm{cl}(\Gamma_1)$. So, there exists $p_i, p_j \in X (i \ne j)$ such that $\{p_i, p_j\} \in \Gamma_1$. Participant p_i owns r_i, r_{n+i}, $a_{i,j} = (r_j + y_j, r_{n+j} + y_{n+j})$, and $S_i(G)$. Participant p_j owns r_j, r_{n+j}, $a_{j,i} = (r_i + y_i, r_{n+i} + y_{n+i})$, and $S_j(G)$. They can recover y_i, y_{n+i}, y_j, y_{n+j}, y_{2n+1}, and y_{2n+2}, and then recover $f(x)$ and the secret K.

(b) Let $X \notin \Gamma$ be a subset of participants. Therefore, there do not exist three participants p_i, p_j, and p_k in X such that $\{p_i, p_j, p_k\} \in \Gamma_2$, or two participants p_i and p_j in X such that $\{p_i, p_j\} \in \Gamma_1$. We assume that X can recover the value y_i for some $i \in \{1, \ldots, 2n\}$.

Hence, there exist participant p_i who owns r_i, and participants p_j and p_k who can recover $r_i + y_i$ (or participant p_j who owns $r_i + y_i$). Thus $\overline{p_jp_k}$ is an edge of G_i (or $\overline{p_ip_j}$ is an edge of G). Thus $\{p_i, p_j, p_k\} \in \Gamma_2$ or $\{p_i, p_j\} \in \Gamma_1$. This is a contradiction. Hence X obtains no information on y_i for $1 \leq i \leq 2n$. In addition, X obtains no information on y_{2n+1}, y_{2n+2} because it does not contain two participants p_i and p_j in X such that $\overline{p_ip_j}$ is an edge of G. Therefore, X obtains no information on y_i, for $1 \leq i \leq 2n+2$, and hence the secret K.

PART II. Second, we show that the information rate of the above constructed secret sharing scheme is at least

$$\frac{6}{(n-1)^2+2}.$$

The share of participant p_i is

$$S_i = \langle r_i, r_{n+i}, a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n}, S_i(G) \rangle .$$

Let $d_i(G_t)$ be the degree of vertex p_i in G_t. The size of $a_{i,t}$ is equal to $\log(q^{d_i(G_t)+1})$ if $p_i \in V(G_t)$ or $\log(q^2)$ if $\overline{p_ip_t} \in E(G)$. The the size of $S_i(G)$ is equal to 0 if $p_i \notin V(G)$, or is equal to $\log(q^{d_i(G)+1})$ if $p_i \in V(G)$, where $d_i(G)$ is the degree of vertex p_i in G. Hence, the size of share S_i is equal to

$$\log\left(q^{\sum_{t:P_i \in G_t}(d_i(G_t)+1)+2}\right),$$

if $p_i \notin V(G)$, or

$$\log\left(q^{\sum_{t:P_i \in G_t}(d_i(G_t)+1)+d_i(G)+3}\right),$$

if $p_i \in V(G)$. Because the size of the secret is equal to $\log(q^6)$, the information rate of the share S_i, ρ_i is equal to

$$\frac{6}{\sum\limits_{t:p_i \in G_t}(d_i(G_t)+1)+2},$$

if $p_i \notin V(G)$, or is equal to

$$\frac{6}{\sum\limits_{t:p_i \in G_t}(d_i(G_t)+1)+d_i(G)+3},$$

if $p_i \in V(G)$.

(a) Γ is uniform: if Γ is a uniform access structure of rank three, then ρ_i is equal to

$$\frac{6}{\sum\limits_{t:p_i \in G_t}(d_i(G_t)+1)+2}.$$

Because $\rho = \min_i\{\rho_i\}$, the information rate of the proposed secret sharing scheme is equal to

$$\frac{6}{\max\limits_i\left\{\sum\limits_{t:p_i \in G_t}(d_i(G_t)+1)\right\}+2},$$

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

$$E(G_i) = \{\overline{p_jp_k} \mid \text{for all } \overline{p_jp_k}, \text{where } \{p_i, p_j, p_k\} \in \Gamma_0\}.$$

In the worst case when $d_i(G_t) = n-2$ for all i and t, the lower bound of the information rate

$$\frac{6}{(n-1)^2+2}$$

can be achieved, where n is the number of participants.

(b) Γ is nonuniform: by the same way in (a), we can prove that

$$\rho_i \geq \frac{6}{(n-1)^2+2},$$

if $p_i \notin V(G)$. If $p_i \in V(G)$ and $\overline{p_i p_t} \in E(G)$, then $d_i(G_t) = 0$. If $p_i \in V(G)$ and $\overline{p_i p_t} \notin E(G)$, then $d_i(G_t) \leq n-k-2$, where $k = d_i(G), 1 \leq k \leq n-2$. Therefore,

$$\rho_i \geq \frac{6}{(n-1)^2+2},$$

if $p_i \notin V(G)$, or

$$\rho_i \geq \frac{6}{(n-k-1)^2+k+3},$$

if $p_i \in V(G)$. Because $(n-1)^2+2 \geq (n-k-1)^2+k+3$ when $n \geq 5$ and $k \geq 1$,

$$\rho_i \geq \min\left\{\frac{6}{(n-1)^2+2}, \frac{6}{(n-k-1)^2+k+3}\right\} = \frac{6}{(n-1)^2+2}.$$

Therefore,

$$\rho = \min_i\{\rho_i\} \geq \frac{6}{(n-1)^2+2}.$$ ∎

Compared with the lower bound provided by Stinson [15] in some cases, our lower bound is better than Stinson's lower bound. The comparison can be seen in Table 1 and Table 2.

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

n	Stinson's Method	Our Method
$n \equiv 0 \pmod 6$	$\rho \geq \frac{6}{n(n+1)}$	$\rho \geq \frac{6}{(n-1)^2+2}^*$
$n \equiv 1,3 \pmod 6$	$\rho \geq \frac{6}{n(n-1)}$	$\rho \geq \frac{6}{(n-1)^2+2}^*$
$n \equiv 2,4 \pmod 6$	$\rho \geq \frac{6}{(n-1)(n-2)}^*$	$\rho \geq \frac{6}{(n-1)^2+2}$
$n \equiv 5 \pmod 6$	$\rho \geq \frac{6}{(n+1)(n+2)}$	$\rho \geq \frac{6}{(n-1)^2+2}^*$

Table 2. Bounds on the information rate for nonuniform access structures of rank three on n participants for $n \geq 5$, where $*$ denotes the method providing the better bound.

n	Stinson's Method	Our Method
$n \equiv 0 \pmod 6$	$\rho \geq \frac{4}{n(n+1)}$	$\rho \geq \frac{6}{(n+1)^2+2}^*$
$n \equiv 1,3 \pmod 6$	$\rho \geq \frac{4}{n(n-1)}$	
$n \equiv 2,4 \pmod 6$	$\rho \geq \frac{4}{(n-1)(n-2)}$	
$n \equiv 5 \pmod 6$	$\rho \geq \frac{4}{(n+1)(n+2)}$	

4. SECRET SHARING SCHEMES WITH UNIFORM ACCESS STRUCTURES OF RANK m

In this section, we propose a decomposition construction of secret sharing schemes with uniform access structures of rank m. We construct secret sharing schemes with uniform access structures of rank m by using the secret sharing schemes with uniform access structures of rank $m-1$. Let Γ be a uniform access structure of rank m on n participants. Assume that $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ is the set of participants and the basis of Γ is Γ_0. We can decompose Γ_0 into the union of Γ_i's, for $1 \leq i \leq n$, where $\Gamma_i = \{X : X \in \Gamma_0 \text{ and } X \text{ contains participant } p_i\}$. Thus $\Gamma = \mathrm{cl}(\Gamma_0) = \mathrm{cl}(\Gamma_1) \cup \cdots \cup \mathrm{cl}(\Gamma_n)$. We define $\Gamma_i^* = \{X : X \cup \{p_i\} \in \Gamma_i\}$, i.e., Γ_i^* is the set of Γ_i which participant p_i is removed from each element in Γ_i. Therefore, each $\mathrm{cl}(\Gamma_i^*)$ is a uniform access structure of rank $m-1$. Here we define $h(i)$ to be a function which indicates the secret space of the secret sharing schemes with uniform access structures of rank i to be $(GF(q))^{h(i)}$. We assume that the secret $K = (K_1, K_2, \ldots, K_m)$, where each K_i, for $1 \leq i \leq m$, is taken randomly from $(GF(q))^{h(m-1)}$. The dealer selects a polynomial $f(x)$ of degree $m \cdot h(m-1) - 1$ with coefficients K and computes y_i as follows:

$$y_i = f(i) \,(\mathrm{mod}\, q), \qquad \text{for } i = 1, \ldots, n \cdot h(m-1).$$

Thus one who gets $m \cdot h(m-1)$ or more y_i's can recover $f(x)$ and then the secret K. However, one without knowledge of any y_i obtains no information on the secret. We use $Y_1, Y_2, \ldots, Y_n$ over $(GF(q))^{h(m-1)}$ to denote these $n \cdot h(m-1)$ y_i's. The dealer selects n random numbers $R_1, R_2, \ldots, R_n$ over $(GF(q))^{h(m-1)}$. We assume that there exists a secret sharing scheme realizing $\mathrm{cl}(\Gamma_i^*)$ 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

$$S_i = \left\langle R_i, S_i(\Gamma_1^*), \ldots, S_i(\Gamma_{i-1}^*), S_i(\Gamma_{i+1}^*), \ldots, S_i(\Gamma_n^*) \right\rangle.$$

Thus, the constructed secret sharing scheme is a perfect secret sharing scheme with access structure Γ.

THEOREM 4.1. *Let Γ be a uniform access structure of rank m on n participants. Then there exists a*

$$PS\left(\Gamma, \frac{n-m+1}{\binom{n}{m}}, q^{m!}\right),$$

for $q > n \cdot (m-1)!$.

PROOF.

(I) First we show that the above constructed secret sharing scheme is a perfect secret sharing scheme realizing the uniform access structure Γ of rank m.

(a) Let X be a subset of participants and $X \in \Gamma$. Without loss of generalization, we assume that $X = \{p_1, p_2, \ldots, p_m\}$. Because $X \backslash \{p_i\} \in \Gamma_i^*$, X can recover $R_i + Y_i$, for $1 \leq i \leq m$. In addition, each participant p_i owns R_i. Therefore, they can recover Y_i, for $1 \leq i \leq m$, and then recover the $f(x)$ and the secret K.

(b) Let X be a subset of participants and $X \notin \Gamma$. We assume that X can recover y_i. Then X must be able to recover r_i and $r_i + y_i$. Thus, $p_i \in X$ and there exists a subset X' of X such that $X' \in \Gamma_i^*$. Therefore, $X' \cup \{p_i\} \in \Gamma_i$. That is, $X' \cup \{p_i\}$ is a qualified subset. Because $X' \cup \{p_i\} \subseteq X$, X is also a qualified subset. This is a contradiction. Hence X cannot recover any y_i. Thus X obtains no information on the secret K.

(II) Second, we show that the information rate of the above constructed secret sharing scheme is at least

$$\frac{n-m+1}{\binom{n}{m}}.$$

The secret space $(GF(q))^{h(m)}$, of the constructed secret sharing scheme is equal to $(GF(q))^{m \cdot h(m-1)}$. Therefore, $h(m) = m \cdot h(m-1)$. From Section 2, we know that there exist secret sharing schemes with access structure of rank two in which $h(2)$ is equal to 2. Therefore, we can obtain $h(m) = m!$. That is, the secret space of the constructed secret sharing scheme is equal to $(GF(q))^{m!}$. We define $\rho(m,n)$ to be the lower bound of the information rate of secret sharing schemes with uniform access structures of rank m on n participants. Therefore,

$$\rho(m,n) = \frac{m}{(n-1) \cdot (1/\rho(m-1,n-1)) + 1}.$$

Because

$$0 \le \rho(m-1,n-1) \le 1, \qquad \frac{\rho(m,n)}{\rho(m-1,n-1)} = \frac{m}{(n-1)+\rho(m-1,n-1)} \ge \frac{m}{n}.$$

We can obtain

$$\rho(m,n) \ge \frac{m}{n} \cdot \rho(m-1,n-1) \ge \frac{m \cdot (m-1) \cdot \ldots \cdot 3}{n \cdot (n-1) \cdot \ldots \cdot (n-k+3)} \cdot \rho(2,n-k+2).$$

From Section 2, we know that

$$\rho(2,n-k+2) \ge \frac{2}{n-k+2}.$$

Therefore,

$$\rho(m,n) \ge \frac{m! \cdot (n-m+1)!}{n!} = \frac{n-m+1}{\binom{n}{m}}.$$ ∎

Compared with the best previous lower bound of $\rho(m,n)$, studied by Stinson [15], which is

$$\frac{m}{(2m-1) \cdot \binom{n-1}{m-2} + d},$$

where d is the maximum degree of any participant, our lower bound is better than Stinson's lower bound when

$$m \ge \frac{3+\sqrt{8n+1}}{4}.$$

5. CONCLUSIONS

Based on the secret sharing schemes with graph-based access structures, we propose a decomposition construction to realize the perfect secret sharing schemes with uniform access structures of rank 3. In addition, we give a recursive construction for perfect secret sharing schemes with uniform access structures of constant rank. If Γ is an access structure (either uniform or nonuniform) of rank three on n participants, we show that there exists a secret sharing scheme with information rate

$$\rho \ge \frac{6}{(n-1)^2+2},$$

for $n \ge 5$. If Γ is a uniform access structure of rank m on n participants, we show that there exists a secret sharing scheme with information rate

$$\rho \ge \frac{n-m+1}{\binom{n}{m}}.$$

Compared with the best previous constructions, our constructions have some improved lower bounds on the information rate.

REFERENCES

1. 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).
2. M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, In *Proc. IEEE Globecom'87*, Tokyo, pp. 99–102, (1987).
3. G.R. Blakley, Safeguarding cryptographic keys, In *Proc. 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. M. van Dijk, On the information rate of perfect secret sharing schemes, *Designs, Codes and Cryptography* **6**, 143–169, (1995).
7. E.D. Karnin, J.W. Greene and M.E. Hellman, On secret sharing systems, *IEEE Trans. on Inform. Theory* **29**, 35–41, (1983).
8. R.M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, *Journal of Cryptology* **6**, 157–167, (1993).
9. R.G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, (1968).
10. R.W. Hamming, *Coding and Information Theory*, Prentice-Hall, Englewood Cliffs, NJ, (1986).
11. M. Ito, A. Saito and T. Nishizeki, Multiple assignment scheme for sharing secret, *Journal of Cryptology* **6**, 15–20, (1993).
12. C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, On the information rate of secret sharing schemes, In *Advance in Cryptology-CRYPTO'92, Lecture Notes in Comput. Sci.*, Volume 740, pp. 148–167, (1993).
13. C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, In *Advance in Cryptology-Proceedings of Eurocrypt'92, Lecture Notes in Comput. Sci.*, Volume 658, pp. 1–24, (1993).
14. C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, *Journal of Cryptology* **8**, 39–63, (1995).
15. 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.*, Volume 740, pp. 168–182, (1993).
16. D.R. Stinson, Decomposition constructions for secret sharing schemes, *IEEE Trans. Inform. Theory* **40**, 118–125, (1994).
17. C. Blundo, A. De Santis, R. De Simone and U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Designs, Codes and Cryptography* **11** (1), 1–25, (1997).