The Optimal Linear Secret Sharing Scheme for Any Given Access Structure

Tang Chunming, Gao Shuhong, and Zhang Chengli

***Abstract*—Any linear code can be used to construct a linear secret sharing scheme. In this paper, it is shown how to decide optimal linear codes (i.e., with the biggest information rate) realizing a given access structure over finite fields. It amounts to solving a system of quadratic equations constructed from the given access structure and the corresponding adversary structure. The system becomes a linear system for binary codes. An algorithm is also given for finding the adversary structure for any given access structure.**

***Index Terms*—Cryptography, secret sharing, linear code, access structure, adversary structure.**

I. Introduction

Secret sharing schemes were first introduced by Blakley [4] and Shamir [22] in 1979. Since then, many constructions have been proposed. The relationship between Shamir's secret sharing scheme and Reed-Solomon codes was pointed out by McEliece and Sarwate in 1981 [18]. Later several authors have considered construction of secret sharing schemes using linear error correcting codes. Massey utilized linear codes for secret sharing schemes and pointed out the relationship between the access structure and the minimal codewords of the dual code of the underlying codes [15], [16]. Several authors have investigated minimal codewords for several classes of codes and characterized their access structures [1], [2], [3], [10], [11], [21], [23]. Unfortunately, determining minimal codewords is an NP-hard problem for general linear codes.

As pointed out by Massey [17], the main problem is to characterize which access structures can be realized by linear codes. We call this the access structure problem.

In [14], Karchmer and Widgerson gave a significant result that there exists a linear code for any access structure among n participants, however, there still exist the following problems:

1) whether does there exist an ideal linear code realizing given access structure? how to construct it if it exists? A linear code is ideal if the length of code is equal to $n+1$, where n is the number of participants.
2) how to gain the optimal linear code realizing given access structure if there is not ideal linear code? A linear code is optimal if the length of code is the shortest among all linear codes which realize the given access structure. Obviously, the length of optimal linear code is bigger than $n+1$.

Our Contributions.

Tang Chunming is with the Department of Mathematics and Information Science, Guangzhou University, Guangzhou, 510006 China e-mail: ctang@gzhu.edu.cn

1) An access structure uniquely determines an adversary structure and vice versa. We first give an algorithm for finding the adversary structure R corresponding to a given access structure Γ.
2) We show that finding linear codes for an access structure Γ is equivalent to solving a system of quadratic polynomial equations which is constructed from Γ and R. The given access structure Γ is realizable by a linear code over F_q if and only if the system has a solution over F_q. When the underlying field is F_2, the system becomes a linear system, so can be solved in polynomial time (in terms of the sizes of Γ and R).
3) We show how to reduce the number variables that are used in the polynomial equations, hence speeding up any algorithm for solving the polynomial system. This seems to be the first algorithmic approach for the access structure problem.
4) We propose an algorithm to construct the optimal linear code realizing a given access structure if the ideal linear code does not exist.

Related Works. The secret sharing schemes we consider in this paper are ideal and perfect. A secret sharing scheme is called ideal if the size of each share is equal to the size of the secret, and called perfect if every subset of shares can either reconstruct the secret or get no partial information at all on the secret, that is, if a subset of the participants can deduce any partial information on the secret then they can completely reconstruct the secret. The span program proposed by Karchmer and Widgerson [14] is a secret sharing scheme that can be perfect but not ideal. In their paper, an access structure corresponds to a monotone Boolean function. They show how to compute monotone functions via matrices over finite fields (which correspond to generating matrices for linear codes). They pointed out that it is easy to realize any access structure via non ideal secret sharing schemes. Further results in this direction can be found in [5], [8], [9], [12], [13], [24], [25].

Outline of the Paper. The paper is organized as follows. In Section II, we recall the relationships between secret sharing schemes and linear codes. In Section III, we consider the existence of linear codes over a finite field F_q for a given access structure and present an efficient algorithm for finding the adversary structure for any given access structure. In Section IV, we give improvements on results in Section III, especially on what reducing the number of constraints needed from R. In Section V, an algorithm to find optimal linear code is proposed.

II. Secret Sharing Schemes and Linear Codes

A linear code C of length $n+1$ over $\mathbb{F}_q$ is simply a linear subspace of $\mathbb{F}_q^{n+1}$. If C has dimension k, then C is generated by the rows of a $k \times (n+1)$ matrix $G = (\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_n)$ of rank k, which is called a generating matrix of C. There are several ways to use linear codes to construct secret sharing schemes [15], [21]. We focus mainly on secret sharing schemes that are perfect and ideal.

Suppose a secret s is to be shared among n participants, identified as $1, ..., n$. We assume that the secret s can be viewed as an element in a finite field $\mathbb{F}_q$. Let C be a linear code of length $n+1$ over $\mathbb{F}_q$ with dimension k. To compute the shares of s, a dealer D chooses a random codeword $\mathbf{t} = (t_0, t_1, ..., t_n) \in C$ such that $t_0 = s$. Then t_i is the share for the participant i, $1 \leq i \leq n$. More concretely, this can done as follows. Suppose $G = (\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_n)$ is a generating matrix for C where each g_i is a column vector of length k. Choose a random vector $\mathbf{u} = (u_0, ..., u_{k-1}) \in \mathbb{F}_q^k$ such that $s = \mathbf{u}\mathbf{g}_0$. There are altogether q^{k-1} such vectors $\mathbf{u} \in \mathbb{F}_q^k$. The dealer D computes the corresponding codeword

$$\mathbf{t} = (t_0, t_1, ..., t_n) = \mathbf{u}G,$$

then securely sends t_i to participant i as a share for $i = 1, 2, ..., n$.

The dual code $C^\perp$ of C is defined as

$$C^\perp = \{\mathbf{c} \in \mathbb{F}_q^{n+1} | G\mathbf{c}^t = 0\},$$

that is, a vector $\mathbf{c} \in \mathbb{F}_q^{n+1}$ is in $C^\perp$ iff $\mathbf{c}$ is orthogonal to all codewords in C. If $\mathbf{c} = (c_0, c_1, ..., c_n) \in C^\perp$ with $c_0 \neq 0$ then, for any codeword $(s, t_1, \ldots, t_n) \in C$, we have

$$s = \sum_{i=1}^{n} -\frac{c_i}{c_0} t_i. \tag{1}$$

Let

$$S_\mathbf{c} = \{i | 1 \leq i \leq n, \text{ and } c_i \neq 0\}.$$

Then the equation (1) implies that the secret s can be reconstructed from the shares $t_i, i \in S_\mathbf{c}$. Now suppose S is any subset of $[1, n] = \{1, \ldots, n\}$. The following lemma tells us when the participants in S can reconstruct the secret.

Lemma 1. *Let $(s, t_1, \ldots, t_n) \in C$ be a random codeword where C is generated by a matrix $G = (\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_n)$. Then, for any subset S of $[1, n]$,*

(a) *if $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_i, i \in S$, then the participants in S can reconstruct the secret s by a linear function as in (1) for some $\mathbf{c} \in C^\perp$; and*

(b) *if $\mathbf{g}_0$ is not a linear combination of $\mathbf{g}_i, i \in S$, then the participants in S can not compute any information on s.*

Part (a) is straightforward. Part (b) needs some clarifications. When $(s, t_1, \ldots, t_n)$ is a random codeword in C, the values $s, t_1, \ldots, t_n$ can be viewed as random variables. Then it is straightforward to show that the conditional Shannon entropy $H(s|t_i, i \in S) = 0$ in part (b). Hence the values $t_i, i \in S$ do not contain any information on s. This means that there is no function (linear or nonlinear) nor algorithm to compute s from the shares $t_i, i \in S$.

A subset $S \subseteq [1, n]$ is called an access or accepted set of C if there is $\mathbf{c} \in C^\perp$ such that $\mathbf{c}_0 = 1$ and

$$\text{supp}(\mathbf{c}) \subseteq S \cup \{0\},$$

where supp$(\mathbf{c}) = \{i \in [0, n] | \mathbf{c}_i \neq 0\}$, called the support of $\mathbf{c}$. If S is an accepted set then any set containing S is also accepted. An access set S is called minimal if no proper subset of it is an access set. Let $\Gamma(C)$ denote the set of all minimal access sets in C. Then a subset S is an access set of C iff S contains one of the sets on $\Gamma(C)$.

A subset S is called a rejected set of C if it is not an access set. If S is a rejected set then its any subset is also rejected. A rejected subset S is called maximal if every subset proper containing S is an access set. Let $R(C)$ denote the set of all maximal rejected sets of C.

Note that, given a code C, we do not know any efficient algorithm to find $\Gamma(C)$, as the problem of finding vectors of minimum Hamming weight in an arbitrary linear code is NP-hard. In the next section, we shall show how to find $\mathcal{R}(C)$ from $\Gamma(C)$, and give necessary and sufficient conditions for an access structure to be realizable by linear codes.

Before we proceeds to the next section, we briefly mention more general secret sharing schemes constructed from linear codes. Suppose the secret is a vector $(s_1, \ldots, s_\ell)$ of ℓ elements from a finite field $\mathbb{F}_q$, and it is to be shared by n participants $1, \ldots, n$. Let $m \geq n$. We use a linear code C of length $m + \ell$ over $\mathbb{F}_q$ to get a secret sharing scheme as follows. Partition the set $[1, m] = \{1, 2, \ldots, m\}$ as

$$[1, m] = T_1 \cup T_2 \cup \cdots \cup T_n.$$

Suppose C has a generator matrix of the form

$$G = (\mathbf{u}_1, \ldots, \mathbf{u}_\ell, \mathbf{g}_1, \ldots, \mathbf{g}_m),$$

where the column vectors $\mathbf{u}_1, \ldots, \mathbf{u}_\ell$ are linearly independent over $\mathbb{F}_q$. To share a secret $(s_1, \ldots, s_\ell)$, a dealer picks a random codeword

$$\mathbf{c} = (u_1, \ldots, u_\ell, t_1, \ldots, t_m) \in C$$

such that $(u_1, \ldots, u_\ell) = (s_1, \ldots, s_\ell)$. The share for the participant i $(1 \leq i \leq n)$ is the sequence $t_j, j \in T_i$.

When $\ell = 1$, this secret sharing scheme is equivalent to the span program of Karchmer and Widgerson [14], which is perfect but not ideal. It is easy to show that an arbitrary access structure can be realized by choosing a large m and a proper partition of $[1, m]$. So the access structure problem for this class of secret sharing schemes is trivial. However, finding the smallest m to realize a given assess structure is still wide open, which corresponds to the shortest program to compute a monotone Boolean function.

When $\ell > 1$, the above secret sharing scheme is not perfect any more, that is, it is possible that a subset of the participants can compute some partial information on the secret $(s_1, \ldots, s_\ell)$, but can not completely determine the secret. These schemes are studied by I Cascudo and H Chen et al in [6], [7], and by W. Ogata and K Kurosawa in [19], [20].

III. Linear Codes for Given Access Structures

Let $\Gamma = \{S_1, ..., S_m\}$ be any collection of subsets of $[1, n]$. Without loss of generality, we assume that no subset in Γ contains another subset in Γ. Then Γ defines an access structure for which a subset S of $[1, n]$ is accepted iff S contains a subset in Γ. Our goal in this section is characterizing, for a given access structure Γ, when there is a linear code C over $\mathbb{F}_q$ such that $\Gamma = \Gamma(C)$.

A subset T of $[1, n]$ is called rejected if it does not contain any subset in Γ. The collection of all rejected sets is called the adversary structure of Γ. Let $\mathcal{R}$ denote the collection of all maximal rejected sets of Γ.

Example 1. Assume an access structure

$$\Gamma = \{(1, 2, 3), (3, 4, 5), (3, 5, 6)\}$$

in a secret sharing scheme with participants $\{1, 2, 3, 4, 5, 6\}$. Then its adversary structure is

$$\mathcal{R} = \{(1, 2, 4, 5, 6), (1, 3, 4, 6), (2, 3, 4, 6), (1, 3, 5), (2, 3, 5)\}.$$

A. Finding Adversary Structures from Access Structures

Suppose we are given an access structure:

$$\Gamma = \{S_1, ..., S_m\},$$

where $S_i \subset [1, n]$ for $1 \le i \le m$. Γ can be denoted by a matrix:

$$\Gamma = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ & & \dots & \\ h_{m1} & h_{m2} & \dots & h_{mn} \end{pmatrix}$$

where $h_{ij} \neq 0$ if $j \in S_i$, else $h_{ij} = 0$ for $1 \le i \le m$, $1 \le j \le n$. Also, we define a $m \times (n+1)$ matrix $\mathbb{H}$ with the following form:

$$\mathbb{H} = \begin{pmatrix} \mathbf{1} & \Gamma \end{pmatrix} = \begin{pmatrix} 1 & h_{11} & h_{12} & \dots & h_{1n} \\ 1 & h_{21} & h_{22} & \dots & h_{2n} \\ & & \dots & & \\ 1 & h_{m1} & h_{m2} & \dots & h_{mn} \end{pmatrix} = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \dots \\ \mathbf{h}_m \end{pmatrix}, \quad (2)$$

where $\mathbf{1}$ is an all-one column vector.

We shall assume in the rest of the paper that each participant $i \in [1, n]$ is in some subset in Γ, so $\mathbb{H}$ has no all-zero column. Compared with matrix Γ, the matrix $\mathbb{H}$ is only added a column called the 0th column, and other columns of $\mathbb{H}$ are called the 1st,... nth column. The i-th column of $\mathbb{H}$ corresponds to participant i for $i = 1, 2, ..., n$.

Let $\mathbf{z}_j$ denote the jth column of $\mathbb{H}$, $1 \le j \le n$. For each $1 \le i \le m$, define

$$A_i = \{1 \le j \le n | \, |\text{supp}(\mathbf{z}_j)| = i\},$$

where$|S|$ denotes the number elements in a set S. Each A_i can be partitioned as

$$A_i = A_{i1} \cup \dots \cup A_{is},$$

where $k, l \in A_i$ are in one group iff the kth and lth column of $\mathbb{H}$ have the same support. This implies that if k, l are in different groups, there exist $j_1, j_2 \in \{1, 2, ..., m\}$ such that $h_{j_1 k} \neq 0, h_{j_1 l} = 0$ and $h_{j_2 k} = 0, h_{j_2 l} \neq 0$. Certainly, $s \le \binom{i}{m}$.

Also, for any subset $B \subseteq [1, m]$, let $\mathbb{H}_B$ denote the submatrix $\mathbb{H}$ consisting of the rows indexed by elements in B. We say a subset $T \subseteq [1, n]$ overlays a subset $B \subseteq [1, m]$ if, for each $i \in B$, there exists $j \in T$ such that $h_{ij} \neq 0$.

Lemma 2. *Let $B \subseteq [1, m]$ with $|B| = t$. If $T_1 \subseteq A_i$, $|T_1| > \mathrm{C}_{t-1}^{i}$, and any two elements in T_1 are in different groups in A_i, then T_1 must overlay B.*

Proof: There exist at most $\binom{i}{t-1}$ different groups in A_i in $t-1$ rows of $\mathbb{H}_B$, hence, T_1 must overlay B. □

Note that if $A \cup A' = [1, n]$ and $A \cap A' = \emptyset$, then $\overline{A} = A'$. We have the following simple lemma.

Lemma 3. *Let $B \subseteq [1, m]$. Then $T \subseteq [1, n]$ overlays B if and only if $\overline{T}$ does not contain any $S_i \in \Gamma$ with $i \in B$.*

Theorem 1. *A subset $\overline{T} \subseteq [1, n]$ is a maximal rejected set of Γ iff $[1, m]$ is overlayed by T but not by any proper subset.*

Proof: For any $k \in T$, $\overline{T} \cup \{k\}$ contains at least a $S_i \in \Gamma$. That is, $\overline{T}$ is a rejected set, but $\overline{T} \cup \{k\}$ is not a rejected set for any $k \in T$, i.e., $k \notin \overline{T}$, hence $\overline{T}$ is a maximal rejected set according to the definition of maximal rejected set.

On the other hand, if $S \in \mathcal{R}$, then $\overline{S}$ must overlay $[1, m]$ from Lemma 3. Now, assume there exists a proper subset $\overline{S'} \subset \overline{S}$ such that $\overline{S'}$ overlaps $[1, m]$, then S' is a rejected set. However, $S \subset S'$ is contrary to the assumption that S is a maximal rejected set. That is, if S is a maximal rejected set, then it must be generated by a set T which overlays $[1, m]$, however, $[1, m]$ is not overlayed by any proper subset of T.□

According to this theorem, we provide an algorithm to generate adversary structure $\mathcal{R}$ of Γ.

Algorithm: Finding $\mathcal{R}$ from Γ.

1) Initially $\mathcal{R}$ is empty. Define A_i's from Γ as above.
2) If $A_m \neq \emptyset$, then add $\overline{\{i\}}$ to $\mathcal{R}$ for each $i \in A_m$.
3) For i from $m-1$ down to 1, if $A_{m-i} \neq \emptyset$, find all subsets
$$T_1 \subseteq A_{m-i}, \quad T_2 \subseteq A_1 \cup \dots \cup A_{m-i-1},$$
such that $[1, m]$ is overlayed by $T_1 \cup T_2$ not by any proper subset of $T_1 \cup T_2$, and $|T_1| \ge 1$. For each of them, add $\overline{T_1 \cup T_2}$ to $\mathcal{R}$.
4) Return $\mathcal{R}$.

This algorithm may still have exponential running time when n is large. We hope to improve it to polynomial time in terms of the sizes of Γ and $\mathcal{R}$. Note that it is possible that the size of $\mathcal{R}$ itself may be exponentially larger than that of Γ. So there is no algorithm that is polynomial in the size of $\mathcal{R}$ alone.

B. Finding Linear Codes for Given Access Structures

In this section, we propose a method to decide when an access structure Γ can be realized by linear codes, that is, whether there is a linear code C over $\mathbb{F}_q$ such that $\Gamma = \Gamma(C)$. We need another characterization of rejected sets.

Lemma 4. *Let $C \subseteq \mathbb{F}_q^{n+1}$ be any linear code. Then a subset $T \subseteq [1, n]$ is a rejected set of C iff there is a codeword $\mathbf{c} = (c_0, c_1, \dots, c_n) \in C$ such that $c_0 = 1$ and $c_i = 0$ for* *all $i \in T$.*

Proof: Let $G = (\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_n)$ be any generator matrix for C. Suppose G has k rows (which need not be linearly independent). First assume that T is a rejected set of C. By definition, this means that $\mathbf{g}_0$ is not a linear combination of the vectors $\mathbf{g}_i, i \in T$. By linear algebra, there is a vector $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{F}_q^k$ such that

$$\mathbf{v}\mathbf{g}_0 = 1, \quad \mathbf{v}\mathbf{g}_i = 0, \text{ for all } i \in T.$$

Hence the codeword $\mathbf{c} = \mathbf{v}G \in C$ has the required the property.

Conversely, suppose C contains such a codeword $\mathbf{c} \in C$. Then $\mathbf{c} = \mathbf{v}G$ for some vector $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{F}_q^k$. T must be a rejected set, since if T were an accepted set then $\mathbf{g}_0$ would be a linear combination of the vectors $\mathbf{g}_i, i \in T$. Since $\mathbf{c}_i = \mathbf{v}\mathbf{g}_i = 0$ for all $i \in T$, we would have $c_0 = \mathbf{v}\mathbf{g}_0 = 0$, a contradiction. □

This lemma immediately gives us a method for finding linear codes to realize a given access structure $\Gamma = \{S_1, S_2, \ldots, S_m\}$. Let $\mathbb{H}$ be defined as above where $h_{ij} \neq 0$ were treated as unknowns for all $j \in S_i$. Suppose we have found the corresponding adversary structure of Γ:

$$\mathcal{R} = \{R_1, R_2, \ldots, R_\ell\}.$$

Define

$$\mathbb{G} = \begin{pmatrix} 1 & g_{11} & g_{12} & \cdots & g_{1n} \\ 1 & g_{21} & g_{22} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & g_{\ell 1} & g_{\ell 2} & \cdots & g_{\ell n} \end{pmatrix}, \tag{3}$$

where $g_{ij} = 0$ if $j \in R_i$ and g_{ij} is an unknown for all $j \notin R_i$.

Theorem 2 *There is a linear code for a given access structure $\Gamma = \{S_1, ..., S_m\}$ if and only if the following system of quadratic equations*

$$\mathbb{G}\mathbb{H}^\top = \mathbf{0}, \tag{4}$$

has a solution for h_{ij}, $j \in S_i$, and g_{ij}, $j \notin R_i$, over $\mathbb{F}_q$ with $h_{ij} \neq 0$ for $j \in S_i$.

Proof: Assume there exists a linear code C so that $\Gamma(C) = \Gamma$. Then all the minimal codewords with the first component 1 in $C^\perp$ are just $\mathbf{h}_1, ..., \mathbf{h}_m$, and for each $R_i \in \mathcal{R}$, there is no codeword $\mathbf{h} \in C^\perp$ such that $h_0 = 1$ and $\text{supp}(\mathbf{h}) \setminus \{0\} \subseteq R_i$. According to Lemma 4, $R_i \in \mathcal{R}$ if and only if if there exists a codeword $\mathbf{g}_i \in C$ such that $g_{i0} = 1$ and $g_{ij} = 0$ if $j \in R_i$. Obviously, $\langle \mathbf{g}_i, \mathbf{h}_j \rangle = 0$ for $1 \leq i \leq \ell$ and $1 \leq j \leq m$. Hence the system (4) has a required solution over $\mathbb{F}_q$.

Now, assume G and H is a solution to (4). Let C be the row span of G. Obviously, $\mathbf{h}_1, ..., \mathbf{h}_m \in C^\perp$, hence $S_1, ..., S_m \in \Gamma(C)$. Also, the ith row of G implies that $R_i \in \mathcal{R}(C)$ for $1 \leq i \leq \ell$. Therefore, C has no other minimal accepted sets, so is a linear code so that $\Gamma(C) = \Gamma$. □

C. Some Examples

Example 2. *Find a linear code over $\mathbb{F}_q^7$ for $\Gamma = \{(1,2,3),(3,4,5),(3,5,6)\}$.*

According to Theorem 1, $\mathcal{R} = \{(1,2,4,5,6),(1,3,4,6),(2,3,4,6),(1,3,5),(2,3,5)\}$. Let

$$\mathbb{H} = \begin{pmatrix} 1 & h_{11} & h_{12} & h_{13} & 0 & 0 & 0 \\ 1 & 0 & 0 & h_{23} & h_{24} & h_{25} & 0 \\ 1 & 0 & 0 & h_{33} & 0 & h_{35} & h_{36} \end{pmatrix},$$

$$\mathbb{G} = \begin{pmatrix} 1 & 0 & 0 & g_{13} & 0 & 0 & 0 \\ 1 & 0 & g_{22} & 0 & 0 & g_{25} & 0 \\ 1 & g_{31} & 0 & 0 & 0 & g_{35} & 0 \\ 1 & 0 & g_{42} & 0 & g_{44} & 0 & g_{46} \\ 1 & g_{51} & 0 & 0 & g_{54} & 0 & g_{56} \end{pmatrix},$$

where $h_{ij} \in \mathbb{F}_q^*$ for $1 \leq i \leq 3, 1 \leq j \leq 6$, and $g_{ij} \in F_q$ for $1 \leq i \leq 5, 1 \leq j \leq 6$.

According to Theorem 2, we need to solve the following system of equations:

$$\begin{cases} 1 + h_{13}g_{13} = 0 \\ 1 + h_{12}g_{22} = 0 \\ 1 + h_{11}g_{31} = 0 \\ 1 + h_{12}g_{42} = 0 \\ 1 + h_{11}g_{51} = 0 \\ 1 + h_{23}g_{13} = 0 \\ 1 + h_{25}g_{25} = 0 \\ 1 + h_{25}g_{35} = 0 \\ 1 + h_{24}g_{44} = 0 \\ 1 + h_{24}g_{54} = 0 \\ 1 + h_{33}g_{13} = 0 \\ 1 + h_{35}g_{25} = 0 \\ 1 + h_{35}g_{35} = 0 \\ 1 + h_{36}g_{46} = 0 \\ 1 + h_{36}g_{56} = 0 \end{cases} \tag{5}$$

It is straightforward to find a general solution: $h_{13} = h_{23} = h_{33}$, $h_{25} = h_{35}$, $g_{31} = g_{51} = -h_{11}^{-1}$, $g_{22} = g_{42} = -h_{12}^{-1}$, $g_{44} = g_{54} = -h_{24}^{-1}$, $g_{25} = g_{35} = -h_{25}^{-1}$, $g_{46} = g_{56} = -h_{36}^{-1}$, $g_{13} = -h_{13}^{-1}$. Hence there is a linear code C in $\mathbb{F}_q^7$ for the access structure Γ. □

Example 3. *Find a linear code C in $\mathbb{F}_q^5$ for $\Gamma = \{(1,2),(2,3),(3,4)\}$.*

According to Theorem 1, $\mathcal{R} = \{(1,3),(1,4),(2,4)\}$. Let

$$\mathbb{H} = \begin{pmatrix} 1 & h_{11} & h_{12} & 0 & 0 \\ 1 & 0 & h_{22} & h_{23} & 0 \\ 1 & 0 & 0 & h_{33} & h_{34} \end{pmatrix},$$

$$\mathbb{G} = \begin{pmatrix} 1 & 0 & g_{12} & 0 & g_{14} \\ 1 & 0 & g_{22} & g_{23} & 0 \\ 1 & g_{31} & 0 & g_{33} & 0 \end{pmatrix},$$

where $h_{ij} \in F_q^*$ for $1 \leq i \leq 3, 1 \leq j \leq 4$, and $g_{ij} \in F_q$ for $1 \leq i \leq 3, 1 \leq j \leq 4$.

According to Theorem 2, we obtain the following equations:

$$\begin{cases} 1+h_{12}g_{12}=0 \\ 1+h_{12}g_{22}=0 \\ 1+h_{11}g_{31}=0 \\ 1+h_{22}g_{12}=0 \\ 1+h_{22}g_{22}+h_{23}g_{23}=0 \\ 1+h_{23}g_{33}=0 \\ 1+h_{34}g_{14}=0 \\ 1+h_{33}g_{23}=0 \\ 1+h_{33}g_{33}=0 \end{cases} \quad (6)$$

It is again straightforward to check that this system has no solution over $\mathbb{F}_q$ for all q. Hence there is no a linear code C in $\mathbb{F}_q^5$ for the access structure Γ. □

For the next example, one can imagine that there are two companies A and B. The administrators of company A are players $1,2,3$ and administrators of company B are players $4,5,6$. They plan to start a joint venture project. The project can be executed only if majority of the administrators of each company agree. Hence the following model could be useful for this situation. Generally, sets A and B may have more elements.

Example 4. Let

$$\begin{aligned}\Gamma \;=\; & \{(1,2,4,5),(1,2,4,6),(1,2,5,6),(1,3,4,5),(1,3,4,6), \\ & (1,3,5,6),(2,3,4,5),(2,3,4,6),(2,3,5,6)\}.\end{aligned}$$

Then

$$\begin{aligned}\mathcal{R} \;=\; & \{(1,2,3,4),(1,2,3,5),(1,2,3,6),(1,4,5,6),(2,4,5,6), \\ & (3,4,5,6)\}.\end{aligned}$$

Let

$$\mathbb{H}=\begin{pmatrix} 1 & h_{11} & h_{12} & 0 & h_{14} & h_{15} & 0 \\ 1 & h_{21} & h_{22} & 0 & h_{24} & 0 & h_{26} \\ 1 & h_{31} & h_{32} & 0 & 0 & h_{35} & h_{36} \\ 1 & h_{41} & 0 & h_{43} & h_{44} & h_{45} & 0 \\ 1 & h_{51} & 0 & h_{53} & h_{54} & 0 & h_{56} \\ 1 & h_{61} & 0 & h_{63} & 0 & h_{65} & h_{66} \\ 1 & 0 & h_{72} & h_{73} & h_{74} & h_{75} & 0 \\ 1 & 0 & h_{82} & h_{83} & h_{84} & 0 & h_{86} \\ 1 & 0 & h_{92} & h_{93} & 0 & h_{95} & h_{96} \end{pmatrix},$$

$$\mathbb{G}=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & g_{15} & g_{16} \\ 1 & 0 & 0 & 0 & g_{24} & 0 & g_{26} \\ 1 & 0 & 0 & 0 & g_{34} & g_{35} & 0 \\ 1 & 0 & g_{42} & g_{43} & 0 & 0 & 0 \\ 1 & g_{51} & 0 & g_{53} & 0 & 0 & 0 \\ 1 & g_{61} & g_{62} & 0 & 0 & 0 & 0 \end{pmatrix},$$

where $h_{ij}\in\mathbb{F}_q^*$ for $1\le i\le 9, 1\le j\le 6$, and $g_{ij}\in\mathbb{F}_q$ for $1\le i\le 6, 1\le j\le 6$.

The general solution is of the form in F_q: $h_{11}=h_{21}=h_{31}=g_{51}^{-1}$, $h_{12}=h_{22}=h_{32}=g_{42}^{-1}$, $h_{41}=h_{51}=h_{61}=g_{61}^{-1}$, $h_{43}=h_{53}=h_{63}=g_{43}^{-1}$, $h_{72}=h_{82}=h_{92}=g_{62}^{-1}$, $h_{73}=h_{83}=h_{93}=g_{53}^{-1}$, $h_{14}=h_{44}=h_{74}=g_{24}^{-1}$, $h_{15}=h_{45}=h_{75}=g_{15}^{-1}$, $h_{24}=h_{54}=h_{84}=g_{34}^{-1}$, $h_{26}=h_{56}=h_{86}=g_{16}^{-1}$, $h_{35}=h_{65}=h_{95}=g_{35}^{-1}$, $h_{36}=h_{66}=h_{96}=g_{26}^{-1}$ where $1+h_{11}g_{61}+h_{12}g_{62}=0$, $1+h_{21}g_{61}+h_{22}g_{62}=0$, $1+h_{31}g_{61}+h_{32}g_{62}=0$, $1+h_{41}g_{51}+h_{43}g_{53}=0$, $1+h_{51}g_{51}+h_{53}g_{53}=0$, $1+h_{61}g_{51}+h_{63}g_{53}=0$, $1+h_{72}g_{42}+h_{73}g_{43}=0$, $1+h_{82}g_{42}+h_{83}g_{43}=0$, $1+h_{92}g_{42}+h_{93}g_{43}=0$, $1+h_{14}g_{34}+h_{15}g_{35}=0$, $1+h_{44}g_{34}+h_{45}g_{35}=0$, $1+h_{74}g_{34}+h_{75}g_{35}=0$, $1+h_{24}g_{24}+h_{26}g_{26}=0$, $1+h_{54}g_{24}+h_{56}g_{26}=0$, $1+h_{84}g_{24}+h_{86}g_{26}=0$, $1+h_{35}g_{15}+h_{36}g_{16}=0$, $1+h_{65}g_{15}+h_{66}g_{16}=0$, $1+h_{95}g_{15}+h_{96}g_{16}=0$.

When $q=2$, the polynomial system (4) becomes a linear system for $\mathbb{G}$, as the nonzero entries of $\mathbb{H}$ must all be 1. Hence the system can be solved by Gauss elimination. Therefore, given an access structure Γ, if the adversary structure $\mathcal{R}$ is found, then one decide in polynomial time (in terms of the sizes of Γ and $\mathcal{R}$) where there is a linear code over $\mathbb{F}_2$ to realize Γ.

IV. Improvement on Adversary Structure

Since $C^\perp$ is the row span space of $\mathbb{H}$. We consider the following definition.

Definition 1[7] *A subset $R\subseteq[1,n]$ is called a real rejected set of C if there is no $\mathbf{y}\in C^\perp$ such that $y_0=1$ and $supp(\mathbf{y})\setminus\{0\}\subseteq R$. A real rejected set R is called a maximal real rejected set if any set R' with $R\subset R'$ can recover the secret.*

According to this above definition, it is obvious that some subsets $R_{i_1},...,R_{i_t}$ in $\mathcal{R}$ are rejected sets because it is impossible for each R_{i_j} $(j=1,2,...,t)$ that there is a codeword $\mathbf{c}\in C^\perp$ such that $supp(\mathbf{c})\setminus\{0\}\subseteq R_{i_j}$. Hence, we only consider a smaller adversary structure called as real adversary structure $\mathcal{R}(C)$ in which each element R maybe satisfy that there is a codeword $\mathbf{c}\in C^\perp$ such that $c_0=1$ and $supp(c)\setminus\{0\}\subseteq R$.

In this section, we will proposed an algorithm to find $\mathcal{R}(C)$.

A. Definition of Real Adversary Structure

Since $C^\perp$ is the row span space of $\mathbb{H}$, any vector $\mathbf{y}\in C^\perp$ is of the form:

$$\mathbf{y}=(y_0,y_1,...,y_n)=(\sum_{i=1}^m k_i,\sum_{i=1}^m k_ih_{i1},...,\sum_{i=1}^m k_ih_{in}) \quad (7)$$

Let $B=\{i_1,i_2,...,i_t\}\subseteq[1,m]$ and $2\le t\le m$. We use $\mathbb{H}_B$ denotes a sub-matrix of $\mathbb{H}$ which is composed of all rows of $\mathbb{H}$ indexed by B, that is,

$$\mathbb{H}_{\mathbf{B}}=\begin{pmatrix} 1 & h_{i_11} & h_{i_12} & \dots & h_{i_1n} \\ 1 & h_{i_21} & h_{i_22} & \dots & h_{i_2n} \\ & & \dots & & \\ 1 & h_{i_t1} & h_{i_t2} & \dots & h_{i_tn} \end{pmatrix}=\begin{pmatrix} \mathbf{h}_{i_1} \\ \mathbf{h}_{i_2} \\ \dots \\ \mathbf{h}_{i_t} \end{pmatrix}. \quad (8)$$

Definition 2. *(Possible Vector of $\mathbb{H}_B$). We call a row vector*

$$\mathbf{y}=(y_0,y_1,...,y_n)=(\sum_{i\in B}k_i,\sum_{i\in B}k_ih_{i1},...,\sum_{i\in B}k_ih_{in})$$

as a possible vector of $\mathbb{H}_B$ where $k_i\in F_q^*$ for $i\in B$.

Definition 3. *(Candidate Accepted Vector of $\mathbb{H}_B$). We call a possible vector $\mathbf{y}=(1,y_1,...,y_n)$ of $\mathbb{H}_B$ as candidate accepted vector of $\mathbb{H}_B$ if $\mathbf{y}$ does not cover any one of vectors $\mathbf{h}_{i_1},...,\mathbf{h}_{i_t}$.*

Definition 4. *(Maximal Candidate Accepted Vector of $\mathbb{H}_B$). A candidate accepted vector $\mathbf{y}=(1,y_1,...,y_n)$ of $\mathbb{H}_B$ is called maximal candidate accepted vector of $\mathbb{H}_B$ if for each i with*

$y_i = 0$, *and there are at least two non-zero entries in the ith column of* $\mathbb{H}_B$, *then there is* $j \in B$ *such that* $supp(\mathbf{h}_j) \subseteq supp(\mathbf{y}) \bigcup \{i\}$.

Let V_{MB} be the set of all maximal candidate accepted vectors of $\mathbb{H}_B$.

Definition 5. *((Maximal) Candidate Accepted Set). A set* $S_{\mathbf{y}}$ *is called as candidate accepted set if* $\mathbf{y}$ *is a candidate accepted vector. A candidate accepted set* $S_{\mathbf{y}}$ *is called as maximal candidate accepted set if* $\mathbf{y}$ *is a maximal candidate accepted vector.*

Let $R_{MB} = \{S_{\mathbf{c}} | \mathbf{c} \in V_{MB}\}$.

Definition 6. *For any* $B \subseteq [1, m]$ *with* $|B| \geq 2$, *let* R'_{MB} *consist of elements in* R_{MB} *that do not contain any one of* $S_1, ..., S_m$. *Let*

$$\mathcal{R}(C) = \cup_{B \subseteq [1,m], |B| \geq 2} R'_{MB}.$$

$\mathcal{R}(C)$ *is called as real adversary structure of* Γ *from* $C^{\perp}$.

Example 5. *Assume access structure* $\Gamma = \{(1,2,3),(3,4,5),(3,5,6)\}$ *in a secret sharing scheme with participants* $\{1,2,3,4,5,6\}$. *Hence* $\mathbb{H}$ *is of the form*

$$\mathbb{H} = \begin{pmatrix} 1 & a_1 & a_2 & a_3 & 0 & 0 & 0 \\ 1 & 0 & 0 & b_1 & b_2 & b_3 & 0 \\ 1 & 0 & 0 & c_1 & 0 & c_2 & c_3 \end{pmatrix}. \quad (9)$$

According to Definition 6, $\mathcal{R}(C) = \{(1,2,4,5,6),(3,4,6)\}$. *Comparing with Example 1,* $|\mathcal{R}(C)| \leq |\mathcal{R}|$.

B. Construction of Real Adversary Structure

Definition 7.*A matrix* M *is called decomposable if there is a row and column permutation transforming* M *into the following form:*

$$M = \begin{pmatrix} M_1 & \mathbf{0} \\ \mathbf{0} & M_2 \end{pmatrix}$$

where each $M_i (i = 1, 2)$ *has at least one non-zero row and* $\mathbf{0}$ *denotes a all-*$\mathbf{0}$ *matrix. Otherwise* M *is called indecomposable.*

By permuting rows and columns, $\mathbb{H}$ can be transformed into the following form:

$$\mathbb{H} = \begin{pmatrix} \mathbf{1} & \Gamma_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \Gamma_2 & \dots & \mathbf{0} \\ & & \dots & & \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \dots & \Gamma_t \end{pmatrix}, \quad (10)$$

where each Γ_i are indecomposable sub-matrixes for $1 \leq i \leq t$.

Definition 8.*Define* $E \oplus F = \{Z | Z = X \cup Y, X \in E, Y \in F\}$, *where* E *and* F *are any two collects of sets.*

Theorem 3. *Suppose*

$$\Gamma = \begin{pmatrix} \Gamma_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \Gamma_2 & \dots & \mathbf{0} \\ & & \dots & \\ \mathbf{0} & \mathbf{0} & \dots & \Gamma_t \end{pmatrix}, \quad (11)$$

and every $\Gamma_i (1 \leq i \leq t)$ *is indecomposable. If* $\mathcal{T}, \mathcal{T}_1, ..., \mathcal{T}_t$ *are real adversary structure of access structure* $\Gamma, \Gamma_1, ..., \Gamma_t$ *respectively, then* $\mathcal{T} = \mathcal{T}_1 \oplus \mathcal{T}_2 \oplus \cdots \oplus \mathcal{T}_t$.

Proof: Let Γ_i be only related with the i_1-th, ..., i_{s_i}-th columns of Γ for $1 \leq i \leq t$, where $s_1 + s_2 + ... + s_t = n$.

Assume any $S \in \mathcal{T}_1 \oplus \mathcal{T}_2 \oplus \cdots \oplus \mathcal{T}_t$, that is, $S = S_1 \cup S_2 \cup \cdots \cup S_t$ and each $S_i \in \mathcal{T}_i$ for $i = 1, 2, ..., t$. Obviously, $S \subset [1, n]$ is a candidate accepted set because it is independent between any S_i and S_j. At the same time, S must be a maximal candidate accepted set, otherwise, then there exists at least a $j \in \overline{S}$ such that $S \cup \{j\}$ is a candidate accepted set, hence j is related with some Γ_i, that is, there exists some S_i such that $S_i \cup \{j\}$ is a candidate accepted set which is contrary to this case that S_i is a maximal candidate accepted set. So $S \in \mathcal{T}$.

Assume any $S \in \mathcal{T}$, then S can be divided into $S = S_1 \cup S_2 \cup \cdots \cup S_t$, where $S_i \subseteq \{i_1, ..., i_{s_i}\}$. Because all participants in S cannot reconstruct the secret, hence all participants in each S_i can not also do it.

If some S_i is only a candidate accepted set, but not in $\mathcal{T}_i$, i.e., it is not a maximal candidate accepted set, however, other $S_j \in \mathcal{T}_j, j \neq i$. For set $\{i_1, ..., i_{s_i}\}$, there must exist a subset $S' \subset \{i_1, ..., i_{s_i}\}$ such that $S' \cup S_i \in \mathcal{T}_i$, hence $S_1 \cup \cdots \cup S' \cup S_i \cup \cdots \cup S_t$ also is a maximal candidate accepted sets, it is contrary to $S = S_1 \cup S_2 \cup \cdots \cup S_t \in \mathcal{T}$. So, each $S_i \in \mathcal{T}_i$, for $i = 1, 2, ..., t$.

That is, if any $S \in \mathcal{T}$, then $S \in \mathcal{T}_1 \oplus \mathcal{T}_2 \oplus \cdots \oplus \mathcal{T}_t$. □

Hence, it is reduced to construct real adversary structure of indecomposable matrix Γ_i when we try to find real adversary structure of Γ.

Let $A_i = \{j | 1 \leq j \leq n, |supp(\mathbf{z}_j)| = i\}$, where z_j is the jth column of $\mathbb{H}_B$. Obviously, $\sum_{i=0}^{m} |A_i| = n$.

Lemma 5. *For any* $\mathbb{H}_B$, *if* $l \in A_1$, *the participant* P_l *must belong to every element in generating adversary structure of* $\mathbb{H}_B$.

Proof: Assume $\mathbf{y} = (1, y_1, ..., y_n)$ is a possible vector of $\mathbb{H}_B$, then the lth component of $\mathbf{y}$ can be computed from $y_l = \sum_{j=1}^{t} k_j h_{i_j l}$. Because $k_1, ..., k_t \in F_q^*$, and only one of $h_{i_1 l}, ..., h_{i_t l}$ does not equal 0, hence $y_l \neq 0$. □

Theorem 4. *If* B *is overlayed by* $T_1 \cup T_2$, *but not by any proper subset of* $T_1 \cup T_2$, *then* $\overline{T_1 \cup T_2} \in \mathcal{T}_B$, *where* $T_1 \cap A_1 = \emptyset$ *and* $T_2 \cap A_1 = \emptyset$. *Every element in* $\mathcal{T}_B$ *can be obtained by this way.*

Proof: For any $k \in T_1 \cup T_2$ and $k \notin A_0$, $T_1 \cup T_2 \setminus \{k\}$ does not overlay B, $\overline{T_1 \cup T_2} \cup \{k\}$ contains at least one $S_j \in \Gamma$ where $j \in B$. That is, $\overline{T_1 \cup T_2}$ is a candidate accepted set, but $\overline{T_1 \cup T_2} \cup \{k\}$ is not a candidate accepted set for any $k \in T_1 \cup T_2$, i.e., $k \notin \overline{T_1 \cup T_2}$, hence $\overline{T_1 \cup T_2}$ is in $\mathcal{T}_B$ according to the definition of maximal candidate accepted set.

$T_1 \cap A_1 = \emptyset$ and $T_2 \cap A_1 = \emptyset$ hold from Lemma 5.

On the other hand, if $S \in \mathcal{T}_B$, then $\overline{S}$ must overlay B from Lemma 3. Now, assume there exists a proper subset $\overline{S'} \subset \overline{S}$ such that $\overline{S'}$ overlays B, then S' is a generating candidate set of $\mathbb{H}_B$. However, $S \subset S'$ is contrary to this case S is a maximal candidate accepted set. That is, if S is a maximal rejected set of $\mathbb{H}_B$, then it must be generated by a set T which overlays B, however, B is not overlayed by any proper subset of T. □

Now, we will provide an algorithm to generate $\mathcal{R}(C)$ for any access structure Γ.

Assume access structure Γ is decomposable and is composed of $\Gamma_1, ..., \Gamma_t$, where each Γ_i is indecomposable for

$i = 1, ..., t$.

Algorithm: Finding $\mathcal{R}(C)$ from Γ.

1) Construct real adversary structure $\mathcal{T}_i$ for Γ_i.
   a) Assume that $\mathbb{H}_i = (\mathbf{1}\,\Gamma_i)$ is an $m_i \times (n_i+1)$ matrix, for simplicity we denote its rows and columns by using symbols $\{r_1, r_2, ..., r_{m_i}\}$ and $\{0, l_1, ..., l_{n_i}\}$ respectively, where column 0 denotes the first column of $\mathbb{H}_i$, $\sum_{i=1}^{t} m_i = m$ and $\sum_{i=1}^{t} n_i = n$. $\mathbb{H}_{i_B}$ is a sub-matrix of $\mathbb{H}_i$ which is composed of all rows of $\mathbb{H}_i$ indexed by B which is a subset of $\{r_1, r_2, ..., r_{m_i}\}$ and $2 \le t(= |B|) \le m_i$.
   b) The following algorithm will generate $\mathcal{T}_{i_B}$ of $\mathbb{H}_{i_B}$ (initially $\mathcal{T}_{i_B}$ is empty. Assume
   $$A_j = \{l_k | k \in \{1, ..., n_i\}, |supp(\mathbf{s}_k)| = j\}$$
   where column vector $\mathbf{s}_k$ is the kth column of $\mathbb{H}_{i_B}$.
      i) If $A_t \neq \emptyset$, then add $\{l_1, ..., l_{n_i}\} \setminus \{j\}$ to $\mathcal{T}_{i_B}$ for each $j \in A_t$.
      ii) Assume $A_{t-j} \neq \emptyset$. If $j = 1, ..., t-3$ and $T_1 \subseteq A_{t-j}, T_2 \subseteq A_2 \cup ... \cup A_{t-j-1}$, add $\{l_1, ..., l_{n_i}\} \setminus T_1 \cup T_2$ to $\mathcal{T}_{i_B}$, or if $j = t-2$ and $T_1 \subseteq A_2, T_2 \subseteq A_2$, then add $\{l_1, ..., l_{n_i}\} \setminus T_1 \cup T_2$ to $\mathcal{T}_{i_B}$, where B is overlayed by $T_1 \cup T_2$ but not by any proper subset of $T_1 \cup T_2$, and $|T_1| \ge 1$.
   c) Construct $\mathcal{T}_i$. Assume $\mathcal{T}_{i_B} = \mathcal{T}'_{i_B} \cup D$, where any $b \in \mathcal{T}'_{i_B}$ must not include any set $S_{\mathbf{y}}$ where $\mathbf{y}$ is any one row vector of H_i, then
   $$\mathcal{T}_i = \cup_{\substack{B \subseteq [1, m_i] \\ |B| \ge 2}} \mathcal{T'}_{i_B}.$$
2) Construct $\mathcal{R}(C)$ for Γ. According to Theorem 3, $\mathcal{R}(C) = \mathcal{T}_1 \oplus ... \oplus \mathcal{T}_t$.

This algorithm may still have exponential running time when n is large. However, we will find adversary structure $\mathcal{R}(C)$ with smaller size if there exist only one non-zero element in some columns of $\mathbb{H}$. Especially, the size of $\mathcal{R}(C)$ will be smaller if these columns with only one non-zero elements of $\mathbb{H}$ are more.

Let

$$\mathbb{G}_1 = \begin{pmatrix} 1 & g_{11} & g_{12} & \cdots & g_{1n} \\ 1 & g_{21} & g_{22} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & g_{l1} & g_{l2} & \cdots & g_{ln} \end{pmatrix} = \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \cdots \\ \mathbf{g}_l \end{pmatrix}, \quad (12)$$

where $g_{ij} = 0$ if $j \in R_i$ and $\mathcal{R}(C) = \{R_1, R_2, ..., R_l\}$.

Corollary 1. *There is a linear code for a given access structure $\Gamma = \{S_1, ..., S_m\}$ if and only if the following system of quadratic equations*

$$\mathbb{G}_1 \mathbb{H}^\top = \mathbf{0}, \quad (13)$$

has a solution for h_{ij}, $j \in S_i$, and g_{ij}, $j \notin R_i$, over $\mathbb{F}_q$ with $h_{ij} \neq 0$ for $j \in S_i$.

Example 6. *(Continued Example 2)*

Answer: According to Theorem 4, $\mathcal{R}(C) = \{(1, 2, 4, 5, 6), (3, 4, 6)\}$.

Let

$$\mathbb{H} = \begin{pmatrix} 1 & h_{11} & h_{12} & h_{13} & 0 & 0 & 0 \\ 1 & 0 & 0 & h_{23} & h_{24} & h_{25} & 0 \\ 1 & 0 & 0 & h_{33} & 0 & h_{35} & h_{36} \end{pmatrix},$$

$$\mathbb{G}_1 = \begin{pmatrix} 1 & 0 & 0 & g_{13} & 0 & 0 & 0 \\ 1 & g_{21} & g_{22} & 0 & 0 & g_{25} & 0 \end{pmatrix},$$

where $h_{ij} \in F_q^*$ for $1 \le i \le 3, 1 \le j \le 6$, and $g_{ij} \in F_q$ for $1 \le i \le 2, 1 \le j \le 6$.

According to Corollary 1, we obtain the following equations.

$$\begin{cases} 1 + h_{13} g_{13} = 0 \\ 1 + h_{11} g_{21} + h_{12} g_{22} = 0 \\ 1 + h_{23} g_{13} = 0 \\ 1 + h_{25} g_{25} = 0 \\ 1 + h_{33} g_{13} = 0 \\ 1 + h_{35} g_{25} = 0 \end{cases} \quad (14)$$

Obviously, Equations 14 has solutions in any finite field F_q.$\square$

Since $|\mathcal{R}(C)| \le |\mathcal{R}|$, the matrix $\mathbb{G}_1$ determined by $\mathcal{R}(C)$ is much less than the matrix $\mathbb{G}$ determined by $\mathcal{R}$. Hence, it is easier to resolve equation 12 than to resolve equation 4.

V. The Optimal Linear Code

In Section III, we solve this problem that how to construct an ideal linear code realizing given access structure Γ if it exists, however, how can we gain the optimal linear code realizing given access structure if there does not exist an ideal linear code? In this section, we will propose an algorithm to find the optimal linear code realizing given access structure.

A. An Algorithm to Find the Optimal Linear Code

For given access structure Γ, how can we obtain the optimal linear code if there does not exist an ideal linear code realizing it? that is, how can we obtain the optimal linear code realizing Γ if there is no solution for quadratic equations (4)?

In an ideal linear code, each participant in Γ "owns" an only component of a code, hence he "owns" an only corresponding column of generator matrix $\mathbb{G}$ and check matrix $\mathbb{H}$. In the optimal linear code, each participant in Γ "owns" some components of a code, as a result, he "owns" some corresponding columns of $\mathbb{G}$ and $\mathbb{H}$. However, the generator matrix $\mathbb{G}$ and check matrix $\mathbb{H}$ of the optimal linear code realizing Γ still satisfies quadratic equations (4), hence,we can obtain the following algorithm which can find the optimal linear code realizing Γ.

Algorithm: *The optimal linear code realizing* Γ.

1) Adding to a column in matrixes $\mathbb{G}$ and $\mathbb{H}$ respectively, we obtain two matrixes $\mathbb{G}_1$ and $\mathbb{H}_1$ with $n+2$ columns. We emphasis that the new column is the ith column of $\mathbb{G}_1$ and $\mathbb{H}_1$ respectively, furthermore, the ith column has same forms with the $(i+1)$th column in $\mathbb{G}_1$ and $\mathbb{H}_1$ respectively for every $i = 2, 3, ..., n$. Two columns have same forms if their elements satisfies restrictions in Theorem 2.
   There exists a linear code with length $n+2$ realizing Γ if the system of quadratic equations $\mathbb{G}_1 \mathbb{H}_1^T = 0$ has a solution. There is an output which is a linear code realizing Γ.
2) If there does not exist solution of $\mathbb{G}_1 \mathbb{H}_1^T = 0$, two columns are added up in matrixes $\mathbb{G}$ and $\mathbb{H}$ which are changed into two matrixes $\mathbb{G}_2$ and $\mathbb{H}_2$ with length $n+3$

respectively. New two columns have same forms with two columns or one column of $\mathbb{G}$ and $\mathbb{H}$ respectively.
There exists a linear code with length $n+3$ realizing Γ if the system of quadratic equations $\mathbb{G}_2\mathbb{H}_2^T = 0$ has a solution. There is an output which is a linear code realizing Γ.

3) Suppose there does not exist solution of $\mathbb{G}_i\mathbb{H}_i^T = 0$, where matrixes $\mathbb{G}_i$ and $\mathbb{H}_i$ are obtained by being added up i columns from matrixes $\mathbb{G}$ and $\mathbb{H}$ respectively. $i+1$ columns are added up in matrixes $\mathbb{G}$ and $\mathbb{H}$ which are changed into two matrixes $\mathbb{G}_{i+1}$ and $\mathbb{H}_{i+1}$ with $n+i+2$ columns respectively. New $i+1$ columns have same forms with $i+1$ columns, or i columns, ..., or one column of $\mathbb{G}$ and $\mathbb{H}$ respectively.
There exists a linear code with length $n+i+2$ realizing Γ if the system of quadratic equations $\mathbb{G}_{i+1}\mathbb{H}_{i+1}^T = 0$ has a solution. There is an output which is a linear code realizing Γ.
4) repeating the step 3, and obtaining a linear code realizing Γ until the system of quadratic equations $\mathbb{G}_{i+1}\mathbb{H}_{i+1}^T = 0$ has a solution for some i.

Remarks: in order to obtain the optimal linear code, 1) in step 2, let new two columns have same forms with two columns of $\mathbb{G}$ and $\mathbb{H}$ respectively, then new two columns have same forms with one column of $\mathbb{G}$ and $\mathbb{H}$ respectively if there is not a linear code when two columns have forms of two columns.

2) In step 3, let new $i+1$ columns first have forms of $i+1$ columns, then forms of i columns if there is not a linear code for forms of $i+1$ columns, then forms of $i-1$ columns if there is not a linear code for forms of i columns ,..., then same forms if there is not a linear code for forms of 2 columns.

3) In step 3, if new $i+1$ columns have forms of j columns in $\mathbb{G}$ (or $\mathbb{H}$), its information rate is belongs to $\{\frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{i+2}\}$, where $1 \le j \le i+1$. So, we first consider the linear code with information rate $\frac{1}{2}$, then $\frac{1}{3}$, $\cdots$, finally $\frac{1}{i+2}$.

Theorem 5. *Given access structure Γ, the optimal linear code realizing it must can be found from the above algorithm.*
Proof: According to [14], the above algorithm must have outputs which is a linear code realizing Γ. Next, we will prove this linear code is the optimal linear code realizing Γ.

Case 1: If there is an output in step 1, then this output must be the optimal linear code realizing Γ because there is not ideal linear code realizing Γ and our linear code has the shortest length $n+2$. The information rate of the optimal linear code is $\frac{1}{2}$.

Case 2: The linear code with length $n+3$ in step 2 is the shortest among all linear codes realizing Γ because there is not linear code with length $n+1$ and $n+2$ which can realize Γ. We can obtain the optimal linear code according to remark 1, and its information rate is $\frac{1}{2}$ or $\frac{1}{3}$,

Case 3: The linear code with length $n+i+2$ in step 3 is the shortest among all linear codes realizing Γ because there is not linear code with length $j = n+1, n+2, ..., n+i+1$ which can realize Γ. We can obtain the optimal linear code realizing Γ according to remark 2 and remark 3, and its information rate is belongs to $\{\frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{i+2}\}$ □

B. An Example

In this section, we show an example to explain our algorithms. According to Example 3, there is not an ideal linear code realizing $\Gamma = \{(1,2),(2,3),(3,4)\}$ in $\mathbb{F}_q^5$. Now, we will find its optimal linear code according to our algorithm in section 5.1.

According to step 1 of our algorithms in section 5.1, we can obtain $(\mathbb{H}_1, \mathbb{G}_1)$ with the following forms:

$$(a) \quad \mathbb{H}_1 = \begin{pmatrix} 1 & h'_{11} & h_{11} & h_{12} & 0 & 0 \\ 1 & 0 & 0 & h_{22} & h_{23} & 0 \\ 1 & 0 & 0 & 0 & h_{33} & h_{34} \end{pmatrix},$$

$$\mathbb{G}_1 = \begin{pmatrix} 1 & 0 & 0 & g_{12} & 0 & g_{14} \\ 1 & 0 & 0 & g_{22} & g_{23} & 0 \\ 1 & g'_{31} & g_{31} & 0 & g_{33} & 0 \end{pmatrix};$$

$$(b) \quad \mathbb{H}_1 = \begin{pmatrix} 1 & h_{11} & h'_{12} & h_{12} & 0 & 0 \\ 1 & 0 & h'_{22} & h_{22} & h_{23} & 0 \\ 1 & 0 & 0 & 0 & h_{33} & h_{34} \end{pmatrix},$$

$$\mathbb{G}_1 = \begin{pmatrix} 1 & 0 & g'_{12} & g_{12} & 0 & g_{14} \\ 1 & 0 & g'_{22} & g_{22} & g_{23} & 0 \\ 1 & g_{31} & 0 & 0 & g_{33} & 0 \end{pmatrix};$$

$$(c) \quad \mathbb{H}_1 = \begin{pmatrix} 1 & h_{11} & h_{12} & 0 & 0 & 0 \\ 1 & 0 & h_{22} & h'_{23} & h_{23} & 0 \\ 1 & 0 & 0 & h'_{33} & h_{33} & h_{34} \end{pmatrix},$$

$$\mathbb{G}_1 = \begin{pmatrix} 1 & 0 & g_{12} & 0 & 0 & g_{14} \\ 1 & 0 & g_{22} & g'_{23} & g_{23} & 0 \\ 1 & g_{31} & 0 & g'_{33} & g_{33} & 0 \end{pmatrix};$$

$$(d) \quad \mathbb{H}_1 = \begin{pmatrix} 1 & h_{11} & h_{12} & 0 & 0 & 0 \\ 1 & 0 & h_{22} & h_{23} & 0 & 0 \\ 1 & 0 & 0 & h_{33} & h'_{34} & h_{34} \end{pmatrix},$$

$$\mathbb{G}_1 = \begin{pmatrix} 1 & 0 & g_{12} & 0 & g'_{14} & g_{14} \\ 1 & 0 & g_{22} & g_{23} & 0 & 0 \\ 1 & g_{31} & 0 & g_{33} & 0 & 0 \end{pmatrix}.$$

where $h_{ij}, h'_{ij} \in F_q^*$ for $1 \le i \le 3, 1 \le j \le 4$, and $g_{ij}, g'_{ij} \in F_q$ for $1 \le i \le 3, 1 \le j \le 4$.

According to Theorem 2, we obtain the following equation systems (a'), (b'), (c') and (d') for (a), (b), (c) and (d) respectively:

$$(a') \begin{cases} 1 + g_{12}h_{12} = 0 \\ 1 + g_{12}h_{22} = 0 \\ 1 + g_{14}h_{34} = 0 \\ 1 + g_{22}h_{12} = 0 \\ 1 + g_{22}h_{22} + g_{23}h_{23} = 0 \\ 1 + g_{23}h_{33} = 0 \\ 1 + g_{31}h_{11} + g'_{31}h'_{11} = 0 \\ 1 + g_{33}h_{23} = 0 \\ 1 + g_{33}h_{33} = 0 \end{cases}$$

$$(b')\begin{cases} 1+g_{12}h_{12}+g'_{12}h'_{12}=0\\ 1+g_{12}h_{22}+g'_{12}h'_{22}=0\\ 1+g_{14}h_{34}=0\\ 1+g_{22}h_{12}+g'_{22}h'_{12}=0\\ 1+g_{22}h_{22}+g'_{22}h'_{22}+g_{23}h_{23}=0\\ 1+g_{23}h_{33}=0\\ 1+g_{31}h_{11}=0\\ 1+g_{33}h_{23}=0\\ 1+g_{33}h_{33}=0 \end{cases}$$

$$(c')\begin{cases} 1+g_{12}h_{12}=0\\ 1+g_{12}h_{22}=0\\ 1+g_{14}h_{34}=0\\ 1+g_{22}h_{12}=0\\ 1+g_{22}h_{22}+g_{23}h_{23}+g'_{23}h'_{23}=0\\ 1+g_{23}h_{33}+g'_{23}h'_{33}=0\\ 1+g_{31}h_{11}=0\\ 1+g_{33}h_{23}+g'_{33}h'_{23}=0\\ 1+g_{33}h_{33}+g'_{33}h'_{33}=0 \end{cases}$$

$$(d')\begin{cases} 1+g_{12}h_{12}=0\\ 1+g_{12}h_{22}=0\\ 1+g_{14}h_{34}+g'_{14}h'_{34}=0\\ 1+g_{22}h_{12}=0\\ 1+g_{22}h_{22}+g_{23}h_{23}=0\\ 1+g_{23}h_{33}=0\\ 1+g_{31}h_{11}=0\\ 1+g_{33}h_{23}=0\\ 1+g_{33}h_{33}=0 \end{cases}$$

There exist solution for systems (b'),(c')over $\mathbb{F}_q$, and no solution for systems (a'),(d') over $\mathbb{F}_q$, hence there is the optimal linear code with length 6 in $\mathbb{F}_q^6$ for the access structure Γ.

VI. Conclusion

In this paper, we consider existence of ideal linear code for given access structure Γ, and give a method to construct the optimal linear code realizing Γ if there is not an ideal linear code realizing Γ. This is the best work so far in this field.

References

[1] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inf. Theory 44(5) 1998, pp. 2010-2017.
[2] A. Ashikhmin, A. Barg, G. Cohen, and L. Huguet, Variations on minimal codewords in linear codes. Proc. AAECC, 1995, pp.96-105
[3] R.J. Anderson, C. Ding, T. Helleseth, and T. Klove, How to build robust shared control systems. Design, Codes and Cryptography, 15 (1998), pp. 111-124
[4] G.R. Blakley. Safeguarding cryptographic keys. Proc. NCC AFIPS, 1979, pp.313-317
[5] H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. Advances in Crypto 2006, 516-531, 2006
[6] I. Cascudo, H. Chen, R. Cramer and C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication Over Any Fixed Finite Field. Advances in Cryptology -CRYPTO 2009, pp. 466-486, 2009 20.
[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan and V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. EuroCrypto 2007, LNCS 4515, pp. 291-310, 2007
[8] R. Cramer, I. Damgard, R. de Haan. Atomic Secure Multiplication with Low Communication. Advances in Eurocrypt 2007, 291-310, 2007
[9] R. Cramer, I. Damgard, U. Maurer. Efficient General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme. Advances in EURCRYPTO 2000, 316-334, 2000
[10] C. Ding and A. Salomaa. Secret Sharing Schemes with Nice Access Structure. Fundamenta Informaticae. Vol 731-251-63 2006
[11] C. Ding and J Yuan. Covering and Secret Sharing with Linear Codes. DMTCS 2003, 11-25, 2003
[12] S. Goldwasser. Multi-party computations: Past and present. In proceddings of the 16th Annual ACM Symposium on Principles of Distributed Computing, 1997, 1-6
[13] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing any access structure. Proc. IEEE Globecom 87. (1987) 99-102.
[14] M. Karchmer and A. Wigderson. On Span Programes. Proc. 8-th Annual Structure in Complexity Theory Conference, IEEE Computer Society Press, pp. 102-111, 1993.
[15] J.L. Massey. Minimal codewords and secret sharing, Proc. 6th Joint Swedish-Russian Workshop on Information Theory, August 22-27, 1993, pp. 276-279
[16] J.L. Massey. Some applications of coding theory in cryptography, Codes and Ciphers: Cryptography and Coding IV, 1995, pp.33-47
[17] J.L. Massey. Three Coding Problems. Report in Trondhjemsgade 3, 2TH DK-2100 Copenhagen, Denmark, 2009
[18] R.J. McEliece and D.V. Sarwate. On sharing secrets and Reed-Solomon codes, Comm. ACM 24 (1981), pp. 583-584.
[19] W. Ogata and K. Kurosawa. Some new results on nonperfect secret sharing schemes. Technical report of IEICE, Vol 95(423), pp. 45-52, 1995
[20] W. Ogata, K. Kurosawa and S. Tsujii. Nonperfect secret sharing schemes. Advances in Cryptology- AUSCRYPT'92, pp. 56-66, 1993
[21] A. Renvall and C. Ding. The access structure of some secret sharing schemes. Information Security and Privacy, Lecture Notes in Computer Science, Vol. 1172, pp. 67-78, 1996.
[22] A. Shamir. How to share a secret, Comm. ACM 22 (1979), pp 612-613.
[23] J. Yuan and C. Ding, Secret sharing schemes from two-weight codes. The Bose Centenary Symposium on Discrete Mathematics and Applications, Dec 2002.
[24] J. Xu and X Zha. Secret Sharing Schemes with General Access Structure Based on MSPs. Journal of Communications. Vol 2, No 1, 2007.
[25] M. Liu and Z Zhang. Secret Sharing Schemes and Secure Multiparty Computation (Chinese). Publishing House of Electronics Industry. 2008