# Optimal Multiple Assignments with $(m,m)$-Scheme for General Access Structures

Qiang Li*, Xiangxue Li†, Dong Zheng*, and Kefei Chen‡
*School of Information Security Engineering Shanghai Jiaotong University, P.R.China
†Department of Computer Science and Technology, East China Normal University, P.R.China
‡Department of Computer Science and Engineering, Shanghai Jiaotong University, P.R.China
Email: {qiangl,xxli,dzheng,kfchen}@sjtu.edu.cn

***Abstract*—Given the number $n$ of the participants, one can solve an integer programming on $2^n$ variables to construct an optimal multiple assignment with threshold schemes for general access structure. In this paper, we focus on finding optimal multiple assignments with $(m,m)$-schemes. We prove that most of the variables in the corresponding integer programming take the value of 0, while the remaining variables take the values of either 0 or 1. We also show that given a complete access structure, an optimal scheme may be obtained directly from the scheme by Ito, Saito, and Nishizeki (Secret sharing scheme realizeing any access structure, in Globecom 1987).**

***Keywords*—multiple assignments, threshold scheme, integer programming, access structure.**

## I. Introduction

In a secret sharing scheme (SSS) [1], [2], a dealer $P_0$ distributes a secret among several participants $P = \{P_1, \cdots, P_n\}$, and a pair of algorithms, a distribution algorithm and a reconstruction algorithm, are involved. Given a secret $s$ in a finite domain $S$, the dealer $P_0$ runs the distribution algorithm to compute the *shares* $s_i, (i = 1, \cdots, n)$ which are further sent to the participant $P_i, (i = 1, \cdots, n)$, respectively. The *qualified* subset of $P$ can take their shares as input of the reconstruction algorithm to re-derive the secret $s$. We say a SSS is *perfect* if any unqualified subset of $P$ can not get any information about $s$.

An *access structure* $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ contains two families of subsets of $P$ and is *monotone* in the sense that, if a subset U is in the access structure, all sets that contain U as a subset should also form part of the access structure. A SSS realizes $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ over $S$ if: 1) it shares secret in $S$; 2) the subset of $P$ in $\mathcal{A}$ is qualified; and 3) the subset of $P$ in $\mathcal{F}$ is unqualified. It is known [6], [7] that there exist SSSs which realize any monotone access structure $\Gamma$ over a given $S$. In a $(k,n)$-threshold access structure, $\mathcal{A}$ contains all subset of $P$ that has at least $k$ participants. A SSS realizing $(k,n)$-threshold access structure is a $(k,n)$-threshold SSS. If any subset of $P$ belongs to either $\mathcal{A}$ or $\mathcal{F}$, we call the access structure *complete*.

Generally, the efficiency of a SSS is measured by entropy. The entropies of the secret $s$ and shares $s_i, (i = 1, \cdots, n)$ satisfy $H(s_i) \geq H(s)$, for every perfect SSS and any given access structure [3], [4], [5]. An access structure $\Gamma$ is *ideal* over $S$ if there exists a SSS realizing $\Gamma$ over $S$ such that $H(s) = H(s_i), i = 1, \cdots, n$. $\Gamma$ is *universally ideal* if $\Gamma$ is ideal over every finite $S$. The $(k,n)$-threshold access structure over $S$ where $|S| > n$ is ideal, and can be realized by the scheme proposed in [1]. Although many types of ideal access structures have been studied [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], it is an open problem to characterize the ideal access structure. Brickell and Davenport [9] explore this problem with matroids. Beimel and Chor [10] show that an access structure is universally ideal if and only if it is ideal over binary and ternary domains. The character of weighted threshold secret sharing is given in [21].

More generally, another open problem is to find the optimal SSS for general access structure. Benoloh and Leichter [7] propose a SSS for general access structure by combining several $(m,m)$-thresholds SSSs, which is simple but inefficient and is extended by [19], [20]. Comparing with the method in [7], [19], [20] that use the information of qualified subsets, Itoh, Saito and Nishizeki [6], [28] realize an access structure from the information of the unqualified subsets. [6], [28] use a single $(m,m)$-threshold SSS to realize general access structure and thus are applicable to visual secret sharing schemes [24], [25]. The SSS in [6], [28] is not efficient, especially for a $(k,n)$-threshold access structure with $k \neq n$. A modified method [22] can achieve a better efficiency for a nearly $(k,n)$-threshold access structure. The SSSs in [6], [28], [22] are *multiple assignment schemes* and assign multiple primitive shares for each participant where the primitive shares are selected from the shares set of a single $(k,m)$-threshold SSS. [23], [26] propose independently a novel method to obtain the optimal efficiency among all multiple assignment schemes by solving integer programming (IP, for short), and the method is extended in [27] to incomplete and/or ramp access structures. The complexity of solving an integer programming problem is related to the cardinality of the constraint variables set.

Generally, constructing a multiple assignment scheme for a given access structure with $(k,m)$-scheme will obtain higher efficiency than with $(m,m)$-scheme [23], [26]. But in some cases, constructing scheme from $(m,m)$-scheme is the only choice [29], [30]. For example, as $(k,m)$-threshold access structure is not universally ideal but $(m,m)$-threshold access is, there exists some domain $S$ such that there is no ideal $(k,m)$-threshold SSS over $S$. Another example, only $(m,m)$-threshold SSSs are appropriate to construct a visual secret sharing scheme.

In this paper, we propose a method to reduce the number of constraint variables in the integer programming problem [23], [26], [27]. We prove that the integer programming problem will be simplified to a 0-1 programming problem if the multiple assignment scheme is constructed with $(m, m)$-threshold SSSs. We also show that the scheme in [6] attains the optimal efficiency among all multiple assignment schemes which are constructed with $(m, m)$-threshold SSSs to realize a given complete access structure.

This paper is organized as follows. In Section 2, we give the definitions of SSSs and introduce the main result of [23], [26]. In Section 3, we point out that some constraint variables of the integer programming problem in [23], [26] take the value of 0, and further prove that the integer programming problem will be simplified to a 0-1 programming problem if the multiple assignment scheme is constructed with $(m, m)$-threshold SSSs. We show in Section 4 that the scheme in [6] achieves the optimal efficiency if all multiple assignment schemes are constructed with $(m, m)$-threshold SSSs to realize a given complete access structure. Conclusions are drawn in Section 5.

## II. Preliminaries

### A. Definitions

Let $P$ be a finite set and $\mathcal{A}, \mathcal{F} \supseteq 2^P$, we say $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ is monotone if:

$$\begin{cases} A \in \mathcal{A} \Rightarrow \forall A' \supseteq A, A' \in \mathcal{A} \\ F \in \mathcal{F} \Rightarrow \forall F' \subseteq F, F' \in \mathcal{F} \\ \mathcal{A} \cap \mathcal{F} = \emptyset \end{cases} \quad (1)$$

Let $\Pi$ be a SSS. Suppose the dealer $P_0$ wants to share a secret $s \in S$ among $P = \{P_1, \cdots, P_n\}$ and the share of participant $P_i$ is $s_i = \mathbf{E}(i, s, r), (1 \leq i \leq n)$. For a subset of participants $A = \{P_{i_1}, \cdots, P_{i_t}\} \subseteq P$, if there exists a reconstruction algorithm $\mathbf{D}_A$ such that

$$\forall s \in S, r \in R : s = \mathbf{D}_A(s_{i_1}, \cdots, s_{i_t}) \quad (2)$$

then $A$ is a qualified subset of $\Pi$. If such an algorithm does not exist, $A$ is a unqualified subset of $\Pi$.

Let $\mathcal{A}_\Pi$ be the family of all qualified subsets of $\Pi$, and $\mathcal{F}_\Pi$ be the family of all unqualified subsets of $\Pi$. Define the access structure of $\Pi$ as $\Gamma_\Pi \stackrel{\text{def}}{=} \{\mathcal{A}_\Pi, \mathcal{F}_\Pi\}$. It is obvious that $\Gamma_\Pi$ is monotone and $\mathcal{A}_\Pi \cup \mathcal{F}_\Pi = 2^P$. We say $\Pi$ realizes $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ if $\mathcal{A} \subseteq \mathcal{A}_\Pi, \mathcal{F} \subseteq \mathcal{F}_\Pi$.

Monotonicity implies that $\mathcal{A} \cap \mathcal{F} = \emptyset$ for every access structure. It is obvious that if $\mathcal{A} \cup \mathcal{F} = 2^P$, then $\Gamma$ is complete, otherwise $\Gamma$ is incomplete.

As an access structure must be monotone, we can define the family $\mathcal{A}^-$ of *minimal* qualified subsets and the family $\mathcal{F}^+$ of *maximal* unqualified subsets:

$$\begin{cases} \mathcal{A}^- \stackrel{\text{def}}{=} \{A \in \mathcal{A} : \forall P_i \in A, A - \{P_i\} \notin \mathcal{A}\} \\ \mathcal{F}^+ \stackrel{\text{def}}{=} \{F \in \mathcal{F} : \forall P_i \in P - F, F \cup \{P_i\} \notin \mathcal{F}\} \end{cases} \quad (3)$$

$\Gamma_0 = \{\mathcal{A}^-, \mathcal{F}^+\}$ is called the *basis* of $\Gamma = \{\mathcal{A}, \mathcal{F}\}$. It is easy to check that there is a unique basis $\Gamma_0$ corresponding to a given access structure $\Gamma$, and vice versa. Thus monotonicity can also be described as below [28]:

**Theorem 1:** ([28]) $\mathcal{A}, \mathcal{F} \subseteq 2^P$ are monotone if and only if it holds that

$$\forall A \in \mathcal{A}^-, F \in \mathcal{F}^+, A \nsubseteq F$$

A SSS realizes $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ means that any subset $A \in \mathcal{A}$ is qualified, while any subset $F \in \mathcal{F}$ is unqualified. A SSS realizes $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ if and only if:

$$\begin{cases} \forall A \in \mathcal{A}^- : A \text{ is qualified} \\ \forall F \in \mathcal{F}^+ : F \text{ is unqualified} \end{cases} \quad (4)$$

A $(k, n)$-threshold scheme is a perfect SSS which realizes the complete $(k, n)$-threshold access structure.

The efficiency of a SSS is measured by the term *information rate*. The *information rate* of $P_i$ is defined as $\rho_i = H(S_i)/H(S)$. Since there may be $n$ different $\rho_i$ in a SSS, one may define the *average information rate* $\bar{\rho}$ and *worst information rate* $\check{\rho}$ respectively:

$$\bar{\rho} \stackrel{\text{def}}{=} \frac{1}{n} \sum_{i=1}^{n} \rho_i$$
$$\check{\rho} \stackrel{\text{def}}{=} \max\{\rho_i, 1 \leq i \leq n\}$$

### B. Multiple Assignment Schemes

Let $\Omega = \{w_1, \cdots, w_m\}$ be the primitive shares set of a $(k, m)$-threshold SSS over $S$ and $\psi : P \to 2^\Omega$ be a map which assigns each participant a subset of $\Omega$. For a subset $X \subseteq P$ of participants, the primitive shares set held by $X$ is $\Psi(X) \stackrel{\text{def}}{=} \bigcup_{P_i \in X} \psi(P_i)$. If there exists a map $\psi$ s.t.

$$\begin{cases} \forall A \in \mathcal{A}^- : |\Psi(A)| \geq k \\ \forall F \in \mathcal{F}^+ : |\Psi(F)| \leq k - 1 \end{cases} \quad (5)$$

then we can find a perfect SSS realizing $\Gamma$. We call the map $\psi$ a *multiple assignment map*, and the corresponding SSS a *multiple assignment scheme*.

Each primitive share in a $(k, m)$-threshold SSS has the same information entropy as the secret. Thus, $\rho_i, \bar{\rho}, \check{\rho}$ for a multiple assignment scheme can be calculated as follows:

$$\begin{cases} \forall P_i \in P : \rho_i = |\psi(P_i)| \\ \bar{\rho} = \frac{1}{n} \sum_{i=1}^{n} |\psi(P_i)| \\ \check{\rho} = \max\{|\psi(P_i)|, 1 \leq i \leq n\} \end{cases} \quad (6)$$

In [6], [28], the authors provide a multiple assignment scheme to construct the primitive shares set by using a $(m, m)$-threshold SSS. This method can achieve a feasible solution for the integer programming problem [23], [26], [27] and is reviewed below.

**Construction 1:** ([6]) Let $\mathcal{F}^+ = \{F_1, \cdots, F_m\}$ be the family of maximal unqualified subsets of an access structure, and $\Omega = \{w_1, \cdots, w_m\}$ be the primitive shares set of a $(m, m)$-threshold SSS. The multiple assignment map $\psi : P \to 2^\Omega$ is defined as:

$$\psi(P_i) = \{w_j : P_i \notin F_j; j = 1, \cdots, m\}.$$

One can verify that the SSS constructed by Construction 1 realizes the corresponding access structure. Indeed, $\forall F \in$

$\mathcal{F}, \exists F_j \in \mathcal{F}^+$ such that $F \subseteq F_j$, so it follows that $w_j \notin \Psi(F) = \bigcup_{P_i \in F} \psi(P_i)$. On the other hand, $\forall A \in \mathcal{A}$ and $\forall F_j \in \mathcal{F}^+$, it holds that $\exists P_i \in A - F_j$, so $w_j \in \psi(P_i)$, and this means that $\Psi(A) = \Omega$.

### *C. Optimal Multiple Assignment Schemes*

One can construct *optimal multiple assignment schemes* by solving integer programming [23], [26].

We know that, $\forall 0 < j < 2^n, \exists$ unique $j_i \in \{0,1\}, (i = 1, \cdots, n)$ such that $j = \sum_{i=1}^{n} j_i 2^{i-1}$. Let $\Omega_j$ be the set of primitive shares owned by all participants in subset $X_j \overset{\text{def}}{=} \{P_i | j_i = 1, P_i \in P\}$ and denote $x_j$ as $|\Omega_j|$. For subset $X = \{P_{i_1}, P_{i_2}, \cdots, P_{i_l}\} \subseteq P$, we define $j_X \overset{\text{def}}{=} \bigvee_{k=1}^{l} j_{i_k}$ where $\vee$ is the bitwise OR operation. Obviously, $\Psi(X)$ contains the $x_j$ primitive shares iff. $j_X = 1$. As $\{\Omega_j | 0 < j < 2^n\}$ is a partition of the primitive shares set $\Omega$, we have

$$\begin{cases} \forall P_i \in P : |\psi(P_i)| = \sum_{j_i=1} x_j \\ \forall X \subseteq P : |\Psi(X)| = \sum_{j_X=1} x_j \end{cases} \tag{7}$$

Equation (5) implies that a multiple assignment scheme realizes $\Gamma = \{\mathcal{A}, \mathcal{F}\}$ iff.

$$\begin{cases} \forall A \in \mathcal{A}^- : \sum_{j_A=1} x_j \geq k \\ \forall F \in \mathcal{F}^+ : \sum_{j_F=1} x_j \leq k-1 \\ \forall 0 < j < 2^n : x_j \geq 0 \\ k \geq 0 \end{cases} \tag{8}$$

For any given access structure $\Gamma$, the primitive shares in the multiple assignment scheme by construction 1 are selected from a $(m,m)$-threshold SSS, which gives a feasible solution for constraints (8).

Equation (6) tells us that given $\Gamma = \{\mathcal{A}, \mathcal{F}\}$, the problem of finding a multiple assignment scheme with optimal average information rate is equivalent to the following integer programming problem:

$$\text{minimize:} \sum_{i=1}^{n} \sum_{j_i=1} x_j$$
$$\text{s.t:} \begin{cases} \forall A \in \mathcal{A}^- : \sum_{j_A=1} x_j \geq k \\ \forall F \in \mathcal{F}^+ : \sum_{j_F=1} x_j \leq k-1 \\ \forall 0 < j < 2^n : x_j \geq 0 \\ k \geq 0 \end{cases} \tag{9}$$

and the problem of finding a multiple assignment scheme with optimal worst information rate is equivalent to the following integer programming problem:

$$\text{minimize:} d$$
$$\text{s.t:} \begin{cases} \forall A \in \mathcal{A}^- : \sum_{j_A=1} x_j \geq k \\ \forall F \in \mathcal{F}^+ : \sum_{j_F=1} x_j \leq k-1 \\ \forall 1 \leq i \leq n : \sum_{j_i=1} x_j \leq d \\ \forall 0 < j < 2^n : x_j \geq 0 \\ k \geq 0, d \geq 0 \end{cases} \tag{10}$$

## III. Multiple Assignment Schemes with $(m,m)$-Schemes

Every multiple assignment scheme has a unique assignments set $\{x_j | x_j \geq 0, 0 < j < 2^n\}$ when the scheme is fixed. On the other hand, every set $\{x_j | x_j \geq 0, 0 < j < 2^n\}$ determines a multiple assignment scheme, and if $\{x_j | x_j \geq 0, 0 < j < 2^n\}$ satisfies equation (8), then the corresponding multiple assignment scheme realizes the given access structure $\Gamma = \{\mathcal{A}, \mathcal{F}\}$.

For any given $\Gamma = \{\mathcal{A}, \mathcal{F}\}$, we can obtain the optimal multiple assignment scheme by finding the optimal solution of the IP problems (9) or (10) [23], [26]. The complexity of integer programming is related with the number of variables and the constraints on variables: less variables or more strict constraints on variables will decrease the computing complexity on finding solution of IP. Our coming arguments are towards this.

**Theorem 2:** $x_{2^n-1}$ must be zero in every optimal solution of IP (9) and (10).

*Proof:* 1)For IP (9): Otherwise, let $\bar{k}, \bar{x}_j, (0 < j < 2^n, \bar{x}_{2^n-1} > 0)$ be an optimal solution of IP (9). Consider $k = \bar{k} - \bar{x}_{2^n-1}, x_j = \bar{x}_j, (0 < j < 2^n - 1), x_{2^n-1} = 0$, it is easy to find that the later is a feasible solution of IP (9) and has a less objective value, which is conflict with the optimality of $\bar{k}, \bar{x}_j, (0 < j < 2^n, \bar{x}_{2^n-1} > 0)$.
2)For IP (10): Otherwise, let $\bar{k}, \bar{d}, \bar{x}_j, (0 < j < 2^n, \bar{x}_{2^n-1} > 0)$ be an optimal solution of IP (10). Consider $k = \bar{k} - \bar{x}_{2^n-1}, d = \bar{d} - \bar{x}_{2^n-1}, x_j = \bar{x}_j, (0 < j < 2^n - 1), x_{2^n-1} = 0$, it is easy to find that the later is a feasible solution of IP (10) and has a less objective value, which is conflict with the optimality of $\bar{k}, \bar{d}, \bar{x}_j, (0 < j < 2^n, \bar{x}_{2^n-1} > 0)$. ■

Theorem 2 says that there is no primitive shares held by all participants in any optimal multiple assignment schemes.

In some cases, primitive shares must be selected from a $(m,m)$-scheme. Next we will focus on this condition. In fact, we can get the optimal multiple assignment scheme from $(m,m)$-schemes with minimal average information rate from

IP (11):

$$\text{minimize: } \sum_{i=1}^{n}\sum_{j_i=1} x_j$$
$$\text{s.t:}$$
$$\begin{cases} \forall A \in \mathcal{A}^- : \sum\limits_{j_A=1} x_j = m \\ \forall F \in \mathcal{F}^+ : \sum\limits_{j_F=1} x_j \le m-1 \\ m = \sum\limits_{j=1}^{2^n-1} x_j \\ \forall 0 < j < 2^n : x_j \ge 0 \end{cases} \tag{11}$$

Also, optimal multiple assignment scheme with $(m, m)$-schemes with minimal worst information rate can be constructed from IP (12):

$$\text{minimize:} d$$
$$\text{s.t:}$$
$$\begin{cases} \forall A \in \mathcal{A}^- : \sum\limits_{j_A=1} x_j = m \\ \forall F \in \mathcal{F}^+ : \sum\limits_{j_F=1} x_j \le m-1 \\ \forall 1 \le i \le n : \sum\limits_{j_i=1} x_j \le d \\ m = \sum\limits_{j=1}^{2^n-1} x_j \\ \forall 0 < j < 2^n : x_j \ge 0 \end{cases} \tag{12}$$

Obviously, IP (11) and (12) have same constraints (13):

$$\begin{cases} \forall A \in \mathcal{A}^- : \sum\limits_{j_A=1} x_j = m \\ \forall F \in \mathcal{F}^+ : \sum\limits_{j_F=1} x_j \le m-1 \\ m = \sum\limits_{j=1}^{2^n-1} x_j \\ \forall 0 < j < 2^n : x_j \ge 0 \end{cases} \tag{13}$$

Let $\wedge$ be the bitwise AND operation, then we have:

**Theorem 3:** For every feasible solution satisfying constraints (13), the following holds:

$$\begin{cases} \forall 0 < j < 2^n : \bigwedge\limits_{A \in \mathcal{A}^-} j_A = 0 \Rightarrow x_j = 0 \\ \forall F \in \mathcal{F}^+ : \sum\limits_{j_F=0} x_j \ge 1 \\ \forall 0 < j < 2^n : x_j \ge 0 \end{cases} \tag{14}$$

On the other hand, every solution satisfying constraints (14) will also satisfy constraints (13). In others words, constraints (13) are equal to constraints (14).

*Proof:* 1) We first prove: If $x_j, (0 < j < 2^n)$ satisfy constraints (14), then constraints (13) hold.

1.1): $\forall A \in \mathcal{A}^- : \sum_{j_A=1} x_j = m$. From $\forall 0 < j < 2^n : \bigwedge_{A \in \mathcal{A}^-} j_A = 0 \Rightarrow x_j = 0$. we get the result: $m = \sum_{j=1}^{2^n-1} x_j = \sum_{\bigwedge_{A\in\mathcal{A}^-} j_A=1} x_j$. Obviously, $\forall A \in \mathcal{A}^- : \bigwedge_{A \in \mathcal{A}^-} j_A = 1 \Rightarrow j_A = 1$, but $\forall 0 < j < 2^n : x_j \ge 0$, so $m = \sum_{\bigwedge_{A\in\mathcal{A}^-} j_A=1} x_j \le \sum_{j_A=1} x_j \le \sum_{j=1}^{2^n-1} x_j = m$

1.2): $\forall F \in \mathcal{F}^+ : \sum_{j_F=1} x_j \le m-1$. Because $j_X$ is either 0 or 1 for every subset $X \subseteq P$, we have $\forall F \in \mathcal{F}^+ : \sum_{j_F=1} x_j + \sum_{j_F=0} x_j = \sum_{j=1}^{2^n-1} x_j$ then $\forall F \in \mathcal{F}^+ : \sum_{j_F=0} x_j \ge 1$ is equal to $\forall F \in \mathcal{F}^+ : \sum_{j_F=1} x_j \le m-1$

2) Now we will prove: If $x_j, (0 < j < 2^n)$ satisfy constraints (13), then constraints (14) hold.

2.1): $\forall 0 < j < 2^n : \bigwedge_{A \in \mathcal{A}^-} j_A = 0 \Rightarrow x_j = 0$.

Otherwise, there is a $\bar{j}, (0 < \bar{j} < 2^n)$ and a subset $A \in \mathcal{A}^-$ such that $x_{\bar{j}} \ge 1, \bar{j}_A = 0$, but this means

$$\sum_{j_A=1} x_j \le \sum_{j \ne \bar{j}} x_j = m - x_{\bar{j}} \le m-1$$

2.2): $\forall F \in \mathcal{F}^+ : \sum_{j_F=0} x_j \ge 1$.

We have just proved this in 1.2). ■

From Theorem 3, if $\bigwedge_{A \in \mathcal{A}^-} j_A = 0$, then $x_j$ will be zero. This means that we can delete all these $x_j$s from the integer programming and thus decrease the complexity. We can also obtain more strict constraints on the remaining $x_j$s in the following theorem.

**Theorem 4:** If $\bar{x}_j, (0 < j < 2^n, \bar{x}_{\bar{j}} \ge 2)$ is a feasible solution satisfying constraints (14), then $x_j = \bar{x}_j, (0 < j \ne \bar{j} < 2^n), x_{\bar{j}} = 1$ is another feasible solution satisfying constraints (14). Furthermore, $\rho_i, (P_i \in P), \bar{\rho}, \check{\rho}$ for the later solution are not greater than those for the former solution, respectively.

*Proof:* It's easy to check that $x_j = \bar{x}_j, (0 < j \ne \bar{j} < 2^n), x_{\bar{j}} = 1$ is another feasible solution satisfying constraints (14). If we denote $f_i$ as the number of primitive shares held by $P_i$ in the former solution and $g_i$ the number of primitive shares held by $P_i$ in the later solution, then we have

$$f_i - g_i = \begin{cases} 0 & \bar{j}_i = 0 \\ \bar{x}_{\bar{j}} - 1 \ge 1 & \bar{j}_i = 1 \end{cases} \tag{15}$$

which means $\rho_i$ for the later solution is less than or equal to the one for the former solution. From the definition of $\bar{\rho}, \check{\rho}$, we complete the proof. ■

Theorem 4 says that integer programming for finding optimal multiple assignment schemes with $(m, m)$-schemes can be reduced to $0-1$ programming. In other words, the constraints (14) can be changed to the constraints (16):

$$\begin{cases} \forall 0 < j < 2^n : \bigwedge\limits_{A \in \mathcal{A}^-} j_A = 0 \Rightarrow x_j = 0 \\ \forall F \in \mathcal{F}^+ : \sum\limits_{j_F=0} x_j \ge 1 \\ \forall 0 < j < 2^n : x_j \in \{0, 1\} \end{cases} \tag{16}$$

## IV. Multiple Assignment Schemes with $(m, m)$-Schemes for Complete Access Structure

We now consider multiple assignment schemes from $(m.m)$-schemes for complete access structure. Surprisingly, we can get an optimal scheme without solving the $0-1$ programming. This is expressed as follows.

First, $\forall S \subseteq P$, denote $j(S) = \sum_{i=1}^{n} j_{(i,S)} 2^{i-1}$ where

$$j_{(i,S)} = \begin{cases} 0 & P_i \in S \\ 1 & P_i \in P - S. \end{cases}$$

**Theorem 5:** Let $\{\mathcal{A}^-, \mathcal{F}^+\}$ be the basis for a complete access structure, then the equation (16) leads to constraints (17):

$$\forall F \in \mathcal{F}^+, x_{j(F)} = 1 \tag{17}$$

*Proof:* $\forall F \in \mathcal{F}^+$, primitive shares not owned by participants in $F$ must be owned by all participants in $P - F$. Otherwise, suppose $P_i \in P - F$ does not own some primitive shares which are not owned by participants in $F$, then this shares are not owned by participants in $F \cup \{P_i\}$, and this means that $F \cup \{P_i\}$ is an unqualified subset, but this is contradictory with $F \in \mathcal{F}^+$. Up to now, we proved that if $P_i \in P - F, j_i = 0$, then $x_j = 0$. On the other hand, from $\forall F \in \mathcal{F}^+ : \sum_{j_F=0} x_j \geq 1$ and $\forall 0 < j < 2^n : x_j \in \{0, 1\}$, It follows that if $F \in \mathcal{F}^+$ then $x_{j(F)} = 1$. ∎

Set

$$x_j = \begin{cases} 1 & \exists F \in \mathcal{F}^+ \text{ such that } j = j(F) \\ 0 & \text{others.} \end{cases} \tag{18}$$

Theorem 5 tells us that solution assigned by (18) is a feasible solution to constraints (16). Furthermore, for every participant $P_i \in P$ there is no solution satisfying constraints (16) such that: the number of primitive shares owned by $P_i$ in this solution is less than the one in solution assigned by (18). In other words, solution assigned by (18) is optimal for every participant $P_i \in P$. As a result, this solution achieves the minimal $\rho_i, (P_i \in P), \bar{\rho}, \check{\rho}$. Note that the solution assigned by (18) is the same as that by [6].

## V. Conclusion

We consider multiple assignment schemes with $(m, m)$-schemes in this paper. Our contributions are two-fold: 1) most variables in the corresponding integer programming in such a case will be vanished, and the remaining variables take the value of either 0 or 1; 2) when the access structure is complete, then the optimal scheme can be constructed directly by the method [6]. One open problem is to simplify the $0-1$ programming for non-complete access structure.

## Acknowledgment

The authors would like to thank the support from National Natural Science Foundation of China (NSFC No. 61070249, 60970111, 60803146).

## References

[1] A. Shamir, "How to share a secret", Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys", AFIPS 1979 Nat. Computer Conf., vol. 48, pp. 313-317, 1979.

[3] E. D. Karnin, J. W. Green and M. E. Hellman, "On secret sharing systems", IEEE Trans. Inform. Theory, no. 29, pp. 35-41, 1983.

[4] R. M. Capocelli, A. D. Santis, L. Gargano and U. Vaccaro, "On the size of shares for secret sharing schemes", J. of Crytology, vol. 6, pp. 157-167, 1993.

[5] L. Csirmaz, "The size of a share must be large", J. of Cryptology, vol. 10, pp. 223-231, 1997.

[6] M. Ito, A. Saito and T. Nishizeki, "Secret sharing scheme realizeing any access structure", in Proc. IEEE Global Telecommunication Conf., Globecom'87, 1987, pp. 99-102.

[7] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions", in Advances in Cryptology-CRYPTO'88 Proceedings, vol. 403 of Lecture Notes in Computer Science, S. Goldwasser, Ed. New York: Springer-Verlag, 1990, pp. 27-35.

[8] E. F. Brickell, "Some ideal secret sharing schemes", Journal of Combin. Math. and Combin. Comput., 6:105-113, 1989.

[9] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes", J. of Cryptology, vol. 4, no. 73, pp. 123-134, 1991.

[10] A. Beimel and B. Chor, "Universally ideal secret sharing schemes", IEEE Trans. on Information Theory, 40(3): 786-794, 1994.

[11] W. Jackson, K. M. Martin and C. M. O'Keefe, "Ideal secret sharing schemes with multiple secrets", J. of Cryptology, 9(4):233-255, 1996.

[12] J. Martí-Farré and C. Padró, "Secret sharing schemes on access structures with intersection number equal to one", 3rd SCN, vol. 2576 of LNCS, pp. 354-363. 2002.

[13] K. M. Martin, "Discrete Structures in the Theory of Secret Sharing", PhD thesis, University of London, 1991.

[14] P. Morillo, C. Padró, G. Sáez and J. L. Villa, "Weighted threshold secret sharing schemes", Inform. Process. Lett., 70(5):211-216, 1999.

[15] C. Padró and G. Sáez, "Secret sharing schemes with bipartite access structure", IEEE Trans. on Information Theory, 46:2596-2605, 2000.

[16] P. D. Seymour, "On secret-sharing matroids", J. of Combinatorial Theory, Series B, 56:69-73, 1992.

[17] J. Simonis and A. Ashikhmin, "Almost affine codes", Designs, Codes and Cryptography, 14(2):179-197, 1998.

[18] T. Tassa, "Hierarchical threshold secret sharing", In M. Naor, editor, First Theory of Cryptography Conference, TCC 2004, vol. 2851 of LNCS, pages 473-490, 2004.

[19] D. R. Stinson, "Decomposition construction for secret-sharing schemes", IEEE Trans. Inform. Theory, vol. 40, no. 1, pp.118-125, 1994.

[20] K. Tochikubo, T. Uyematsu and R. Matusmoto, "Efficient secret sharing schemes based on authorized subsets", IEICE Trans. Fundamentals, vol. E88-A, no. 1, pp. 322-326, 2005.

[21] A. Beimel, T. Tassa and E. Weinreb, "Characterizing Ideal Weighted Threshold Secret Sharing", Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Comput. Sci. 3378 (2005) 600-619.

[22] K. Tochikubo, "Efficient secret sharing schemes realizing general access structures", IEICE Trans. Fundamentals, vol. E87-A, no.7, pp. 1788-1797, 2004.

[23] Q. Li, H. Yan and K. F. Chen, "A New Method Of Using (k,n)-Threshold Scheme To Realize Any Access Structure", (in Chinese), Journal of Shanghai Jiaotong University (ISSN:1006-2467), vol. 38, no. 1, pages 103-106, Jan. 2004.

[24] G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson, "Visual cryptography for general access structures", Information and Computation, vol. 129, pp. 86-106, 1996.

[25] H. Koga, M. Iwamoto and H. Yamamoto, "An analytic construction of the visual secret sharing scheme for color images", IEICE Trans. Fundamentals, vol. E84-A, no. 1, pp.262-272,2001.

[26] M. Iwamoto, H. Yamamoto and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes", Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on, 27 June-2 July 2004 Page(s): 16 -

[27] M. Iwamoto, H. Yamamoto and H.Ogawa, "Optimal Multiple Assignments Based on Integer Programming in Secret Sharing Schemes with General Access Structures", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2007 E90-A(1):101-112

[28] M. Ito, A. Saito and T. Nishizeki, "Multiple Assignment Scheme for Sharing Secret", J. of Cryptology, vol.6, pp. 15-20, 1993.

[29] G.Ateniese, C.Blundo, A.D.Santis, and D.R.Stinson: Visual cryptography for general access structures. Information and Computation, vol. 129, pp. 86-106, 1996.

[30] H.Koga, M.Iwamoto, and H. Yamamoto. An analytic construction of the visual secret sharing scheme for color images. IEICE Trans. Fundamentals, vol. E84-A, no. 1, pp. 262-272, 2001