Information Sciences 240 (2013) 83–94

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

New bounds on the average information rate of secret-sharing schemes for graph-based weighted threshold access structures

Hui-Chuan Lu [a,b,*,1], Hung-Lin Fu [b,2]

[a] Center for Basic Required Courses, National United University, Miaoli 36003, Taiwan
[b] Department of Applied Mathematics, National Chaio Tung University, Hsinchu 30010, Taiwan

ARTICLE INFO

Article history:
Received 23 July 2011
Received in revised form 13 March 2013
Accepted 25 March 2013
Available online 2 April 2013

Keywords:
Secret-sharing scheme
Access structure
Optimal information rate
Optimal average information rate
Weighted threshold access structure
Complete multipartite covering

ABSTRACT

A secret-sharing scheme is a protocol by which a dealer distributes shares of a secret key among a set of n participants in such a way that only qualified subsets of participants can reconstruct the secret key from the shares they received, while unqualified subsets have no information about the secret key. The collection of all qualified subsets is called the access structure of this scheme. The information rate (resp. average information rate) of a secret-sharing scheme is the ratio between the size of the secret key and the maximum size (resp. average size) of the shares. In a weighted threshold scheme, each participant has his or her own weight. A subset is qualified if and only if the sum of the weights of participants in the subset is not less than the given threshold. Morillo et al. [19] considered the schemes for weighted threshold access structure that can be represented by graphs called k-weighted graphs. They characterized this kind of access structures and derived a result on the information rate. In this paper, we deal with the average information rate of the secret-sharing schemes for these structures. Two sophisticated constructions are presented, each of which has its own advantages and both of them perform very well when n/k is large.

1. Introduction

A *secret-sharing scheme* is a protocol by means of which a dealer distributes a secret key among a set of participants $\mathcal{P}$ so that only qualified subsets of $\mathcal{P}$ can reconstruct the secret key whereas unqualified subsets of $\mathcal{P}$ have no information about the secret key. The family of all qualified subsets is called the *access structure* of the scheme. In practice, an access structure has to be *monotone* which means any subset of $\mathcal{P}$ containing a qualified subset must also be qualified. The *basis* Γ_0 of an access structure Γ is the set of all minimal subsets in Γ. The access structure Γ is called the *closure* of Γ_0, denoted as $\Gamma = Cl(\Gamma_0)$. In addition, Γ is r-homogeneous if the cardinality of each subset in Γ_0 is r.

The first secret-sharing schemes were (t,n)-*threshold schemes*. These schemes were introduced by Shamir [22] and Blakley [2] independently in 1979. The basis of the access structure for such a scheme consists of all t-subsets of the set $\mathcal{P}$ of participants of size n. Related problems have received considerable attention since then. Secret-sharing schemes for various access structures have been widely studied [2–7,9,12,15,19,20,22,24–26]. Many modified versions of secret-sharing schemes with additional capacities were proposed [8,11,13,14,16,17,21,23,27]. The reader is referred to [1] for a comprehensive survey. Secret sharing has been an interesting branch of modern cryptography.

[*] Corresponding author at: Center for Basic Required Courses, National United University, Miaoli 36003, Taiwan.
E-mail addresses: hjlu@nuu.edu.tw, hht0936@seed.net.tw (H.-C. Lu).

[1] Research supported in part by NSC 100-2115-M-239-001.

[2] Research supported in part by NSC 100-2115-M-009-005-MY3.

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.03.047

One of the most important research directions regarding secret-sharing schemes is to establish bounds on the size of the shares given to the participants and thereby obtain bounds on the storage and communication complexity. There are two major tools to measure the efficiency of a secret-sharing scheme, namely the *information rate* and the *average information rate* of a scheme. The information rate of a secret-sharing scheme is the ratio between the length (in bits) of the secret key and the maximum length of the shares given to the participants. The average information rate of a secret-sharing scheme is the ratio between the length of the secret key and the average length of all shares given to the participants. In a practical implementation of a secret-sharing scheme, these rates are expected to be as high as possible. Therefore, researchers also concern about the highest rates a secret-sharing scheme can have for a given access structure. The *optimal (average) information rate* of an access structure is the maximum (average) information rate over all secret-sharing schemes which realize that access structure.

Graph-based access structures have been widely studied during the past decades. In such an access structure, each vertex of a graph G represents a participant and each edge represents a minimal qualified subset, that is, $\mathcal{P} = V(G)$ and $\Gamma = Cl(E(G))$. The optimal information rate (resp. optimal average information rate) of an access structure based on a graph G is denoted as $\rho^*(G)$ (resp. $\tilde{\rho}^*(G)$). It is easy to see that $\rho^*(G) \leqslant \tilde{\rho}^*(G) \leqslant 1$ and that $\rho^*(G) = 1$ if and only if $\tilde{\rho}^*(G) = 1$. A secret-sharing scheme with the information rate equal to one is then called an ideal secret-sharing scheme. An access structure is ideal if there exists an ideal secret-sharing scheme for it. Brickell and Devenport [6] have completely characterized ideal graph-based access structures. For general graphs, Stinson [26] showed that $\rho^*(G) \geqslant \frac{2}{d+1}$ where d is the maximum degree of G and $\tilde{\rho}^*(G) \geqslant \frac{2n}{2m+n}$ where $n = |V(G)|$ and $m = |E(G)|$. Due to the difficulty of the derivation of good results on general graphs, most efforts have been focused on small graphs [5,12,15] and graphs with better structures [3,5,9,10,18,26].

Morillo et al. [19] considered the weighted threshold secret-sharing schemes. This is the case when every participant is given a weight depending on his or her position in an organization. A set of participants is in the access structure if and only if the sum of the weights of all participants in the set is not less than the given threshold. Morillo et al. characterized weighted threshold access structures based on graphs and studied their optimal information rate. Since these access structures are more applicable in real-life situation, an in-depth investigation can have a significant contribution to the application of secret sharing. We are motivated to construct better secret-sharing schemes for them and have a more detailed analysis of the average information rate of our schemes.

This paper is organized as follows. Definitions, notations and basic known results are introduced in Section 2. Morillo's characterization and constructions of secret-sharing schemes of graph-based weighted threshold access structures are presented in Section 3. In Section 4, we start with an observation on the structure of the graphs that represent weighted threshold access structures, and then our first construction is introduced. Subsequently, one more sophisticated construction is presented in Section 5. Finally, we give a comparison of these constructions in Section 6.

2. Preliminaries

Let $\mathcal{P}$ be the set of all participants, $\mathcal{K}$ be the set of all secret keys, $\Gamma \subseteq 2^{\mathcal{P}}$ be the access structure and S be the set of all possible shares. Given a secret key $d \in \mathcal{K}$, a dealer D gives to participant p a share $s_{p,d} \in S_p$ where S_p is the set of all shares participant p receives from the dealer corresponding to all keys in $\mathcal{K}$. A *distribution rule* is a function $f : \{D\} \cup \mathcal{P} \to \mathcal{K} \cup S$ with $f(D) \in \mathcal{K}$ and $f(p) \in S$ for all $p \in \mathcal{P}$. $f(D)$ is the secret key to be distributed and $f(p)$ is the share participant p receives from the dealer for key $f(D)$. Let $\mathcal{F}$ be a collection of distribution rules and $\mathcal{F}_d = \{f \in \mathcal{F} : f(D) = d\}$. We call $\mathcal{F}$ a perfect secret-sharing scheme if the following two conditions are satisfied:

(i) Given any $B \in \Gamma$ and $f, g \in \mathcal{F}$, if $f(p) = g(p)$ for all $p \in B$, then $f(D) = g(D)$.
(ii) Given any $B \notin \Gamma$ and any function g: $B \to S$, there exists a nonnegative integer $\lambda(g,B)$ such that, for each $d \in \mathcal{K}$,

$$|\{f \in \mathcal{F}_d | f(p) = g(p),\ \forall p \in B\}| = \lambda(g, B).$$

The first condition guarantees that the shares given to a qualified subset uniquely determine the secret key, while the second ensures that the shares given to an unqualified subset reveal no information about the secret key. When these two conditions are made, we say that this secret-sharing scheme $\mathcal{F}$ realizes the access structure Γ. Since all schemes mentioned in this paper are perfect, we will simply use "secret-sharing scheme" for "perfect secret-sharing scheme" throughout this paper. In a secret-sharing scheme $\mathcal{F}$, the information rate, denoted $\rho(\mathcal{F})$, is defined as

$$\rho(\mathcal{F}) = \frac{\log_2|\mathcal{K}|}{\max\{\log_2|S_p| : p \in \mathcal{P}\}}$$

and the average information rate, denoted $\tilde{\rho}(\mathcal{F})$, is defined as

$$\tilde{\rho}(\mathcal{F}) = \frac{\log_2|\mathcal{K}|}{\frac{1}{|\mathcal{P}|}\sum_{p\in\mathcal{P}}\log_2|S_p|} = \frac{|\mathcal{P}|\log_2|\mathcal{K}|}{\sum_{p\in\mathcal{P}}\log_2|S_p|}.$$

Example 2.1. $\mathcal{P} = \{a, b, c\}$, $\Gamma_0 = \{\{a,b\},\{b,c\}\}$, $\mathcal{K} = GF(3)$. Let $\mathcal{F} = \{f_{r,d} | r, d \in GF(3)\}$ where $f_{r,d}(D) = d$, $f_{r,d}(a) = f_{r,d}(c) = r$ and $f_{r,d}(b) = r + d$. This scheme can be represented by the following table:

D	a	b	c
0	0	0	0
0	1	1	1
0	2	2	2
1	0	1	0
1	1	2	1
1	2	0	2
2	0	2	0
2	1	0	1
2	2	1	2

Note that each row in the table represents a distribution rule. One can easily check that this scheme is a secret-sharing scheme and $\rho(\mathcal{F}) = \tilde{\rho}(\mathcal{F}) = 1$ since $\mathcal{K} = S_a = S_b = S_c = GF(3)$. This scheme is in fact an ideal one.

In this paper, only graph-based access structures are considered. In this case, $\Gamma = Cl(E(G))$ is 2-homogeneous. The graphs with optimal rate $\rho^*(G) = 1$ or $\tilde{\rho}^*(G) = 1$ have been completely characterized by Brickell and Devenport.

Theorem 2.2 [6]. *Suppose that G is a connected graph, then $\rho^*(G) = 1$ if and only if G is a complete multipartite graph.*

Example 2.1 shows that $\rho^*(K_{1,2}) = 1$ since the access structure of the scheme is $Cl(K_{1,2})$. For graphs that are not complete multipartite graphs, Blundo et al. [5] have shown the following fact.

Theorem 2.3 [5]. *Suppose that G is a connected graph that is not a complete multipartite graph, then $\rho^*(G) \leqslant \frac{2}{3}$ and $\tilde{\rho}^*(G) \leqslant \frac{n}{n+1}$ where $n = |V(G)|$.*

When dealing with information rates, the following lemma is especially helpful.

Lemma 2.4 [5]. *If G' is an induced subgraph of graph G, then $\rho^*(G) \leqslant \rho^*(G')$.*

Stinson [26] proposed a very useful decomposition construction which enables us to build up secret-sharing schemes for larger graphs using smaller complete multipartite graph through *complete multipartite coverings*. A complete multipartite covering of a graph G is a collection of complete multipartite subgraphs $\{G_1, G_2, \ldots, G_l\}$ of G such that each edge of G belongs to at least one subgraph G_i.

Theorem 2.5 [26]. *Suppose that $\{G_1, G_2, \ldots, G_l\}$ is a complete multipartite covering of a graph G with $V(G) = \{1, 2, \ldots, n\}$. Let $R_i = |\{j | i \in V(G_j)\}|$ and $R = \max_{1 \leqslant i \leqslant n} R_i$. Then there exists a secret-sharing scheme for access structure Cl(E(G)) with information rate ρ and average information rate $\tilde{\rho}$ where*

$$\rho = \frac{1}{R} \quad \text{and} \quad \tilde{\rho} = \frac{n}{\sum_{i=1}^{n} R_i} = \frac{n}{\sum_{i=1}^{l} |V(G_i)|}.$$

According to the theorem, in order to construct a secret-sharing scheme with higher information rate (resp. average information rate), we need a complete multipartite covering with less maximum number of occurrence of a vertex (resp. less total number of occurrences of the vertices) in the covering.

3. Weighted threshold secret-sharing scheme

Given a set of n participants $\mathcal{P}$, a threshold $t > 0$ and a weight function $w : \mathcal{P} \to \mathbb{R}$ with $w(p) \geqslant 0$ for all $p \in \mathcal{P}$, the (t, n, w)-weighted threshold access structure consists of all subset $A \subseteq \mathcal{P}$ such that $w(A) = \sum_{p \in A} w(p) \geqslant t$. Morillo et al. [19] showed that any weighted access structure determined by a non-integer-valued weight function and a non-integer threshold can also be determined by an integer-valued weight function and an integer threshold. So, considering integer-valued weight functions is sufficient in our problem. In the remainder of the paper, we assume that a weight function w is given. An access structure $\Gamma = Cl(\Gamma_0)$ is said to be *connected* if for any participant $p \in \mathcal{P}$, there exists $A \in \Gamma_0$ such that $p \in A$. Throughout this paper, we consider 2-homogeneous connected weighted threshold access structure and exclude the case where any participant has zero-weight. This kind of access structure can be represented by a graph G. In this graph, there is a set C of vertices, each of which is adjacent to all other vertices in G. The weight of each vertex in C is higher than the weight of any vertex not in C. If $C \neq V(G)$, removing C from the graph G produces a nonempty set A of isolated vertices, each of which has lower weight than any other vertex not in A. If $C \cup A \neq V(G)$, the subgraph G' induced by $V(G) \backslash (C \cup A)$ represents a 2-homogeneous connected weighted threshold access structure $\Gamma' = \{B \subseteq \mathcal{P} \setminus (C \cup A) | w(B) \geqslant t\}$. Repeating these processes, the structure of G can be clearly characterized in the following theorem.

Theorem 3.1 [19]. *Let G be a graph that represents the 2-homogeneous connected weighted threshold access structure Γ. Then, there exists a unique partition of the vertices of G,*

$$P = C_1 \cup A_1 \cup C_2 \cup A_2 \cup \cdots \cup C_k \cup A_k,$$

where $C_i \neq \emptyset$ for i = 1, . . . , k, $A_i \neq \emptyset$ if i = 1, . . . , k − 1 and either $A_k = \emptyset$ and $|C_k| \geqslant 2$ or $|A_k| \geqslant 2$, such that the set of edges of G is

$$\Gamma_0 = \left\{ \{u, v\} | u, v \in \bigcup_{i=1}^{k} C_i, u \neq v \right\} \cup \{\{v, p\} | v \in C_i,\ p \in A_j,\ 1 \leqslant i \leqslant j \leqslant k\}.$$

They also showed that any graph with a partition described in Theorem 3.1 represents a 2-homogeneous connected weighted threshold access structure. A such graph is then called k-weighted where k is the parameter used in Theorem 3.1. Since the structure of a k-weighted graph is completely determined by the values $|A_i|$'s and $|C_i|$'s, $i = 1, 2, \ldots, k$, we denote the k-weighted graph by $W(|A_1|, \ldots, |A_k|, |C_1|, \ldots, |C_k|)$. Observe that the subgraph induced by $\bigcup_{i=1}^{l}(A_{j_i} \cup C_{j_i})$ where $1 \leqslant j_1 < j_2 < \cdots < j_l \leqslant k$ is an l-weighted graph $W(|A_{j_1}|, \ldots, |A_{j_l}|, |C_{j_1}|, \ldots, |C_{j_l}|)$. Morillo et al. gave a complete multipartite decomposition for $(2^q - 1)$-weighted graph in which the maximum number of occurrence R of a vertex is not greater than q. Then, by Lemma 2.4, a lower bound on optimal information rate for k-weighted graph for all k follows.

Theorem 3.2 [19]. *Let $\Gamma = \{A \subseteq \mathcal{P} | w(A) \geqslant t\}$ be an access structure that is represented by a k-weighted graph G. Then* $\rho^*(G) \geqslant \frac{1}{\lceil \log_2(k+1) \rceil}$.

For the average information rate, we need to find complete multipartite coverings for k-weighted graphs for each value of k. For convenience, we make a slight modification to the notation given in Theorem 3.1. In the case where $A_k = \emptyset$ and $|C_k| \geqslant 2$, we move one (arbitrarily chosen) vertex from C_k to A_k. So, in our model, none of A_i's and C_i's are empty. Now, we are ready for our constructions.

4. Construction (I)

4.1. An observation

We observe that any k-weighted graph can be obtained by alternately applying two graph operations starting with a single vertex. Let us introduce these operations first. By "*splitting* vertex v of a graph G into m vertices $v_1, \ldots, v_m$", denoted $S(v; \{v_1, \ldots, v_m\})$, we obtain a graph $G^{S(v;\{v_1,\ldots,v_m\})} = G^*$ where $V(G^*) = (V(G) - \{v\}) \cup \{v_1, v_2, \ldots, v_m\}$ and $E(G^*) = E(G - v) \cup \{v_i u | vu \in E(G)$ and $i = 1,2,\ldots,m\}$. If we further add the set of edges $\{v_i v_j | 1 \leqslant i < j \leqslant m\}$ to $E(G^*)$, then we obtain a graph $G^{E(v;\{v_1,\ldots,v_m\})}$. This graph is said to be obtained by "*expanding* vertex v into m vertices $v_1, \ldots, v_m$ from the original graph G and this operation is denoted by $E(v; \{v_1, \ldots, v_m\})$. For convenience, we use $\langle V_1, V_2 \rangle_G$ to denote the set of edges $\{uv | u \in V_1, v \in V_2$ and $uv \in E(G)\}$ for any two disjoint subsets of vertices V_1 and V_2 in G.

Given a k-weighted graph $G = W(a_1, a_2, \ldots, a_k, c_1, c_2, \ldots, c_k)$, we let $A_i = \left\{u_1^i, u_2^i, \ldots, u_{a_i}^i\right\}$ and $C_i = \left\{v_1^i, v_2^i, \ldots, v_{c_i}^i\right\}$, $i = 1,2,\ldots,k$. In what follows, we propose an algorithm showing how the given graph is constructed from a single vertex by splitting and expanding.

Algorithm 1

```
$G_0 \leftarrow \{u_0\}$.
For $i \leftarrow 1$ to $k$ do
    $G_i \leftarrow G_{i-1}^{E(u_0;C_i \cup \{u_0\})}$
    $G_i \leftarrow G_i^{S(u_0;A_i^*)}$ where $A_i^* = \begin{cases} A_i \cup \{u_0\}, & \text{if } 1 \leqslant i < k; \\ A_k, & \text{if } i = k. \end{cases}$
Output the $k$-weighted graph $G_k$.
```

Theorem 4.1. *The proposed algorithm produces the given k-weight graph G from a single vertex.*

Proof. The edges in $\langle A_i, C_j \rangle, j \leqslant i$, are produced by the operation $S(u_0; A_i^*)$ and edges in $\langle C_i, C_j \rangle, j < i$, and within the part C_i are all produced by $E(u_0, C_i^*)$. So, G is a subgraph of G_k. Next, the number of edges produced in this algorithm is

$$\sum_{i=1}^{k-1}\left(\binom{c_i+1}{2}+c_i\sum_{j=1}^{i-1}c_j+a_i\sum_{j=1}^{i}c_j\right)+\binom{c_k+1}{2}+c_k\sum_{j=1}^{k-1}c_j+(a_k-1)\sum_{j=1}^{k}c_j=\sum_{i=1}^{k}\left(\binom{c_i+1}{2}+c_i\sum_{j=1}^{i-1}c_j+a_i\sum_{j=1}^{i}c_j\right)$$
$$-\sum_{j=1}^{k}c_j=\sum_{j=1}^{k}\left(\binom{c_i}{2}+c_i\sum_{j=1}^{i-1}c_j+a_i\sum_{j=1}^{i}c_j\right)$$

which is exactly the size of the given G. Hence, the proof is completed. □

4.2. Construction (I)

Before we can literally describe our first construction, there are some more notations needed to be introduced. For any l disjoint sets of vertices $V_1, V_2, \ldots, V_l$, we use $K(V_1, V_2, \ldots, V_l)$ to denote the complete multipartite graph with partite sets V_1, V_2, $\ldots$ and V_l. Let G_l be the l-weighted graph with vertex set $\left(\bigcup_{i=1}^{l}A_i\right)\cup\left(\bigcup_{i=1}^{l}C_i\right)$, $l\leqslant k$. Define B_l, $l\leqslant k$, to be the graph obtained from G_l by removing all edges connecting vertices in $\bigcup_{i=1}^{l}C_i$. Then B_l is a bipartite graph with partite sets $\bigcup_{i=1}^{l}A_i$ and $\bigcup_{i=1}^{l}C_i$. Next, we use M_{l_1,l_2} to denote the complete multipartite graph $K\left(C_1, C_2, \ldots, C_{l_1-1}, \left\{v_1^{l_1}\right\}, \left\{v_2^{l_1}\right\}, \ldots, \left\{v_{c_{l_1}}^{l_1}\right\}, \left(\bigcup_{j=l_1+1}^{l_2}C_j\right)\cup\left(\bigcup_{j=l_1}^{l_2}A_j\right)\right)$, $1\leqslant l_1\leqslant l_2\leqslant k$. In the following lemma, H_j stands for the complete multipartite graph $K(C_1, C_2, \ldots, C_{j-1}, A_{j-1}, A_j)$, $2\leqslant j\leqslant k$.

Lemma 4.2. *Π_l^B is a complete multipartite covering of B_l where*

$$\Pi_l^B=\begin{cases}\{H_{2i}, K(A_{2i}, C_{2i})\mid i=1,2,\ldots,\frac{l}{2}\}, & \text{if } l \text{ is even;}\\ \{K(A_1, C_1), H_{2i+1}, K(A_{2i+1}, C_{2i+1})\mid i=1,2,\ldots,\frac{l-1}{2}\}, & \text{if } l \text{ is odd.}\end{cases}$$

Proof. When l is even, the edges in $\langle A_{2i}, C_j\rangle_{B_l}$ with $j<2i$ and in $\langle A_{2i-1}, C_j\rangle_{B_l}$ with $j\leqslant 2i-1$ appear in the subgraph H_{2i}, for $i=1,2,\ldots,\frac{l}{2}$, while the edges in $\langle A_{2i}, C_{2i}\rangle_{B_l}$ appear in the subgraph $K(A_{2i}, C_{2i})$. The edges of B_l are then all used up. For odd l, the argument is similar. □

With these notations in mind, we are able to give our complete multipartite covering Π_k of G_k. Let Π_k be obtained recursively by letting $\Pi_1=\{G_1\}$, $\Pi_2=\left\{K\left(\{v_1^1\},\{v_2^1\},\ldots,\left\{v_{c_1}^1\right\},A_1\right),M_{2,2}\right\}$, $\Pi_3=\left\{K\left(\{v_1^1\},\{v_2^1\},\ldots,\left\{v_{c_1}^1\right\},A_1\right),\right.$ $K\left(\{v_1^3\},\ldots,\left\{v_{c_3}^3\right\},A_3\right),M_{2,3}\}$ and, for $k\geqslant 4$, $\Pi_k=\Pi^B_{\lfloor\frac{k+1}{2}\rfloor}\cup\left\{M_{\lfloor\frac{k+1}{2}\rfloor+1,k}\right\}\cup\Pi_{\lfloor\frac{k}{2}\rfloor-1}$ where $\Pi_{\lfloor\frac{k}{2}\rfloor-1}$ is the complete multipartite covering of the $(\lfloor\frac{k}{2}\rfloor-1)$-weighted subgraph $W\left(a_{\lfloor\frac{k+1}{2}\rfloor+2}, a_{\lfloor\frac{k+1}{2}\rfloor+3}, \ldots, a_k, c_{\lfloor\frac{k+1}{2}\rfloor+2}, c_{\lfloor\frac{k+1}{2}\rfloor+3}, \ldots, c_k\right)$. It is obvious that the edges of G_k which are not in $B_{\lfloor\frac{k+1}{2}\rfloor}$ and $W\left(a_{\lfloor\frac{k+1}{2}\rfloor+2}, \ldots, a_k, c_{\lfloor\frac{k+1}{2}\rfloor+2}, \ldots, c_k\right)$ all lie in $M_{\lfloor\frac{k+1}{2}\rfloor+1,k}$. These three subgraphs literally make up the k-weighted graph G_k. We have the following lemma.

Lemma 4.3. *The collection Π_k stated above is a complete multipartite covering of G_k.*

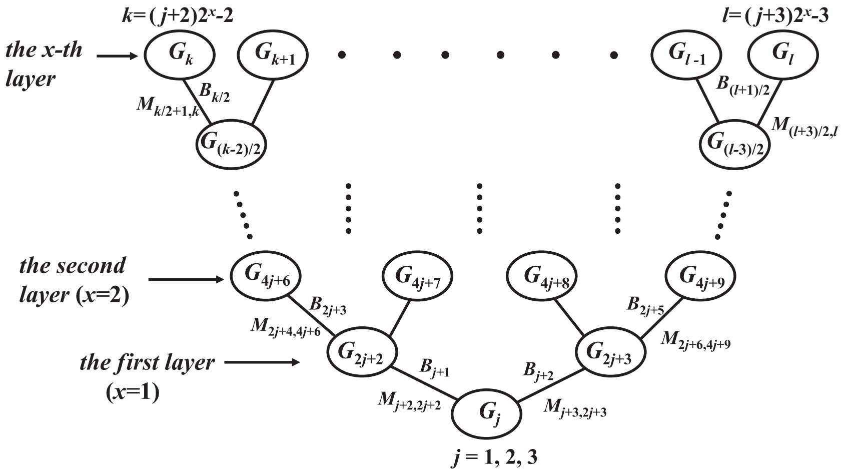

Fig. 4.1. The binary tree for Construction (I).

Our next goal is to find the sum m_k of the orders of all subgraphs in Π_k. Due to the complexity of the enumeration, we consider the reduced forms first. We call $G_k^0 = W(1,\dots,1,1,\dots,1)$ the *reduced form* of a general k-weighted graph $W(a_1,\dots,a_k, c_1,\dots,c_k)$. We also let B_l^0, M_{l_1,l_2}^0 and H_j^0 be the graphs defined in the same ways as B_l, M_{l_1,l_2} and H_j respectively, except that a_i's and c_j's involved are all set to be one. Then G_k^0 and B_k^0 have the complete multipartite covering Π_k^0 and $\Pi_k^{B^0}$ reduced from Π_k and Π_k^B respectively. Note here that G_k^0 has $2k$ vertices. By applying suitable splitting and expanding operations mentioned in Section 4.1 to the reduced form G_k^0 accordingly, one can recover the general k-weighted graph $W(a_1,\dots,a_k,c_1,\dots,c_k)$. For the evaluation of the sum m_k^0 of the orders of all subgraphs in Π_k^0, we introduce a specially designed binary tree.

Note that we have decomposed G_k^0 into $B^0_{\lfloor\frac{k+1}{2}\rfloor}$, $M^0_{\lfloor\frac{k+1}{2}\rfloor+1,k}$ and $G^0_{\lfloor\frac{k}{2}\rfloor-1}$. Since $\lfloor\frac{k+1}{2}\rfloor$ equals $\left(\lfloor\frac{k}{2}\rfloor-1\right)+1$ or $\left(\lfloor\frac{k}{2}\rfloor-1\right)+2, G_j^0$ can either go with B_{j+1}^0 and $M_{j+2,2j+2}^0$ to compose G_{2j+2}^0 or go with B_{j+2}^0 and $M_{j+3,2j+3}^0$ to compose G_{2j+3}^0. Recursively repeating this process, all G_k^0's can be composed from some B_l^0's, $M_{l_1,k}^0$'s and just G_1, G_2 and G_3. We illustrate this relation by means of a binary tree in Fig. 4.1. In this tree, each path from the root represents the conformation of a k-weighted graph of reduced form in our covering. For example, the leftmost path from the root G_j to G_{4j+6} represents that G_{2j+2}^0 is composed of G_j^0, B_{j+1}^0 and $M_{j+2,2j+2}^0$ and then G_{4j+6}^0 is composed of G_{2j+2}^0, B_{2j+3}^0 and $M_{2j+4,4j+6}^0$. Hence the path shows how G_{4j+6}^0 is built up. The 2^x paths of length x from the root give the conformations of the 2^x k-weighted graphs where k ranges from $(j+2)2^x-2$ to $(j+3)2^x-3, j = 1,2,3$.

Theorem 4.4. *Let $\Gamma = \{A \subseteq \mathcal{P} | w(A) \geqslant t\}$ be an access structure represented by a k-weighted graph G_k^0 of reduced form, $k_1 = (j+2)2^x - 2$ and $k_2 = (j+3)2^x - 3$, $x \geqslant 1$, $j = 1, 2, 3$. If $k_1 \leqslant k \leqslant k_2$, then there exists a secret-sharing scheme for the access structure Γ with average information rate $\tilde{\rho}$ with*

$$\frac{24k_2}{k_2^2+60k_2-84\log_2\left(\frac{k_2+2}{j+3}\right)-37-\delta_2^{(j)}} \leqslant \tilde{\rho} \leqslant \frac{24k_1}{k_1^2+58k_1-60\log_2\left(\frac{k_1+2}{j+2}\right)-32-\delta_1^{(j)}}$$

where

$$\left(\delta_1^{(j)},\delta_2^{(j)}\right) = \begin{cases} (0,0), & \text{if } j=1; \\ (28,24), & \text{if } j=2; \\ (40,44), & \text{if } j=3. \end{cases}$$

Proof. Let m_k^0 and $m_l^{B^0}$ be the sum of orders of all subgraphs in Π_k^0 and $\Pi_l^{B^0}$ respectively and $m_{l_1,l_2}^{M^0}$ be the order of M_{l_1,l_2}^0, then $m_{l_1,l_2}^{M^0} = 2l_2 - l_1 + 1$. In $\Pi_l^{B^0}, |V(K(C_i,A_i))| = |V(K_2)| = 2$ and $|V(H_i^0)| = i+1$ for each i. So when l is even, $m_l^{B^0} = \sum_{i=1}^{\frac{l}{2}}\left|V\left(H_{2i}^0\right)\right| + |V(K(C_{2i},A_{2i})| = \sum_{i=1}^{\frac{l}{2}}((2i+1)+2) = \frac{1}{4}(l^2+8l)$. When l is odd, $m_l^{B^0} = \sum_{i=1}^{\frac{l-1}{2}}|V\left(H_{2i+1}^0\right)| + \sum_{i=0}^{\frac{l-1}{2}}|V(K(C_{2i+1},A_{2i+1}))| = \sum_{i=1}^{\frac{l-1}{2}}(2i+2) + \sum_{i=0}^{\frac{l-1}{2}}2 = \frac{1}{4}(l^2+8l-1)$.

(1) First, we consider $G_{k_1}^0$ whose composition process is shown by the leftmost path of length x from the root. Adding up the orders of all subgraphs involved, we have

$$\begin{aligned}
m_{k_1}^0 &= m_j^0 + \sum_{i=1}^{x} m^{B^0}_{(j+2)2^{i-1}-1} + \sum_{i=1}^{x} m^{M^0}_{(j+2)2^{i-1},(j+2)2^i-2} \\
&= \begin{cases} m_j^0 + \frac{1}{4}[(j+1)^2+8(j+1)] \\ +\sum\limits_{i=2}^{x}\frac{1}{4}[((j+2)2^{i-1}-1)^2+8((j+2)2^{i-1}-1)-1] \\ +\sum\limits_{i=1}^{x}[2((j+2)2^i-2)-(j+2)2^{i-1}+1], & \text{if } j=1,3; \\ m_j^0 + \sum\limits_{i=1}^{x}\frac{1}{4}[((j+2)2^{i-1}-1)^2+8((j+2)2^{i-1}-1)-1] \\ +\sum\limits_{i=1}^{x}[2((j+2)2^i-2)-(j+2)2^{i-1}+1], & \text{if } j=2. \end{cases} \\
&= m_j^0 + \tfrac{1}{12}((j+2)2^x)^2 + \tfrac{9}{2}(j+2)2^x - 5x - \varepsilon_1^{(j)} = \tfrac{1}{12}(k_1+2)^2 + \tfrac{9}{2}(k_1+2) - 5\log_2\left(\tfrac{k_1+2}{j+2}\right) - \tilde{\varepsilon}_1^{(j)} \\
&= \tfrac{1}{12}\left[k_1^2 + 58k_1 - 60\log_2\left(\tfrac{k_1+2}{j+2}\right) - 32 - \delta_1^{(j)}\right],
\end{aligned}$$

where $\varepsilon_1^{(j)} = \begin{cases} \frac{j^2+58j+109}{12}, & \text{if } j=1,3; \\ \frac{j^2+58j+112}{12}, & \text{if } j=2. \end{cases}$ and $\left(\tilde{\varepsilon}_1^{(1)},\tilde{\varepsilon}_1^{(2)},\tilde{\varepsilon}_1^{(3)}\right) = (12,\frac{43}{3},\frac{46}{3})$.

In the second last step, we combine the value of $\varepsilon_1^{(j)}$ with $m_1^0 = 2$, $m_2^0 = 5$ and $m_3^0 = 9$ to calculate the value of $\tilde{\varepsilon}_1^{(j)}$. With this covering of $G_{k_1}^0$, we are able to construct a secret-sharing scheme with average information rate $\tilde{\rho}_1 = \frac{2k_1}{m_{k_1}^0}$.

(2) We consider $G^0_{k_2}$ whose composition process is shown by the rightmost path of length x from the root. Similar to (1), we have

$$m^0_{k_2} = m^0_j + \sum_{i=1}^{x} m^{B^0}_{(j+3)2^{i-1}-1} + \sum_{i=1}^{x} m^{M^0}_{(j+3)2^{i-1},(j+3)2^i-3}$$

$$= \begin{cases} m^0_j + \sum_{i=1}^{x} \tfrac{1}{4}[((j+3)2^{i-1}-1)^2 + 8((j+3)2^{i-1}-1) - 1] \\ +\sum_{i=1}^{x}\left[2((j+3)2^i - 3) - (j+3)2^{i-1} + 1\right], \quad \text{if } j = 1,3; \\ m^0_j + \tfrac{1}{4}[(j+2)^2 + 8(j+2)] \\ +\sum_{i=2}^{x} \tfrac{1}{4}\left[((j+3)2^{i-1}-1)^2 + 8((j+3)2^{i-1}-1) - 1\right] \\ +\sum_{i=1}^{x}\left[2((j+3)2^i - 3) - (j+3)2^{i-1} + 1\right], \quad \text{if } j = 2. \end{cases}$$

$$= m^0_j + \tfrac{1}{12}((j+3)2^x)^2 + \tfrac{9}{2}(j+3)2^x - 7x - \varepsilon^{(j)}_2 = \tfrac{1}{12}\left(k_2^2 + 60k_2 - 84\log_2\left(\tfrac{k_2+3}{j+3}\right) - 37 - \delta^{(j)}_2\right),$$

where $\varepsilon^{(j)}_2 = \begin{cases} \frac{j^2+60j+171}{12}, & j = 1,3; \\ \frac{j^2+60j+168}{12}, & j = 2. \end{cases}$.

With this covering of $G^0_{k_2}$, we have constructed a secret-sharing scheme with average information rate $\tilde{\rho}_2 = \frac{2k_0}{m^0_{k_2}}$. The result then follows.

As a matter of fact, each m^0_k can be evaluated in a similar way. The resulting expression only slightly differs from the ones for $m^0_{k_1}$ and $m^0_{k_2}$ at some nonleading coefficients.

After dealing with the reduced forms we shall turn back to the model of general forms. We start with introducing notations. Let $\mathbb{Z}_l = (1\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ \cdots 2\ 1)$, $\mathbb{y}_l = ((\frac{l}{2}+1)\,\frac{l}{2}\,\frac{l}{2}\,(\frac{l}{2}-1)\,(\frac{l}{2}-1)\cdots 2\ 2\ 1)$ and $\mathbb{1}_l = (1\ 1 \cdots 1)$ be three l-dimensional vectors. For $l_1 \leqslant l_2$, let $\mathbb{a}(l_1, l_2) = (a_{l_1} a_{l_1+1} a_{l_1+2} \cdots a_{l_2})$ and $\mathbb{c}(l_1, l_2) = (c_{l_1} c_{l_1+1} c_{l_1+2} \cdots c_{l_2})$ where $a_i = |A_i|$ and $c_i = |C_i|$, $i = l_1, l_1 + 1, \dots, l_2$.

Lemma 4.5. *For $k = 3 \cdot 2^x - 2$ and $x \geqslant 1$,*

$$m_k = \sum_{i=1}^{x-1}\left(\mathbb{Z}_{\frac{k+2}{2^i}} + (i-1)\mathbb{1}_{\frac{k+2}{2^i}}\right) \cdot \mathbb{a}\left(\frac{(k+2)(2^{i-1}-1)}{2^{i-1}} + 1, \frac{(k+2)(2^i-1)}{2^i}\right) + xa_{k-3} + (x+1)a_{k-2} + xa_{k-1}$$
$$+ (x+1)a_k + \sum_{i=1}^{x-1}\left(\mathbb{y}_{\frac{k+2}{2^i}} + (i-1)\mathbb{1}_{\frac{k+2}{2^i}}\right) \cdot \mathbb{c}\left(\frac{(k+2)(2^{i-1}-1)}{2^{i-1}} + 1, \frac{(k+2)(2^i-1)}{2^i}\right)$$
$$+ (x+1)c_{k-3} + (x+1)c_{k-2} + xc_{k-1} + (x+1)c_k.$$

Proof. Recall that the expression for m_k depends on all a_i's and c_i's, each of whose coefficients represents the occurrence of the vertices of that part in the covering Π_k.

(1) First, let us examine the occurrence of vertices of B_l, whose partite sets are $\bigcup_{i=1}^{l} A_i$ and $\bigcup_{i=1}^{l} C_i$, in its covering Π^B_l. For odd l, by Lemma 4.2, one can easily see that the vertices in A_1 have occurrence 1 (only in $K(A_1, C_1)$), the vertices in A_{2j}, $j = 1, \dots, \frac{l-1}{2}$, also have occurrence 1 (only in H_{2j+1}) and the vertices in A_{2j+1}, $j = 1, \dots, \frac{l-1}{2}$, have occurrence 2 (in H_{2j+1} and $K(A_{2j+1},C_{2j+1})$). Hence, the occurrences of the vertices in $A_1, A_2, \dots, A_l$ are exactly the first l coordinates in $\mathbb{Z}_{l+1}$. Similarly, the vertices in C_1 have occurrence $\frac{l+1}{2}$ (in $K(A_1,C_1)$ and H_{2i+1}'s, $i = 1, \dots, \frac{l-1}{2}$), the vertices in C_{2j}, $j = 1, \dots, \frac{l-1}{2}$, have occurrence $\frac{l-1}{2} - j + 1$ (in H_{2i+1}'s, $i \geqslant j$) and the vertices in C_{2j+1}, $j = 1, \dots, \frac{l-1}{2}$, have occurrence $\frac{l-1}{2} - j + 1$ (in H_{2i+1}'s, $i \geqslant j + 1$ and $K(A_{2j+1}, C_{2j+1})$). Hence, the occurrences of the vertices in $C_1, C_2, \dots, C_l$ are exactly the first l coordinates in $\mathbb{y}_{l+1} - \mathbb{1}_{l+1}$.

(2) Let us consider the value of m_k now. We prove the result by induction on x. When $x = 1$, $m_4 = a_1 + 2a_2 + a_3 + 2\text{-}_4 = a_1 + 2a_2 + a_3 + 2a_4 + 2c_1 + 2c_2 + c_3 + 2c_4$ by direct counting the occurrences of vertices in Π_4. So, the result holds when $x = 1$. Next, for $k = 3 \cdot 2^{x+1} - 2$,$G_k = W(a_1, \dots, a_k, c_1, \dots, c_k)$ is composed of $B_{3\cdot2^x-1}$, $M_{3\cdot2^x,3\cdot2^{x+1}-2}$ and $G_{3\cdot2^x-2}$. For convenience, denote $M_{3\cdot2^x,3\cdot2^{x+1}-2}$ by M for now. Observe that the vertices in A_i, $1 \leqslant i \leqslant 3 \cdot 2^x - 1$ have the same occurrences in Π_k as they do in the covering $\Pi^B_{3\cdot2^x-1}$ because they do not lie in M and $G_{3\cdot2^x-2}$, while the vertices in C_i, $1 \leqslant i \leqslant 3 \cdot 2^x - 1$, gain one more occurrences in Π_k than they do in $\Pi^B_{3\cdot2^x-1}$ because they also occur in M.

Notice that the vertices in $A_{3\cdot 2^x}$ and $C_{3\cdot 2^x}$ only occur once in Π_k. Besides, the vertices in A_i's and C_i's, $i = 3 \cdot 2^x + 1, - \ldots, k$, also gain one more occurrence in Π_k than they do in the covering $\Pi_{3\cdot 2^x-2}$ of $G_{3\cdot 2^x-2}$. Therefore, by (1) and the induction hypothesis,

$$
\begin{aligned}
&m_{3\cdot 2^{x+1}-2}\\
&= \mathbb{Z}_{3\cdot 2^x} \cdot \mathbb{a}(1, 3\cdot 2^x) + (\mathbb{y}_{3\cdot 2^x} - \mathbb{1}_{3\cdot 2^x}) \cdot \mathbb{c}(1, 3\cdot 2^x) + \mathbb{1}_{3\cdot 2^x} \cdot \mathbb{c}(1, 3\cdot 2^x)\\
&+ \sum_{i=1}^{x-1}\left(\mathbb{Z}_{\frac{3\cdot 2^x}{2^i}} + (i-1)\mathbb{1}_{\frac{3\cdot 2^x}{2^i}} + \mathbb{1}_{\frac{3\cdot 2^x}{2^i}}\right) \cdot \mathbb{a}\left(\frac{3\cdot 2^x(2^{i-1}-1)}{2^{i-1}} + 1 + 3\cdot 2^x, \frac{3\cdot 2^x(2^i-1)}{2^i} + 3\cdot 2^x\right)\\
&+ (x+1)a_{3\cdot 2^x-5+3\cdot 2^x} + (x+2)a_{3\cdot 2^x-4+3\cdot 2^x} + (x+1)a_{3\cdot 2^x-3+3\cdot 2^x} + (x+2)a_{3\cdot 2^x-2+3\cdot 2^x}\\
&+ \sum_{i=1}^{x-1}\left(\mathbb{y}_{\frac{3\cdot 2^x}{2^i}} + (i-1)\mathbb{1}_{\frac{3\cdot 2^x}{2^i}} + \mathbb{1}_{\frac{3\cdot 2^x}{2^i}}\right) \cdot \mathbb{c}\left(\frac{3\cdot 2^x(2^{i-1}-1)}{2^{i-1}} + 1 + 3\cdot 2^x, \frac{3\cdot 2^x(2^i-1)}{2^i} + 3\cdot 2^x\right)\\
&+ (x+2)c_{3\cdot 2^x-5+3\cdot 2^x} + (x+2)c_{3\cdot 2^x-4+3\cdot 2^x} + (x+1)c_{3\cdot 2^x-3+3\cdot 2^x} + (x+2)c_{3\cdot 2^x-2+3\cdot 2^x}\\
&= \mathbb{Z}_{\frac{3\cdot 2^{x+1}}{2}} \cdot \mathbb{a}\left(1, \frac{3\cdot 2^{x+1}}{2}\right) + \mathbb{y}_{\frac{3\cdot 2^{x+1}}{2}} \cdot \mathbb{c}\left(1, \frac{3\cdot 2^{x+1}}{2}\right)\\
&+ \sum_{i=1}^{x-1}\left(\mathbb{Z}_{\frac{3\cdot 2^{x+1}}{2^{i+1}}} + ((i+1)-1)\mathbb{1}_{\frac{3\cdot 2^{x+1}}{2^{i+1}}}\right) \cdot \mathbb{a}\left(\frac{3\cdot 2^{x+1}(2^i-1)}{2^i} + 1, \frac{3\cdot 2^{x+1}(2^{i+1}-1)}{2^{i+1}}\right)\\
&+ (x+1)a_{(3\cdot 2^{x+1}-2)-3} + (x+2)a_{(3\cdot 2^{x+1}-2)-2} + (x+1)a_{(3\cdot 2^{x+1}-2)1} + (x+2)a_{(3\cdot 2^{x+1}-2)}\\
&+ \sum_{i=1}^{x-1}\left(\mathbb{y}_{\frac{3\cdot 2^{x+1}}{2^{i+1}}} + ((i+1)-1)\mathbb{1}_{\frac{3\cdot 2^{x+1}}{2^{i+1}}}\right) \cdot \mathbb{c}\left(\frac{3\cdot 2^{x+1}(2^i-1)}{2^i} + 1, \frac{3\cdot 2^{x+1}(2^{i+1}-1)}{2^{i+1}}\right)\\
&+ (x+2)c_{(3\cdot 2^{x+1}-2)-3} + (x+2)c_{(3\cdot 2^{x+1}-2)-2} + (x+1)c_{(3\cdot 2^{x+1}-2)1} + (x+2)c_{(3\cdot 2^{x+1}-2)}\\
&= \sum_{i=1}^{x}\left(\mathbb{Z}_{\frac{k+2}{2^i}} + (i-1)\mathbb{1}_{\frac{k+2}{2^i}}\right) \cdot \mathbb{a}\left(\frac{(k+2)(2^{i-1}-1)}{2^{i-1}} + 1, \frac{(k+2)(2^i-1)}{2^i}\right)\\
&+ (x+1)a_{k-3} + (x+2)a_{k-2} + (x+1)a_{k-1} + (x+2)a_k\\
&+ \sum_{i=1}^{x}\left(\mathbb{y}_{\frac{k+2}{2^i}} + (i-1)\mathbb{1}_{\frac{k+2}{2^i}}\right) \cdot \mathbb{c}\left(\frac{(k+2)(2^{i-1}-1)}{2^{i-1}} + 1, \frac{(k+2)(2^i-1)}{2^i}\right)\\
&+ (x+2)c_{k-3} + (x+2)c_{k-2} + (x+1)c_{k-1} + (x+2)c_k. \quad \square
\end{aligned}
$$

This lemma presents a sophisticated expression for m_k in terms of a_i's and c_i's. In what follows, we give the conditions on the values of a_i's and c_i's under which m_k attains its minimum value when $n = \sum_{i=1}^{k}(a_i + c_i)$ is fixed. Thereby, the highest possible average information rate via this covering is obtained.

Theorem 4.6. *Let Γ be a weighted threshold access structure represented by a k-weighted graph $G = W(a_1, \ldots, a_k, c_1, \ldots, c_k)$ of order n and $k = 3 \cdot 2^x - 2$. If $c_i = 1$ for all $i \neq \frac{k}{2} + 1$ and $a_i = 1$ for all $i \notin T = \{1, 2, 4, 6, \ldots, \frac{k}{2} + 1\}$. Then*

$$
\tilde{\rho}^*(G) \geqslant \frac{12n}{12n + k^2 + 34k - 60\log_2(\frac{k+2}{3}) - 32}.
$$

Proof. Observe that only $c_{\frac{k}{2}+1}$ and a_i, $i \in T$, have coefficient equal to one in the expression for m_k in Lemma 4.5. So m_k is minimized if $c_i = 1$ for all $i \neq \frac{k}{2} + 1$ and $a_i = 1$ for all $i \notin T$ since this expression for m_k is linear. This case is similar to the reduced form. So, we make an adjustment in the expression for $m^0_{k_1}$ (with $j = 1$) in the proof of Theorem 4.4 to derive what we need here. The sum m_k of orders of subgraphs in this covering is $m^0_{k_1} + \sum_{i\in T} a_i + c_{\frac{k}{2}+1} - (|T| + 1)$. Note that $n = \sum_{i=1}^{k}(a_i + c_i) = \sum_{i\in T} a_i + c_{\frac{k}{2}+1} + \sum_{i\notin T} a_i + \sum_{i\neq\frac{k}{2}+1} c_i = \sum_{i\in T} a_i + c_{\frac{k}{2}+1} + (k - |T|) + (k - 1) = \sum_{i\in T} a_i + c_{\frac{k}{2}+1} + 2k - (|T| + 1)$. Therefore, in this case $m_k = \frac{1}{12}\left[k^2 + 58k - 60\log_2(\frac{k+2}{3}) - 32\right] + n - 2k = \frac{1}{12}\left[12n + k^2 + 34k - 60\log_2(\frac{k+2}{3}) - 32\right]$. The average information rate of the secret-sharing scheme constructed with this covering attains its maximum value $\frac{n}{m_k}$ and the proof is completed. □

Our result appears to be quite good if k is relatively small compared with n. In fact, as k fixed, the rate given in Theorem 4.6 asymptotically approaches "1" which is the optimal value for the rate.

5. Construction (II)

Our second construction is similar to the first, while it performs better than Construction I when $k \geqslant 31$. The major difference is that B_l is replaced with G_l in the covering. With the notations used before, we define our second covering $\widetilde{\Pi}_k$ of

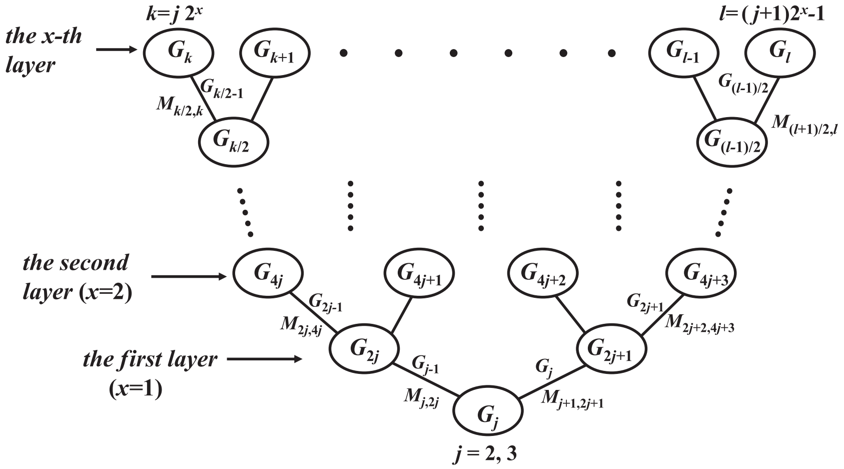

Fig. 5.1. The binary tree for Construction (II).

$G_k = W(a_1, \ldots, a_k, c_1, \ldots, c_k)$ recursively as follows. $\widetilde{\Pi}_i = \Pi_i, i = 1, 2, 3$. For $k \geqslant 4$, $\widetilde{\Pi}_k = \widetilde{\Pi}_{\lfloor\frac{k-1}{2}\rfloor} \cup \left\{M_{\lfloor\frac{k-1}{2}\rfloor+1,k}\right\} \cup \widetilde{\Pi}_{\lfloor\frac{k}{2}\rfloor}$ where the $\widetilde{\Pi}_{\lfloor\frac{k}{2}\rfloor}$ is the complete multipartite covering of the $\lfloor\frac{k}{2}\rfloor$-weighted subgraph $\underline{W} = W\left(a_{\lfloor\frac{k-1}{2}\rfloor+2}, a_{\lfloor\frac{k-1}{2}\rfloor+3}, \ldots, a_k, c_{\lfloor\frac{k-1}{2}\rfloor+2}, c_{\lfloor\frac{k-1}{2}\rfloor+3}, \ldots, c_k\right)$. It is obvious that the edges not in the subgraphs $W\left(a_1, \ldots, a_{\lfloor\frac{k-1}{2}\rfloor}, c_1, \ldots, c_{\lfloor\frac{k-1}{2}\rfloor}\right)$ and $\underline{W}$ all lie in $M_{\lfloor\frac{k-1}{2}\rfloor+1,k}$. So, $\widetilde{\Pi}_k$ is a complete multipartite covering of G_k.

Lemma 5.1. *The collection $\widetilde{\Pi}_k$ is a complete multipartite covering of G_k.*

In order to evaluate the sum $\tilde{m}_k$ of the orders of all subgraphs in $\widetilde{\Pi}_k$, we consider the reduced form first. Let $\widetilde{\Pi}_k^0$ and $\tilde{m}_k^0$ be the reduced version of $\widetilde{\Pi}_k$ and $\tilde{m}_k$ respectively. In the covering $\widetilde{\Pi}_k^0$, we decompose G_k^0 into $G^0_{\lfloor\frac{k-1}{2}\rfloor}$, $M^0_{\lfloor\frac{k-1}{2}\rfloor+1,k}$ and $G^0_{\lfloor\frac{k}{2}\rfloor}$. Since $\lfloor\frac{k-1}{2}\rfloor$ equals $\lfloor\frac{k}{2}\rfloor - 1$ or $\lfloor\frac{k}{2}\rfloor, G_j^0$ can either go with G_{j-1}^0 and $M_{j,2j}^0$ to compose G_{2j}^0 or go with G_j^0 and $M^0_{j+1,2j+1}$ to compose G^0_{2j+1}. Recursively, all G_k^0's can be obtained by using this process repeatly from G_1, G_2, G_3 and some $M^0_{i,k}$'s. As we have done in Section 4, this relation is depicted by a binary tree in Fig. 5.1. The 2^x paths of length x from the root give the conformations of 2^x k-weight graphs where $2^{x+1} \leqslant k \leqslant 3 \cdot 2^x - 1$ or $3 \cdot 2^x \leqslant k \leqslant 2^{x+2} - 1$.

Theorem 5.2. *Let Γ be an weighted threshold access structure represented by a k-weighted graph G_k^0 of reduced form, $k_1 = j \cdot 2^x$ and $k_2 = (j + 1) \cdot 2^x - 1$, $x \geqslant 0$, $j = 2, 3$. If $k_1 \leqslant k \leqslant k_2$, then there exists a secret-sharing scheme for the access structure Γ with average information rate $\tilde{\rho}$ with*

$$\frac{2k_2}{\frac{3}{2}(k_2+1)\log_2(k_2+1) + \delta^{(j)}(k_2+1) + 1} \leqslant \tilde{\rho} \leqslant \frac{2k_1}{(\frac{3}{2}k_1 + 2)\log_2 k_1 + \delta_1^{(j)}k_1 + \delta_0^{(j)}}$$

where

$$\left(\delta^{(j)}, \delta_1^{(j)}, \delta_0^{(j)}\right) = \begin{cases} \left(\frac{4}{3} - \frac{3}{2}\log_2 3, -1, 2\right), & \text{if } j = 2; \\ \left(-1, \frac{4}{3} - \frac{3}{2}\log_2 3, 5 - 2\log_2 3\right), & \text{if } j = 3. \end{cases}$$

Proof. Recall that $M^0_{l_1,l_2}$ has order $m_{l_1,l_2}^{M^0} = 2l_2 - l_1 + 1$, $\tilde{m}_i^0 = m_i^0$, $i = 1,\ 2,\ 3$. $m_1^0 = 2$, $m_2^0 = 5$, and $m_3^0 = 9$.

(1) First, we consider $G^0_{k_2}$. For each $l = 2^i(j + 1) - 1$, G_l is composed of two $G_{\frac{l-1}{2}}$'s and one $M_{\frac{l+1}{2},l}$. So $\tilde{m}_k^0$ can be evaluated recursively as follows.

$$\begin{aligned} \tilde{m}^0_{k_2} &= 2\tilde{m}^0_{2^{x-1}(j+1)-1} + 3 \cdot 2^{x-1}(j+1) - 1 = 2^x m_j^0 + \sum_{i=1}^{x}(2^{i-1}(3 \cdot 2^{x-i}(j+1) - 1)) = 2^x \cdot m_j^0 + 3x \cdot 2^{x-1}(j+1) - (2^x - 1) \\ &= 3 \cdot \frac{k_2+1}{2}\log_2\left(\frac{k_2+1}{j+1}\right) + \frac{m_j^0 - 1}{j+1} \cdot (k_2+1) + 1 = \frac{3}{2}(k_2+1)\log_2(k_2+1) + \left(\frac{m_j^0 - 1}{j+1} - \frac{3}{2}\log_2(j+1)\right)(k_2+1) + 1 \\ &= \frac{3}{2}(k_2+1)\log_2(k_2+1) + \delta^{(j)}(k_2+1) + 1. \end{aligned}$$

Hence, the secret-sharing scheme constructed with $\widetilde{\Pi}^0_{k_2}$ has average information rate $\tilde{\rho}_2 = \frac{2k_2}{\tilde{m}^0_{k_2}}$.

(2) The composition process of $G^0_{k_1}$ is shown on the leftmost path of length x from the root. Adding up the orders of all subgraphs involved, we have $\tilde{m}^0_{k_1} = \tilde{m}^0_j + \tilde{m}^0_{j-1} + \sum_{i=1}^{x-1} \tilde{m}^0_{2^i \cdot j-1} + \sum_{i=1}^{x} m^{M^0}_{2^{i-1} j, 2^i j}$. Making use of the equation $\tilde{m}^0_{2^x(j+1)-1} = 2^x \cdot m^0_j + 3x \cdot 2^{x-1}(j+1) - (2^x - 1)$ from the derivation in (1), we can continue to evaluate $\tilde{m}^0_{k_1}$ according to the value of j as follows.

(i) If $j = 3$,

$$\begin{aligned}\tilde{m}^0_{3 \cdot 2^x} &= m^0_j + m^0_{j-1} + um_{i=1}^{x-1}[2^i \cdot m^0_{j-1} + 3 \cdot i \cdot 2^{i-1} \cdot j - (2^i - 1)] + \sum_{i=1}^{x}(3 \cdot 2^{i-1} \cdot j + 1) \\ &= m^0_3 + m^0_2 + m^0_2(2^x - 2) + 9((x-2)2^{x-1} + 1) - (2^x - 1 - x) + 9(2^x - 1) + x = 9x2^{x-1} + 4 \cdot 2^x + 2x + 5 \\ &= \frac{3k}{2}\log_2 k_1 + \left(\frac{4}{3} - \frac{3}{2}\log_2 3\right)k_1 + 2\log_2 k_1 + (5 - 2\log_2 3).\end{aligned}$$

(ii) If $j = 2$,

$$\begin{aligned}\tilde{m}^0_{2^{x+1}} &= m^0_j + m^0_{j-1} + \sum_{i=1}^{x-1}\left[2^{i-1} m^0_3 + 3(i-1)2^{i-2} \cdot 4 - (2^{i-1} - 1)\right] + \sum_{i=1}^{x}(3 \cdot 2^{i-1} \cdot j + 1) = 3x \cdot 2^x + 2^x + 2x + 4 \\ &= \frac{3}{2}k_1 \log_2 k_1 - k_1 + 2\log_2 k_1 + 2.\end{aligned}$$

Hence $\tilde{m}^0_{k_1} = (\frac{3}{2}k_1 + 2)\log_2 k_1 + \delta^{(j)}_1 k_1 + \delta^{(j)}_0$ and we have a secret-sharing scheme with average information rate $\tilde{\rho}_1 = \frac{2k_1}{\tilde{m}^0_{k_1}}$. The result follows immediately. □

Next, we give the expression for $\tilde{m}_k$ for a k-weighted graph of general form.

Lemma 5.3. *Let $k = 2^x \cdot (j + 1) - 1$, $x \geqslant 0$, $j = 2, 3$. If $\tilde{m}_k = \sum_{i=1}^{k} \alpha^x_{j,i} a_i + \sum_{i=1}^{k} \beta^x_{j,i} c_i$ is the sum of the orders of all subgraphs in the covering $\widetilde{\Pi}_k$ of a k-weighted graph $G_k = W(a_1, \ldots, a_k, c_1, \ldots, c_k)$. Then the values of $\alpha^x_{j,i}$'s and $\beta^x_{j,i}$'s can be obtained by the recursive relations $\alpha^x_{j,i} = \alpha^x_{j,\frac{k+1}{2}+i} - 1 = \alpha^{x-1}_{j,i}$, $\beta^x_{j,i} = \beta^x_{j,\frac{k+1}{2}+i} = \beta^{x-1}_{j,i} + 1$ and $\alpha^x_{j,\frac{k+1}{2}} = \beta^x_{j,\frac{k+1}{2}} = 1$, $1 \leqslant i \leqslant \frac{k-1}{2}$, with initial values $\alpha^0_{j,1} = \alpha^0_{j,2} = \beta^0_{j,2} = 1$ and $\beta^0_{j,1} = \alpha^0_{3,3} = \beta^0_{3,3} = 2$.*

Proof. We prove this result by induction on x. When $x = 0$, $k = j$, the occurrences of the vertices in A_i's and C_i's in $\widetilde{\Pi}_j$ are exactly the initial values $\alpha^0_{j,i}$'s and $\beta^0_{j,i}$'s respectively. For $x > 0$, recall that G_k is composed of $W_1 = W(a_1, \ldots, a_{2^{x-1}(j+1)-1}, c_1, \ldots, c_{2^{x-1}(j+1)-1})$, $W_2 = W(a_{2^{x-1}(j+1)+1}, \ldots, a_k, c_{2^{x-1}(j+1)+1}, \ldots, c_k)$ and $M = M_{2^{x-1}(j+1), 2^x(j+1)-1}$. Each vertex in $A_i, 1 \leqslant i \leqslant \frac{k-1}{2} = 2^{x-1}(j+1) - 1$, has the same occurrence in $\widetilde{\Pi}_k$ as it does in the covering of W_1 since it does not occur in either W_2 or M. So, $\alpha^x_{j,i} = \alpha^{x-1}_{j,i}$. However, each vertex in $C_i, 1 \leqslant i \leqslant \frac{k-1}{2}$, gains one more occurrence in $\widetilde{\Pi}_k$ than it does in the covering of W_1 because it also occurs in M. This is also true for vertices in A_i and $C_i, \frac{k+1}{2} = 2^{x-1}(j+1) + 1 \leqslant i \leqslant k$, because all of them occur in graph M. Hence, we also have $\beta^x_{j,i} = \beta^{x-1}_{j,i} + 1, \alpha^x_{j,\frac{k+1}{2}+i} = \alpha^{x-1}_{j,i} + 1$ and $\beta^x_{j,\frac{k+1}{2}+i} = \beta^{x-1}_{j,i} + 1$ for $1 \leqslant i \leqslant \frac{k-1}{2}$. Besides, the vertices in $A_{\frac{k+1}{2}}$ and $C_{\frac{k+1}{2}}$ have occurrence one because they only appear in M. Hence, $\alpha^x_{j,\frac{k+1}{2}} = \beta^x_{j,\frac{k+1}{2}} = 1$. This proves that the coefficients $\alpha^x_{j,i}$'s and $\beta^x_{j,i}$'s satisfy the given recursive relations. □

Now, we consider the case when $n = \sum_{i=1}^{k}(a_i + c_i)$ is fixed. By evaluating the minimum value of $\tilde{m}_k$, we obtain the highest possible average information rate of a secret-sharing scheme constructed with this covering.

Theorem 5.4. *Let Γ be a weighted threshold access structure represented by a k-weighted graph $G = W(a_1, \ldots, a_k, c_1, \ldots, c_k)$ of order n and $k = (j + 1)2^x - 1$. If $c_i = 1$ for all $i \neq \frac{k+1}{2}$ and $a_i = 1$ for all $i \notin T = \{1,2\} \cup \{(j + 1)2^i - i = 0, 1, \ldots, x - 1\}$. Then*

$$\tilde{\rho}^*(G) \geqslant \frac{n}{n + \frac{3}{2}(k+1)\log_2(k+1) + (\delta^{(j)} - 2)k + (\delta^{(j)} + 1)}$$

where $\delta^{(j)}$ is given in Theorem 5.2.

Proof. The argument is similar to the proof of Theorem 4.6. From the relations given in Lemma 5.3, among all the coefficients of a_i's and c_i's, only $\alpha^x_{j,i}$, $i \in T$, and $\beta^x_{j,\frac{k+1}{2}}$ are equal to one. So $\tilde{m}_k$ is minimized if $a_i = 1$ for all $i \notin T$ and $c_i = 1$ for all $i \neq \frac{k+1}{2}$. We modify the expression for $\tilde{m}^0_{k_2}$ in the proof of Theorem 5.2 to meet what we need here. In this case, $\tilde{m}_k = \tilde{m}^0_{k_2} + \sum_{i \in T} a_i + c_{\frac{k+1}{2}} - (|T| + 1) = \tilde{m}^0_k + n - 2k = n + \frac{3}{2}(k+1)\log_2(k+1) + (\delta^{(j)} - 2)k + (\delta^{(j)} + 1)$. The secret-sharing scheme for this access structure has average information rate $\frac{n}{\tilde{m}_k}$. □

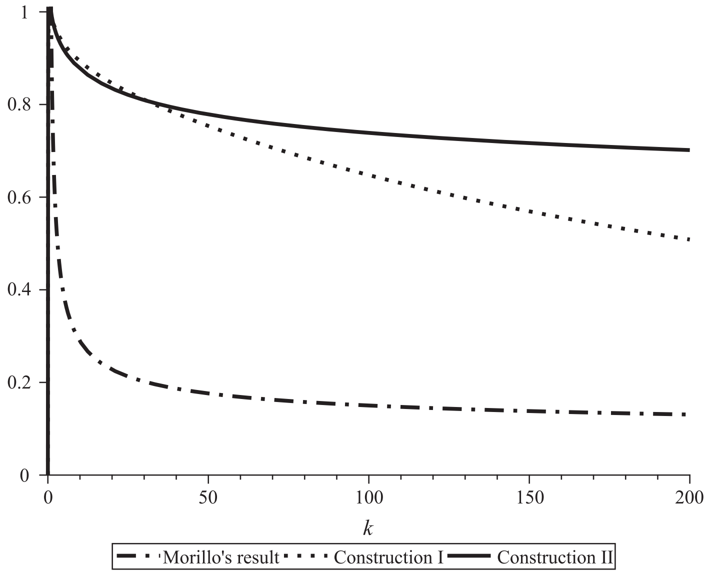

Fig. 6.1. A comparison of the results in the case when $\mu = 20$.

This result is also very good when k is relatively small compared with n. The rate also approaches "1" asymptotically as k fixed. After analyzing the average information rates produced from each of our constructions separately, we shall give a comparison of them in Section 6. For a fair comparison, we consider the same class of k-weighted graphs where $k = 3 \cdot 2^x - 2$. We present the highest possible average information rate for this class as follows.

Theorem 5.5. *Let Γ be a weighted threshold access structure represented by a k-weighted graph $G_k = W(a_1, \ldots, a_k, c_1, \ldots, c_k)$ of order n and $k = 3 \cdot 2^x - 2$. If $c_i = 1$ for all $i \neq \frac{k}{2}$ and $a_i = 1$ for all $i \notin T = \{1\} \cup \{3 \cdot 2^i - 1 | \ i = 0, 1, \ldots, x - 1\}$. Then*

$$\tilde{\rho}^*(G_k) \geqslant \frac{n}{n + \left(\frac{3}{2}k + 2\right)\log_2(k+2) - \left(\frac{2}{3} + \frac{3}{2}\log_2 3\right)k + \frac{2}{3} - 2\log_2 3}.$$

Proof. Suppose $\left(\bigcup_{i=1}^k A_i\right) \cup \left(\bigcup_{i=1}^k C_i\right)$ is the vertex set of G_k where $|A_i| = a_i$ and $|C_i| = c_i$, $i = 1, 2, \ldots, k$. Denote $\{u\}$ by A_0 and $\{v\}$ by C_0. Let $\left(\bigcup_{i=0}^k A_i\right) \cup \left(\bigcup_{i=0}^k C_i\right)$ be the vertex set of the $(k+1)$-weighted graph $G_{k+1} = W(|A_0|, a_1, \ldots, a_k, |C_0|, c_1, \ldots, c_k)$ of order $n + 2$ where $k + 1 = 3 \cdot 2^x - 1$. Then G_{k+1} satisfies the criteria in Theorem 5.4, and the sum $\tilde{m}_{k+1}$ of the orders of all subgraphs in its covering $\widetilde{\Pi}_{k+1}$ is $n + 2 + \frac{3}{2}(k+2)\log_2(k+2) + (\delta^{(2)} - 2)(k+1) + \delta^{(2)} + 1$. Now, observe that $G_k = G_{k+1} - (A_0 \cup C_0)$ and the collection of subgraphs obtained from $\widetilde{\Pi}_{k+1}$ by deleting u and v from each subgraphs in $\widetilde{\Pi}_{k+1}$ is exactly the complete multipartite covering $\widetilde{\Pi}_k$ of G_k since G_{k+1} is composed of $W\left(|A_0|, a_1, \ldots, a_{\frac{k}{2}-1}, |C_0|, c_1, \ldots, c_{\frac{k}{2}-1}\right), M_{\frac{k}{2}+1,k+1}$ (in G_{k+1}) and $W\left(a_{\frac{k}{2}+1}, \ldots, a_k, c_{\frac{k}{2}+1}, \ldots, c_k\right)$ and G_k is composed of$W\left(a_1, \ldots, a_{\frac{k}{2}-1}, c_1, \ldots, c_{\frac{k}{2}-1}\right), M_{\frac{k}{2},k}$ (in G_k) and $W\left(a_{\frac{k}{2}+1}, \ldots, a_k, c_{\frac{k}{2}+1}, \ldots, c_k\right)$. From the relations in Lemma 5.3, one can see that the occurrence of u in $\widetilde{\Pi}_{k+1}$ is one and the occurrence of v in $\widetilde{\Pi}_{k+1}$ is $\beta_{2,1}^x = x + 2 = \log_2\left(\frac{k+2}{3}\right) + 2$. Hence, the sum $\tilde{m}_k$ of the orders of all subgraphs in $\widetilde{\Pi}_k$ is $\tilde{m}_{k+1} - 1 - \left(\log_2\left(\frac{k+2}{3}\right) + 2\right) = n + \left(\frac{3}{2}k + 2\right)\log_2(k+2) - \left(\frac{2}{3} + \frac{3}{2}\log_2 3\right)k + \frac{2}{3} - 2\log_2 3$. The result is then obtained. □

6. Conclusion

The weighted threshold access structure is a more applicable structure of secret-sharing schemes in reality. In the implementation of such a scheme, the value of k represents the number of departments or divisions in an organization. Let $\tilde{\rho}_1 = \frac{12n}{12n + k^2 + 34k - 60\log_2\left(\frac{k+2}{3}\right) - 32}$ and $\tilde{\rho}_2 = \frac{n}{n + \left(\frac{3}{2}k+2\right)\log_2(k+2) - \left(\frac{2}{3} + \frac{3}{2}\log_2 3\right)k + \frac{2}{3} - 2\log_2 3}$ be the highest possible average information rate derived from our two constructions in Theorems 4.6 and 5.5, respectively. Both rates perform very well when n/k is large. If k is constant, both rates approaches "1" asymptotically. Let $n = \mu k$ where μ represents the average size of departments in the organization. When μ is larger, both $\tilde{\rho}_1$ and $\tilde{\rho}_2$ become higher as well for each value of k. Fig. 6.1 shows the behavior of Morillo's rate [19], $\tilde{\rho}_1$ and $\tilde{\rho}_2$ in the case when $\mu = 20$. As indicated in the figure, $\tilde{\rho}_1$ performs better than $\tilde{\rho}_2$ when $k \leqslant 30$, whereas $\tilde{\rho}_2$ becomes superior to $\tilde{\rho}_1$ for all $k \geqslant 31$. Actually, this fact remains true for all values of μ. Therefore, Construction I is more suitable for organizations with fewer departments, whereas Construction II performs especially well for organizations with more departments.

Dealing with average information rate is in general very tedious. In this work, we have demonstrated an approach to the analysis of complicated results.

References

[1] A. Beimel, Secret-sharing schemes: a survey, in: Proceedings of the 3rd International Workshop on Coding and Cryptology, Lecture Notes in Computer Science, vol. 6639, 2011, pp. 11–46.

[2] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies Proceedings, vol. 48, 1979, pp. 313–317.

[3] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro, Tight bounds on the information rate of secret-sharing schemes, Designs, Codes and Cryptography 11 (1997) 107–122.

[4] C. Blundo, A. De Santis, A. Giorgio Gaggian, U. Vaccaro, New bounds on the information rate of secret-sharing schemes, IEEE Transactions on Information Theory 41 (1995) 549–554.

[5] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro, Graph decompositions and secret-sharing schemes, Journal of Cryptology 8 (1995) 39–64.

[6] E.F. Brickell, D.M. Davenport, On the classification of ideal secret-sharing schemes, Journal of Cryptology 4 (1991) 123–134.

[7] E.F. Brickell, D.R. Stinson, Some improved bounds on the information rate of perfect secret-sharing schemes, Journal of Cryptology 5 (1992) 153–166.

[8] C.-C. Chang, Y.-H. Chen, H.-C. Wang, Meaningful secret sharing technique with authentication and remedy abilities, Information Sciences 181 (2011) 3073–3084.

[9] L. Csirmaz, An impossibiliuty result on graph secret sharing, Designs, Codes and Cryptography 53 (2009) 195–209.

[10] L. Csirmaz, G. Tardos, Exact Bounds on Tree based Secret Sharing Schemes, Tatracrypt, Slovakia, 2007.

[11] M.H. Dehkordi, S. Mashhadi, New efficient and practical multi-secret sharing shemes, Information Sciences 178 (2008) 2262–2274.

[12] M. van Dijk, On the information rate of perfect secret-sharing schemes, Designs, Codes and Cryptography 6 (1995) 143–169.

[13] L. Harn, C. Lin, Strong (n,t,n) verifiable secret sharing sheme, Information Sciences 180 (2010) 3059–3064.

[14] C.-F. Hsu, Q. Cheng, X. Tang, B. Zeng, An ideal multi-secret sharing scheme based on MSP, Information Sciences 181 (2011) 1403–1409.

[15] W.-A. Jackson, K.M. Martin, Perfect secret-sharing schemes on five participants, Designs, Codes and Cryptography 9 (1996) 267–286.

[16] K. Kaya, A.A. Selcuk, Threshold cryptography based on Asmuth–Bloom secret sharing, Information Sciences 177 (2007) 4148–4160.

[17] C.Y. Lee, Y-S Yeh, D-J Chen, K-L Ku, A probability model for reconstructing secret sharing under the internet environment, Information Sciences 166 (1999) 109–127.

[18] H.-C. Lu, H.-L. Fu, The exact values of the optimal average information ratio of perfect secret-sharing schemes for tree-based access structure, Designs, Codes and Cryptography (2013), http://dx.doi.org/10.1007/s10623-012-9792-1.

[19] P. Morillo, C. Padro, G. Saez, J.L. Villar, Weighted threshold secret-sharing schemes, Information Processing Letters 704 (1999) 211–216.

[20] C. Padro, G. Saez, Secret sharing schemes with bipartite access structure, IEEE Transactions on Information Theory 46 (7) (2000) 2596–2604.

[21] A. Parakh, S. Kak, Space efficient secret sharing for implicit data security, Information Sciences 181 (2011) 335–341.

[22] A. Shamir, How to share a secret, Communications of the ACM 22 (1979) 612–613.

[23] S.J. Shyu, K. Chen, Visual multiple secret sharing based upon turning and flipping, Information Sciences 181 (2011) 3246–3266.

[24] D.R. Stinson, An explication of secret-sharing schemes, Designs, Codes and Cryptography 2 (1992) 357–390.

[25] D.R. Stinson, New general lower bounds on the information rate of perfect secret-sharing schemes, in: E.F. Brickell, (Ed.), Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science vol. 740, 1993, 168–182.

[26] D.R. Stinson, Decomposition constructions for secret-sharing schemes, IEEE Transactions on Information Theory 40 (1994) 118–125.

[27] D. Wang, F. Yi, X. Li, Probabilistic visual secret sharing schemes for grey-scale images and color images, Information Sciences 181 (2011) 2189–2208.