SOME IDEAL SECRET SHARING SCHEMES

A THESIS
SUBMITTED TO THE DEPARTMENT OF COMPUTER ENGINEERING
AND THE INSTITUTE OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

By
Ramazan Yılmaz
August, 2010

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. A. Aydın Selçuk (Advisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Fazlı Can

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Ahmet Muhtar Güloğlu

Approved for the Institute of Engineering and Science:

Prof. Dr. Levent Onural
Director of the Institute

ABSTRACT

SOME IDEAL SECRET SHARING SCHEMES

Ramazan Yılmaz
M.S. in Computer Engineering
Supervisor: Assist. Prof. Dr. A. Aydın Selçuk
August, 2010

A secret sharing scheme is a method of assigning shares for a secret to some participants such that only authorized coalitions of these participants can recover the secret.

In this work, we study several access structure types: we give an ideal perfect secret sharing scheme for disjunctive multilevel access structures. We introduce joint compartmented access structures, which covers compartmented access structures and conjunctive hierarchical access structures as special cases. We provide an almost surely perfect scheme for those joint compartmented access structures that can be realized by an ideal perfect secret sharing scheme. Lastly, we suggest an alternative threshold secret sharing scheme, and we use this scheme to construct a disjunctive multilevel secret sharing scheme.

Keywords: Secret sharing, ideal perfect secret sharing, hierarchical secret sharing, compartmented secret sharing, threshold secret sharing.

ÖZET

BAZI İDEAL GİZLİLİK PAYLAŞIM ŞEMALARI

Ramazan Yılmaz
Bilgisayar Mühendisliği, Yüksek Lisans
Tez Yöneticisi: Assist. Prof. Dr. A. Aydın Selçuk
Ağustos, 2010

Gizlilik paylaşım şemalari bir takım katılımcılar arasında gizli olan bir değeri sadece bazı koalisyonların bulabileceği şekilde dağıtma yöntemidir.

Bu çalışmada, birçok erişim yapılarını inceledik. Alternatifli hiyerarşik erişim yapıları için ideal ve mükemmel bir çözüm önerdik. Kompartmanlı erişim yapıları ve birleşik hiyerarşik erişim yapılarını da özel durum olarak içine alan kesişebilir kompartmanlı erişim yapılarını tanımladık, ve bu yapılar için ideal ve mükemmel bir paylaşım şeması önerdik. Son olarak da alternatif bir eşik değer gizlilik paylaşım şeması önerdik ve bu şema ile alternatifli hiyerarşik erişim yapılarına yönelik başka bir şema tasarladık.

Anahtar sözcükler: Gizlilik paylaşımı, ideal gizlilik paylaşımı, mükemmel gizlilik paylaşımı, hiyerarşik gizlilik paylaşımı, kompartmanlı gizlilik paylaşımı, eşik değer gizlilik paylaşımı.

Acknowledgement

I acknowledge that the SRG meetings held by Assist. Prof. Dr. A. Aydın Selçuk played a key role in my thesis, since most of the ideas and methodologies followed in this thesis are inspirations from SRG discussions. Especially, I would like to thank Murat Ak, Dr. Kamer Kaya and Kerem Kaşkaloğlu for their contributions to the SRG meetings.

I would also like to thank TÜBİTAK for their financial support during my MSc education.

Contents

List of Figures

Chapter 1

Introduction

A secret sharing scheme is a method of assigning shares for a secret to some participants such that only some coalitions of these participants can find the secret, while other coalitions cannot. Such schemes can be used for sharing a private key that is used for digital signatures, or sharing the key that can be used to decrypt the content of a file. These schemes can also be used for authenticating users by multiple servers in a collaborative manner instead of authanticating them by a single server. It is more difficult for more than one participants to be compromised by an adversary, that's why secret sharing schemes may be useful when there is lack of trust or perfect security in case the secret is saved in a single place.

In this chapter, we will first give a preliminary about secret sharing schemes, which will help the readers to understand later chapters. We will also introduce our notation that will be used throughout this work.

1.1 Participants Set and the Dealer

To share a secret, we need the existence of some participants among whom the secret will be shared. We will call this set as the *participants set* and denote it by P.

While sharing the secret, some computations may have to be performed during the share generation phase. The party —not necessarily be contained in P— that accomplishes such tasks is called the *dealer*. It is assumed that the dealer decides the shares of all participants in P and transmits each participant's private share to him in a secure way.

1.2 Access Structure

Before sharing the secret, some subsets (coalition) of P are marked as qualified; and the dealer performs the secret sharing according to these qualified subsets. The set of all qualified subsets are called the *access structure*, and it is denoted by Γ. The dealer should distribute the shares so that a coalition $W' \notin \Gamma$ cannot find the secret, while another coalition $W \in \Gamma$ can.

We will continue with some important definitions about access structures, then we will mention some important access structure types.

1.2.1 Monotonicity

It is logical that a coalition containing a qualified coalition as a subset is also qualified itself. That property is called the *monotonicity*. An access structure is said to be *monotone* if it satisfies

$$W \in \Gamma, W \subset U \subseteq P \Rightarrow U \in \Gamma$$

for all subsets W and U.

1.2.2 Minimal Access Structure

For a monotone access structure Γ; given a coalition $W \in \Gamma$, we can deduce that all supersets of W are also qualified, i.e. contained in Γ. While defining the access structure, we can write down only W instead of writing it together with all its supersets. The set of all such minimal subsets are called the *minimal access structure.*

More formally, the minimal access structure, denoted by Γ^-, is defined as

$$\Gamma^- = \{W \in \Gamma : \forall W' \subset W, W' \notin \Gamma\}$$

Note that $\Gamma^- \subseteq \Gamma$.

1.3 Ideality

A secret sharing scheme is *ideal* when the size of the shares of all participants are less than or equal to the size of the secret that is shared. If there exists a participant with share that is greater than the secret in size, than that secret sharing scheme is said to be *non-ideal.*

1.4 Perfectness

A secret sharing scheme is said to be *perfect* if

- all qualified coalitions can find the secret, and
- unqualified coalitions gain no information about the secret.

The first condition is clear. For the second coalition; when the participants of an an unqualified coalition W' pool their shares, their knowledge about the secret is the same as their knowledge that they had before pooling their shares. If S denotes the domain of the secret, all values in S are equally likely for the secret in a perfect secret sharing scheme when the participants in $W' \notin \Gamma$ pool their shares.

It is shown that all monotone access structures can be realized by a perfect secret sharing scheme [5], so the important question for an access structure is "Is it possible to find a secret sharing scheme that is ideal and perfect?".

1.5 Special Access Structures

In this section, we will discuss some important access structure types such as threshold access structures, compartmented access structures and multilevel access structures. We will also present notable secret sharing schemes realizing threshold access structures since they are crucial for the following chapters.

1.5.1 Threshold Access Structures

In a *threshold access structure*, the only criterion for a subset to be qualified is its size: if the size of a subset meets the predefined threshold value, than it is qualified. A (t, n) threshold access structure defined over the participants set P of size n is:

$$\Gamma = \{W \subset P : |W| \geq t\}$$

and the minimal access structure is defined as

$$\Gamma^{-} = \{W \subset P : |W| = t\}$$

Threshold access structures were introduced by Shamir [9] and Blakley [2]. Here we describe two threshold secret sharing schemes proposed in [9] and [2].

1.5.1.1 Blakley Threshold Secret Sharing Scheme

In a (t, n) Blakley scheme, the dealer selects a secret point $X = (x_1, x_2, \ldots, x_t)$ from $\mathbb{Z}_p^t$ where p is a prime number. The secret key to be shared is the first coordinate of X, i.e. x_1. Other coordinates of X are random.

For each participant $u \in P$, the dealer selects a random $1 \times t$ vector

$$A_u = (a_{u,1}, a_{u,2}, \ldots, a_{u,t}) \tag{1.1}$$

from $\mathbb{Z}_p^t$, and assigns

$$y_u = A_u X^T = \sum_{i=1}^{t} a_{u,i} x_i$$

as the secret share to y_u. A_u is public.

In other words, the dealer assigns a hyperplane equation that is passing through X to each participant u. When a t-member coalition $W = \{u_1, u_2, \ldots, u_t\}$ is present, they have t hyperplanes passing through X. The linear system formed by the shares of $u_i \in W$ is

$$\begin{bmatrix} A_{u_1} \\ A_{u_2} \\ \vdots \\ A_{u_t} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{bmatrix} = \begin{bmatrix} y_{u_1} \\ y_{u_2} \\ \vdots \\ y_{u_t} \end{bmatrix}$$

or simply

$$M_W X^T = Y_W^T \tag{1.2}$$

for M_W denoting the $t \times t$ coefficient matrix induced by the subset W and Y_W denoting the $1 \times t$ vector formed by the shares of participants included in W. Since all entries in M_W are generated randomly, M_W is nonsingular with an overwhelming probability. W can find the secret by solving the linear system in (1.2).

When a coalition W' of size $t' < t$ is present, $M_{W'}$ will have fewer rows than columns. That is why the row vectors of $M_{W'}$ will not span the $1 \times t$ unit vector

$e_1 = (1, 0, \ldots, 0)$ with an overwhelming probability, and W' will not be able to find the secret.

Note that both the secret and the shares belong to the same domain, so this scheme is ideal.

As stated above, qualified coalitions find the secret and unqulified coalitions gain no information about the secret with an overwhelming probability. Even it has a very small probability, M_W may become singular for a qualified W and W cannot find the secret. Also, an unqualified subset W' may find the secret if its row vectors span e_1 by chance. To prevent this, the dealer needs to check the determinants of exponentially many matrices. That is why Blakley threshold secret sharing scheme is not always perfect.

1.5.1.2 Shamir Threshold Secret Sharing Scheme

The dealer selects a random polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$ of degree $t-1$, for t denoting the threshold of the access structure. The secret to be shared is the constant term of the polynomial, i.e. a_0.

For a participant $u \in P$, the dealer selects a random value $x_u \in \mathbb{Z}_p$, and assigns $y_u = f(x_u)$ as the secret share to u. The x_u value, which is sometimes called the identity of u, is made public.

In this scheme, each participant is given a point over a degree $t-1$ polynomial. When a t-member coalition $W = \{u_1, u_2, \ldots, u_t\}$ is present, they can construct the polynomial $f(x)$ by Lagrange interpolation and find the secret a_0, since they have t points over $f(x)$.

Note that Shamir's threshold secret sharing scheme is a special case of Blakley secret sharing scheme: The linear system of a t-member coalition $W =$

$\{u_1, u_2, \ldots, u_t\}$ in Shamir secret sharing scheme is

$$\underbrace{\begin{bmatrix} 1 & x_{u_1} & x_{u_1}^2 & \ldots & x_{u_1}^{t-1} \\ 1 & x_{u_2} & x_{u_2}^2 & \ldots & x_{u_2}^{t-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_{u_t} & x_{u_t}^2 & \ldots & x_{u_t}^{t-1} \end{bmatrix}}_{M_W} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_{u_1} \\ y_{u_2} \\ \vdots \\ y_{u_t} \end{bmatrix} \tag{1.3}$$

Note that the M_W matrix in (1.3) is equivalent to the M_W matrix in (1.2) if A_u vectors in (1.1) is taken as $a_{u,i} = x_u^{i-1}$ for some identity x_u.

As Blakley threshold secret sharing scheme, Shamir threshold secret sharing scheme is also ideal. Moreover, Shamir threshold secret sharing scheme is perfect since the coefficient matrix M_W in (1.3) is a square Vandermonde matrix when W is qualified. So it is always nonsingular. When an unqualified subset W' of size $t' < t$ is present, the coefficient matrix $M_{W'}$ of their linear system is a Vandermonde matrix with less number of rows than columns, which guarantees that the row vectors of $M_{W'}$ never span e_1.

1.5.2 Compartmented Access Structures

In some cases, it may be desired that qualified coalitions are not dominated by some minorities within the participants set. For this reason, the participants set is partitioned into compartments, and a threshold is assigned to each compartment, in addition to the overall threshold that the size of a coalition needs to reach. Such access structures are called *compartmented access structures*, and introduced in [10].

Let $C_1, C_2, \ldots, C_m$ be m disjoint compartments of P such that $P = \cup_{i=1}^m C_i$. The access structure induced by the threshold values $t, t_1, t_2, \ldots, t_m$ is defined as

$$\Gamma = \{W \subset P : |W| \geq t \text{ and } |W \cap C_i| \geq t_i \ \forall i, 1 \leq i \leq m\}$$

1.5.3 Multilevel (Hierarchical) Access Structures

In a multilevel access structure, the participants set contains nested levels (hierarchies), and each level is assigned a threshold. A coalition W may or may not be qualified according to the number of participants within W that comes from a particular level.

Let m denote the number of levels and L_i denote the set of paricipants contained in the ith level, with $L_i \subset L_j$ if $1 \leq i < j \leq m$. For $t_1 < t_2 < \ldots < t_m$ being the thresholds for the corresponding levels, multilevel access structures are introduced as following in [10]:

$$\Gamma = \{W \subset P : |W \cap L_i| \geq t_i \text{ for some } i, 1 \leq i \leq m\} \tag{1.4}$$

Tassa suggested a similar multilevel access structure in [12] as:

$$\Gamma = \{W \subset P : |W \cap L_i| \geq t_i \ \forall i, 1 \leq i \leq m\} \tag{1.5}$$

Note that a coalition is decided to be qualified or unqualified according to the disjunction of m conditions in (1.4), while a coalition is qualified if it satisfies the conjunction of m conditions in (1.5). To avoid confusion, Tassa named the access structures in (1.4) as *disjunctive multilevel (hierarchical) access structures*, and named the access structures in (1.5) as *conjunctive (hierarchical) multilevel access structures.*

1.6 Notation

P will denote the set of participants. All scalar values and computations are in $\mathbb{Z}_p$ for some large prime p, and vectors are denoted as row matrices, unless otherwise is stated.

Chapter 2

Linear Hierarchical Secret Sharing

In this chapter, we deal with disjuntive hierarchical access structures defined in (1.4), and propose two ideal secret sharing schemes realizing such access structures. The first one is the basic scheme and it is almost surely perfect. We include the basic scheme here to make it easier to understand the second one, which is the extended scheme and always perfect. This chapter is an extension of the work published in [8].

Before describing our schemes, we will introduce our notation and give a background regarding hierarchical secret sharing schemes in the literature.

2.1 Notation

Let P be the set of all participants, and let m nested subsets L_i, $1 \leq i \leq m$ be the levels of a hierarchy satisfying $L_i \subset L_j$ if $i < j$ and $L_m = P$. The access structure is defined as

$$\Gamma = \{W \subset P : |W \cap L_i| \geq t_i \text{ for some } i, 1 \leq i \leq m\}$$

where $0 < t_1 < t_2 < ... < t_{m-1} < t_m$ are the threshold values for the levels.

We will denote the set difference $L_i - L_{i-1}$ with C_i for $1 \leq i \leq m$, with $L_0 = \emptyset$.

The pair (A_u, y_u), with y_u being a scalar and $A_u = (a_{u,1}, a_{u,2}, \ldots, a_{u,t})$ being a vector in t dimensional space $\mathbb{Z}_p^t$, represents the hyperplane

$$a_{u,1}x_1 + a_{u,2}x_2 + \ldots + a_{u,t}x_t = y_u$$

assigned to a participant $u \in P$.

2.2 Literature

Brickell [3] proposed several schemes for hierarchical access structures. The main scheme is based on Shamir secret sharing scheme: The dealer determines t_m random coefficients a_i, $0 \leq i \leq t_m - 1$, with a_0 being equal to the secret. For each level i, the dealer defines Shamir polynomials $f_i(x) = \sum_{j=0}^{t_i-1} a_j x^j$ where t_i is the threshold value for the ith level. For a user $u \in C_i$, the dealer selects a public random value $x_u \in \mathbb{Z}_p$, and assigns $y_u = f_i(x_u)$ as the secret share to u. Note that the secret is the same for all polynomials. The drawback of this scheme is that the nonsingularity of the coefficient matrix M_W for a qualified coalition W is not guaranteed, so the dealer needs to check exponentially many matrices.

Ghodosi et al. [4] studied compartmented and hierarchical access structures, and they proposed a Shamir based secret sharing scheme for hierarchical access structures: For each level i, the dealer selects a polynomial $f_i(x)$. These polynomials are selected such that for a participant $u \in L_i$, $f_j(x_u) = y_u$ for all $i \leq j \leq m$. In this way, u can participate in qualified coalitions of level j for $i \leq j \leq m$. The degrees of the polynomials are defined recursively: the degree of $f_{i+1}(x)$ depends on not only thresholds t_i, but also on the degree of $f_i(x)$ and $|L_{i+1} - L_i|$. Because of this, the scheme is not dynamic. A new participant cannot be added to any level, except the last level, without changing the existing participants' shares.

Tassa [11, 12] proposed another scheme for hierarchical access structures. In this scheme, the dealer selects a degree $t_m - 1$ polynomial $f(x)$ with the secret s as the coefficient of x^{t_m-1} term, and gives values on this polynomial to the participants in the last level of the hierarchy. For the other levels, the dealer takes multiple derivatives of $f(x)$ and uses resulting polynomials for assigning values to the participants. For a user u with identity x_u in the ith level, the dealer computes $f_i(x) = f^{(t_m - t_i)}(x)$ and gives $f_i(x_u)$ as its share to u. Note that all polynomials $f_i(x)$ contains the secret as a coefficient. When any t_i participants from the ith level are present, they have t_i equations with t_i unknowns (coefficients). Solving the linear system is actually identical to a Birkhoff interpolation problem. He suggests to pick the identities of the participants in a monotone manner, in this way the resulting Birkhoff interpolation problem becomes *well posed*, i.e. has a unique solution, and the scheme works without probability of failure. Belenkiy [1] later proposed a very similar scheme.

More recently, *conjunctive* hierarchical access structures and schemes realizing such access structures have been introduced by Tassa [12] and Tassa and Dyn [13], where the previously existing hierarchical access structure model are renamed as *disjunctive*. Hierarchical access structures, we will study in this paper, will be disjunctive.

2.3 Proposed Schemes

In this section, we propose two secret sharing schemes for disjunctive hierarchical access structures. The first scheme, which is almost surely perfect, is based on Blakley secret sharing. The second scheme is an extension of the first one such that it is always perfect. The main contribution of the paper is the extended scheme, and we present the basic scheme essentially as an introduction towards main scheme.

2.3.1 Basic Scheme

2.3.1.1 Share Generation

The dealer selects m random points $X_1, X_2, ..., X_m$ over $\mathbb{Z}_p^{t_m}$ such that the first coordinate of all points are equal to the secret. For each point X_i, the last $t_m - t_i$ coordinates are made public. Only the first t_i coordinates, including the secret, are private.

Let C_i denote the set difference $L_i - L_{i-1}$, with $C_1 = L_1$. For a participant $u \in C_i$, the dealer finds a hyperplane (A_u, y_u) passing through X_j for all $i \leq j \leq m$. A_u is made public and y_u is the private share of u.

For each point X_i, since only the first t_i coordinates are private, a coalition needs to have t_i hyperplanes passing through X_i to solve the private coordinates of it. Since the first coordinate of all points are equal to the secret, qualified coalitions of all levels compute the same secret.

2.3.1.2 Reconstruction

When any t_i participants from L_i come together, they will have t_i hyperplanes passing through X_i. Since only the first t_i coordinates of X_i are private, they will compute X_i by solving the $t_i \times t_i$ linear system they have and find the secret $s = x_{i,1}$.

2.3.1.3 Perfectness

As discussed in Section 1.4 a secret sharing scheme is said to be perfect if

- an unqualified subset gains no information about the secret, and
- a qualified subset can compute the secret.

We show that the proposed scheme is perfect with an overwhelming probability in the following lemmas and theorems.

Lemma 1. *For $1 \leq i < j \leq m$, we have $t_j - t_i \geq j - i$.*

Proof. We have $t_i < t_{i+1} < ... < t_{j-1} < t_j$. So

$$\begin{aligned} t_j - t_{j-1} &\geq 1 \\ t_{j-1} - t_{j-2} &\geq 1 \\ &\vdots \\ t_{i+2} - t_{i+1} &\geq 1 \\ t_{i+1} - t_i &\geq 1 \end{aligned}$$

Adding up the inequalities proves the desired result. □ □

Lemma 2. *In the share generation phase, the degree of freedom of the linear system $X_j A_u^T = y_u$, for $i \leq j \leq m$, which the dealer needs to solve for A_u and y_u for user $u \in C_i$, is at least t_i.*

Proof. In the linear system,

$$\begin{aligned} X_i A_u^T &= y_u \\ X_{i+1} A_u^T &= y_u \\ &\vdots \\ X_m A_u^T &= y_u \end{aligned}$$

we have $t_m + 1$ unknowns to solve in A_u and y_u.

The number of linear equations is $m - i + 1$. Therefore, the degree of freedom is at least $(t_m + 1) - (m - i + 1)$. By Lemma 1, we have $t_m - t_i \geq m - i$; hence the degree of freedom is at least t_i. □ □

Before we prove actual probabilities about the perfectness of the basic scheme, we will first prove lemmas regarding a random matrix's probability of being full-rank.

Let $P^{(p)}_{(m,n)}$, for $m \leq n$, denote the probability of a randomly generated $m \times n$ matrix over $\mathbb{Z}_p$ to be full-rank. We have the following lower bound regarding $P^{(p)}_{(m,n)}$:

Lemma 3.

$$P^{(p)}_{(m,n)} \geq \left(1 - \frac{1}{p}\right)^m .$$

Proof. The first row of a full-rank matrix can be anything except for all zeros; so we have $p^n - 1$ possible choices for the first row. The second row cannot be a scalar multiple of the first row; so we have $p^n - p$ possible choices for the second row. In general, the ith row cannot be a linear combination of the first $i-1$ rows; so we have $p^n - p^{i-1}$ possible choices for the ith row. Therefore, the proportion of full-rank matrices among all $m \times n$ matrices is,

$$\begin{aligned} P^{(p)}_{(m,n)} &= \frac{(p^n-1)(p^n-p)\ldots(p^n-p^{m-1})}{(p^n)^m} \\ &= \frac{p^n-1}{p^n}\frac{p^n-p}{p^n}\cdots\frac{p^n-p^{m-1}}{p^n} \\ &\geq \left(\frac{p^n-p^{m-1}}{p^n}\right)^m \\ &\geq \left(\frac{p^n-p^{n-1}}{p^n}\right)^m \\ &= \left(1-\frac{1}{p}\right)^m . \end{aligned}$$

□ □

Let M be an $m \times n$ matrix over $\mathbb{Z}_p$, for $m \leq n$, such that the first m_1 rows of M are given to be linearly independent and the remaining $m_2 = m - m_1$ rows are generated randomly. Let $P^{(p)}_{(m_1,m_2,n)}$ denote the probability that all the rows of M are linearly independent. We have the following lower bound for $P^{(p)}_{(m_1,m_2,n)}$:

Lemma 4.

$$P^{(p)}_{(m_1,m_2,n)} \geq \left(1 - \frac{1}{p^{n-m+1}}\right)^{m_2} .$$

Proof. For the selection of the (m_1+j)th row, $1 \leq j \leq m_2$, there are $p^n - p^{m_1+j-1}$ possible choices given that the previous (m_1+j-1) rows are linearly independent.

Therefore the proportion of the full-rank M matrices, given the first m_1 rows are linearly independent, is

$$\begin{aligned} P^{(p)}_{(m_1,m_2,n)} &= \prod_{j=1}^{m_2} \frac{p^n - p^{(m_1+j-1)}}{p^n} \\ &\geq \left(\frac{p^n - p^{(m-1)}}{p^n}\right)^{m_2} \\ &= \left(1 - \frac{1}{p^{n-m+1}}\right)^{m_2}. \end{aligned}$$

□ □

Note that Lemma 3 is a special case of Lemma 4 for $m_1 = 0$ and $m_2 = m$.

In the following theorems, for a given participant subset W, l_i denotes $|W \cap L_i|$ and c_i denotes $|W \cap C_i|$.

Theorem 1. *Let W be an unqualified user set of size l, and let P_W denote the probability of W not being able to construct the secret. We have,*

$$P_W \geq (1 - \frac{1}{p})^l.$$

Proof. We will first develop the linear system W has on each level i, $1 \leq i \leq m$, and then develop the system over all levels.

W has l_i equations regarding X_i, for $1 \leq i \leq m$. For $u \in L_i$, if the hyperplane assigned to u is (A_u, y_u), we have

$$A_u X_i^T = y_u \tag{2.1}$$

Since the last $t_m - t_i$ coordinates of X_i are public, this can be written as

$$A'_u X_i'^T = y_u^{(i)} \tag{2.2}$$

where X'_i denotes the $1 \times t_i$ private section of X_i, A'_u is the corresponding, first t_i coefficients in A_u, and

$$y_u^{(i)} = y_u - \sum_{j=t_i+1}^{t_m} a_j x_{i,j} \tag{2.3}$$

for $A_u = (a_1, a_2, \dots, a_{t_m})$. W has l_i such equations for each $1 \leq i \leq m$. When these equations are written in matrix form, W has

$$A^{(i)} X_i^{'T} = Y_i, \tag{2.4}$$

for $1 \leq i \leq m$, where the $l_i \times t_i$ matrix $A^{(i)}$ is formed by the $A_u^{'}$ row vectors in (2.2), and the $l_i \times 1$ column vector Y_i is formed by the $y_u^{(i)}$ values in (2.3).

Let D_i denote the first column of $A^{(i)}$, and E_i denote the remaining $l_i \times (t_i - 1)$ part of $A^{(i)}$. Hence $A^{(i)} = [D_i \ E_i]$. Similarly, $X_i^{'} = [s \ V_i]$, for s denoting the secret and V_i denoting the last $t_i - 1$ coordinates of $X_i^{'}$. Then, (2.4) can be written as

$$[D_i \ E_i][s \ V_i]^T = Y_i.$$

When all equations are combined into a single system, we get:

$$\left[\begin{array}{c|ccccc} \overbrace{D_1}^{1} & \overbrace{E_1}^{t_1-1} & \overbrace{0}^{t_2-1} & \overbrace{0}^{t_3-1} & \dots & \overbrace{0}^{t_m-1} \\ D_2 & 0 & E_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ D_m & 0 & \dots & \dots & 0 & E_m \end{array}\right] \begin{bmatrix} s \\ V_1 \\ V_2 \\ \vdots \\ V_m \end{bmatrix} = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_m \end{bmatrix}$$

The coalition W can compute the secret s if and only if the rows of the coefficient matrix above span the unit vector $(1, 0, \dots, 0)$. That requires the E matrix

$$E = \begin{bmatrix} E_1 & 0 & 0 & \dots & 0 \\ 0 & E_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & E_m \end{bmatrix}$$

to have linearly dependent rows (i.e. is not full-rank). E is not full-rank if and only if E_i is not full-rank for some i.

Therefore, W can find the secret only if E_i is not full-rank for some i. If E_i matrices are all full-rank, then W cannot find the secret. The probability of all E_i matrices being full-rank is bounded from below by $(1 - \frac{1}{p})^l$, as we show in Lemma 5. Hence, $P_W \geq (1 - \frac{1}{p})^l$. □ □

Lemma 5. *For an unqualified coalition W of size l, the probability of all E_i matrices, $1 \leq i \leq m$, to be full-rank is bounded from below by*

$$\left(1 - \frac{1}{p}\right)^{l}.$$

Proof. Let Q_i denote the probability of all E_j matrices obtained by an unqualified W, for $1 \leq j \leq i$, being full-rank.

For the first level, note that the degree of freedom in generation of the hyperplane for a user $u \in C_1$ is at least t_1 by Lemma 2; and the rows of $A^{(1)}$ are of size t_1; therefore, $A^{(1)}$ is completely random. Since E_1 is a submatrix of $A^{(1)}$, it is completely random too. Then by Lemma 3, we have,

$$Q_1 = P^{(p)}_{(l_1,t_1-1)} \geq \left(1 - \frac{1}{p}\right)^{l_1} = \left(1 - \frac{1}{p}\right)^{c_1}. \tag{2.5}$$

For $i \geq 2$, first note that $u \in W \cap L_{i-1}$ implies $u \in W \cap L_i$. We can assume that the first l_{i-1} rows of E_i come from $W \cap L_{i-1}$, and E_i contains E_{i-1} as its upper-left corner submatrix. For R_i denoting the probability that E_i is full-rank given that E_{i-1} is full-rank, we have,

$$Q_i = Q_{i-1} R_i. \tag{2.6}$$

To calculate R_i, note that the degree of freedom in generation of the hyperplane for a user $u \in C_i$ is at least t_i, by Lemma 2, and the rows of $A^{(i)}$ are of size t_i too. Therefore, the rows of $A^{(i)}$, hence the rows of E_i, that come from C_i (i.e. those after E_{i-1}) are completely random. So we have,

$$\begin{aligned} R_i &= P^{(p)}_{(l_{i-1},c_i,t_i-1)} \\ &\geq \left(1 - \frac{1}{p^{(t_i-l_i)}}\right)^{c_i}. \end{aligned}$$

Since we always have $l_i < t_i$ for an unqualified set W, we have,

$$R_i \geq \left(1 - \frac{1}{p}\right)^{c_i} \tag{2.7}$$

By substituting (2.7) in (2.6) recursively with the base case (2.5) for Q_1, and by the fact that $\sum_{j=1}^{i} c_j = l_i$, we get,

$$Q_i \geq \left(1 - \frac{1}{p}\right)^{l_i}.$$

For the particular case $i = m$, we have the result:

$$Q_m \geq \left(1 - \frac{1}{p}\right)^{l_m} = \left(1 - \frac{1}{p}\right)^{l}.$$

□ □

Theorem 2. *Given that an unqualified set W cannot find the secret, W gains no information about the secret.*

Proof. Assume an unqualified set W satisfies $|W \cap L_i| = t_i - 1$ for some i. Let the share of a participant $v \notin W$, $v \in L_i$, be y_v. W has t_i equations regarding X_i, and one of them is $A_v X_i^T = y_v$. When they solve the system of equations, they will have $s = k_1 y_v + k_2$ for some $k_1, k_2 \in \mathbb{Z}_p, k_1 \neq 0$. Hence, all values are possible for the secret for an unknown y_v. The situation is more clear when $|W \cap L_i| < t_i - 1$. □ □

Theorem 3. *For a qualified subset W, let i be the smallest integer satisfying $l_i \geq t_i$, and let $\bar{P}_W$ denote the probability of W being able to construct the secret. We have*

$$\bar{P}_W \geq \left(1 - \frac{1}{p^2}\right)^{l_{i-1}} \left(1 - \frac{1}{p}\right)^{c_i}. \tag{2.8}$$

Proof. We have $l_j < t_j$, for $j < i$, and $l_i \geq t_i$. We will consider only the first l_i participants of W that are in L_i and take $l_i = t_i$, for the sake of simplicity. As in (2.4), W has the linear system

$$A^{(i)} X_i'^T = Y_i$$

with $A^{(i)}$ being of size $t_i \times t_i$ this time. W can compute the secret if $A^{(i)}$ is nonsingular. For the probability of $A^{(i)}$ being nonsingular, we will follow a similar methodology that we followed in Lemma 5 for Theorem 1.

W has a linear system of equations $A^{(j)}X_j'^T = Y_j$ for each level j. Let Q_j' denote the probability of all $A^{(k)}$, $1 \leq k \leq j$, to be full-rank for a given j.

As stated in the proof of Lemma 5, the matrix $A^{(1)}$ is completely random. Then,

$$Q_1' = P_{(l_1,t_1)}^{(p)} \geq \left(1 - \frac{1}{p}\right)^{l_1} = \left(1 - \frac{1}{p}\right)^{c_1}. \tag{2.9}$$

As in the proof of Lemma 5, again, $A^{(j-1)}$ can be seen as the upper-left corner submatrix of $A^{(j)}$. For R_j denoting the probability that $A^{(j)}$ is full-rank given that $A^{(j-1)}$ is full-rank, we have,

$$Q_j' = Q_{j-1}' R_j. \tag{2.10}$$

By Lemma 2, the degree of freedom in generation of the hyperplane for a user $u \in C_j$ is at least t_j, which is equal to the size of the rows of $A^{(j)}$. Therefore, the rows of $A^{(j)}$ that come from C_j (i.e. those after $A^{(j-1)}$) are completely random. Hence,

$$\begin{aligned} R_j &= P_{(l_{j-1},c_j,t_j)}^{(p)} \\ &\geq \left(1 - \frac{1}{p^{(t_j - l_j + 1)}}\right)^{c_j}. \end{aligned}$$

For levels $j < i$, we have $l_j < t_j$. Therefore,

$$R_j \geq \left(1 - \frac{1}{p^2}\right)^{c_j}. \tag{2.11}$$

For level i, which is the first level that the threshold is satisfied, we have $l_i = t_i$, and therefore,

$$R_i \geq \left(1 - \frac{1}{p}\right)^{c_i}. \tag{2.12}$$

By substituting (2.12) and (2.11) in (2.10) with the base case (2.9), and by the fact that $\sum_{j=1}^{i-1} c_j = l_{i-1}$, we get,

$$Q_i' \geq \left(1 - \frac{1}{p^2}\right)^{l_{i-1}} \left(1 - \frac{1}{p}\right)^{c_i}.$$

Clearly, the probability of only $A^{(i)}$ to be full-rank, which is sufficient for W to construct the secret, is greater than or equal to the probability of all $A^{(j)}$ matrices, $1 \leq j \leq i$, to be full-rank. Hence the result follows. □ □

As a final remark for the basic scheme, we would like to note that for $m = 1$ (i.e., when there is only one level of users), the scheme we have proposed here becomes identical to the Blakley threshold secret sharing scheme.

2.3.2 Extended Scheme

The second scheme extends the basic scheme by adding new dimensions to the space worked in: The dealer chooses m points over $\mathbb{Z}_p^t$, where $t = t_m + m - 1$, instead of over $\mathbb{Z}_p^{t_m}$. In this way, the coordinates used to solve the final linear system to recover the secret will be separate from the coordinates solved to arrange that the hyperplane of a user at level i passes through the points $X_i, \ldots, X_m$. Moreover, the hyperplane coefficients for the coordinates used to solve the final linear system are generated in a Vandermonde-like fashion so that the final system will always be nonsingular.

2.3.2.1 Share Generation

The dealer selects m random points over $\mathbb{Z}_p^t$, where the ith point is represented as $X_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,t})$, according to the following conditions:

- The first coordinate of every point X_i, $1 \leq i \leq m$, is equal to the secret; i.e. $x_{i,1} = s$, for all $1 \leq i \leq m$.
- For X denoting the $m \times m$ matrix containing the last $m - 1$ coordinates of

the selected points and -1 as its rows,

$$X = \begin{bmatrix} x_{1,t_m+1} & x_{1,t_m+2} & \dots & x_{1,t} & -1 \\ x_{2,t_m+1} & x_{2,t_m+2} & \dots & x_{2,t} & -1 \\ \dots & \dots & \dots & \dots & \dots \\ x_{m,t_m+1} & x_{m,t_m+2} & \dots & x_{m,t} & -1 \end{bmatrix} \tag{2.13}$$

the matrix X is nonsingular.

As in the basic scheme, the dealer publishes the last $t - t_i$ coordinates of each X_i, $1 \le i \le m$; and the first t_i coordinates, including the secret, are kept private.

Also just as in the basic scheme, for a participant $u \in C_i$, the dealer finds a hyperplane (A_u, y_u) passing through X_j for all $i \le j \le m$. The difference is that, the dealer sets $a_{u,j} = u^{j-1}$, $1 \le u \le |U|$, for $1 \le j \le t_m$, for $A_u = (a_{u,1}, a_{u,2}, \dots, a_{u,t})$. Then y_u and the remaining $m-1$ coordinates of A_u will be selected such that

$$A_u X_j = y_u \tag{2.14}$$

for $i \le j \le m$. Note that the number of equations in this linear system is at most m, and the number of unknowns is m.

The motivation for the first condition of selecting the X_i points is the same as that of the basic scheme. The second condition is needed to guarantee the existence of a solution in (2.14) for the last $m-1$ coordinates of A_u and y_u: Assume $u \in C_i$; then the dealer needs to solve the system,

$$\begin{bmatrix} X_i \\ X_{i+1} \\ \vdots \\ X_m \end{bmatrix} A_u^T = \begin{bmatrix} y_u \\ y_u \\ \vdots \\ y_u \end{bmatrix}$$

to generate the hyperplane (A_u, y_u) for user u. The dealer sets the first t_m coordinates of A_u as $a_{u,j} = u^{j-1}, 1 \le j \le t_m$. Then the system becomes

$$\begin{bmatrix} X_i' \\ X_{i+1}' \\ \vdots \\ X_m' \end{bmatrix} A_u'^T - \begin{bmatrix} y_u \\ y_u \\ \vdots \\ y_u \end{bmatrix} = \begin{bmatrix} b_{u,i} \\ b_{u,i+1} \\ \vdots \\ b_{u,m} \end{bmatrix}$$

where $X_j^{'}$ and $A_u^{'}$ denote the last $m-1$ coordinates of X_j and A_u respectively, and $b_{u,k} = -\sum_{j=1}^{t_m} x_{k,j} u^{j-1}$ for $i \leq k \leq m$. By including y_u in the vector of unknowns, the dealer has the linear system,

$$\underbrace{\begin{bmatrix} X_i^{'} & -1 \\ X_{i+1}^{'} & -1 \\ \vdots & \vdots \\ X_m^{'} & -1 \end{bmatrix}}_{X'} \begin{bmatrix} A_u^{'T} \\ y_u \end{bmatrix} = \begin{bmatrix} b_{u,i} \\ b_{u,i+1} \\ \vdots \\ b_{u,m} \end{bmatrix} \tag{2.15}$$

Note that X' is a submatrix of X in (2.13), and it is just equal to X for $i = 1$. Hence, we have the second condition in the selection of the X_i points during the share generation phase in order to guarantee that the system (2.15) always has a solution for A_u' and y_u.

In the following lemmas, we will show that selecting such m points is an easy process for the dealer, i.e. even a random selection will result in a suitable set of points with an overwhelming probability. Note that the two conditions are independent: the first condition is about the first coordinates of the X_i points, while the second condition regards the last $m-1$ coordinates. We will only examine the probability of X matrix to be nonsingular.

Lemma 6. *The equation*

$$x_1 + x_2 + \ldots + x_k = n$$

has p^{k-1} solutions over $\mathbb{Z}_p^k$, for any value of $n \in \mathbb{Z}_p$.

Proof. We will prove the lemma by induction on k.

Obviously, the equation has only one solution when $k = 1$. For $k = 2$, the solutions for (x_1, x_2) are

$$(0, n), (1, n-1), (2, n-2), \ldots, (p-1, n+1).$$

The lemma holds for $k = 1$ and $k = 2$.

Assuming the lemma holds for $k-1$, we can say that for all possible values of x_1 in $\mathbb{Z}_p$, there exists p^{k-2} solutions for $(x_2, x_3, \ldots, x_k)$. Hence the result follows. □ □

Lemma 7. *The X matrix defined in (2.13) is nonsingular with probability (at least)*

$$\left(1 - \frac{1}{p}\right)^{m-1}$$

if the last $m-1$ coordinates of X_i points are selected randomly.

Proof. We will consider the problem as generating a random $m \times m$ matrix X over $\mathbb{Z}_p$ with the last coordinate of all rows being equal to -1. We will follow a similar methodology to the one in the proof of Lemma 3: linearly dependent vectors for each row will be excluded to find the proportion of nonsingular X matrices over all $p^{m(m-1)}$ possible selections. χ_i will denote the selected vector for the ith row.

Random coordinates of the first row can be anything, since the last entry of the row is already set to -1. All p^{m-1} selections are possible for the first row.

The only unsuitable vector for the second row is χ_1, because there is no other vector that is linearly dependent with χ_1 and contains -1 as its last coordinate. Hence $p^{m-1} - 1$ possible selections exist for the second row.

For the selection of ith row in general, we want to exclude all linear combinations of prior $i-1$ row vectors that has -1 as its last coordinate. In other words, we want to exclude the vectors that can be written as

$$k_1\chi_1 + k_2\chi_2 + \ldots + k_{i-1}\chi_{i-1}$$

for some scalar values $k_1, k_2, \ldots, k_{i-1}$ satisfying

$$\sum_{j=1}^{i-1} k_j = 1.$$

By Lemma 6, there are p^{i-2} such vectors, so there are $p^{m-1} - p^{i-2}$ possible selections for the ith row.

From these, we can conclude that the proportion of suitable X matrices over all $p^{m(m-1)}$ is

$$\begin{aligned} & \frac{p^{m-1}(p^{m-1}-1)(p^{m-1}-p)\dots(p^{m-1}-p^{m-2})}{p^{m(m-1)}} \\ = & \frac{(p^{m-1}-1)(p^{m-1}-p)\dots(p^{m-1}-p^{m-2})}{p^{(m-1)(m-1)}} \\ \geq & \left(\frac{p^{m-1}-p^{m-2}}{p^{m-1}}\right)^{m-1} \\ \geq & \left(1-\frac{1}{p}\right)^{m-1} \end{aligned}$$

□ □

2.3.2.2 Reconstruction

The reconstruction of the secret is the same as that of the basic scheme: When t_i participants $\{u_1, u_2, \dots, u_{t_i}\}$ from L_i come together, they have the linear system

$$\begin{bmatrix} A_{u_1} \\ A_{u_2} \\ \vdots \\ A_{u_{t_i}} \end{bmatrix} X_i^T = \begin{bmatrix} y_{u_1} \\ y_{u_2} \\ \vdots \\ y_{u_{t_i}} \end{bmatrix}$$

Since the last $t - t_i$ coordinates of X_i are public, the system becomes

$$\underbrace{\begin{bmatrix} A'_{u_1} \\ A'_{u_2} \\ \vdots \\ A'_{u_{t_i}} \end{bmatrix}}_{A^{(i)}} X_i'^T = \begin{bmatrix} y^{(i)}_{u_1} \\ y^{(i)}_{u_2} \\ \vdots \\ y^{(i)}_{u_{t_i}} \end{bmatrix} \tag{2.16}$$

for A'_{u_j} and X'_i denoting the first t_i coordinates of A_{u_j} and X_i, respectively. Then $y^{(i)}_{u_j}$ becomes

$$y^{(i)}_{u_j} = y_{u_j} - \sum_{k=t_i+1}^{t} a_{u_j,k} x_{i,k}$$

for $A_{u_j} = (a_{u_j,1}, a_{u_j,2}, \ldots, a_{u_j,t})$.

Since the first $t_m(\geq t_i)$ coordinates of all A_{u_j} vectors are generated in Vandermonde-like fashion, $A^{(i)}$ in (2.16) is a $t_i \times t_i$ Vandermonde matrix. That is why, qualified coalitions of all levels can always find the secret.

Additionally, if desired, Lagrange interpolation can also be used as in Shamir secret sharing: Assume a qualified subset W satisfying $|W \cap L_i| \geq t_i$ for some i is present. Let $f_i(z)$ denote the degree $t_i - 1$ polynomial, $\sum_{j=1}^{t_i} x_{i,j} z^{j-1}$. Since the last $t - t_i$ coordinates of X_i are public, each participant $u \in W$ can compute $f_i(u)$ as $y_u - \sum_{j=t_i+1}^{t} x_{i,j} a_{u,j}$. Since the coalition W has t_i points on polynomial f_i, they can compute $f_i(0) = x_{i,1} = s$.

2.3.2.3 Perfectness

As explained in Section 2.3.2.2, a qualified set will have t_i points over a degree $t_i - 1$ polynomial. Just as in Shamir secret sharing, the coefficient matrix will be a Vandermonde matrix, which is always nonsingular. A qualified subset will always be able to compute the secret uniquely.

When a non-qualified subset W is present, the E_i matrices defined in Section 2.3.1.3 will be truncated Vandermonde matrices, i.e.

$$E_i = \begin{bmatrix} u_1 & u_1^2 & \ldots & u_1^{t_i-1} \\ u_2 & u_2^2 & \ldots & u_2^{t_i-1} \\ \ldots & \ldots & \ldots & \ldots \\ u_{l_i} & u_{l_i}^2 & \ldots & u_{l_i}^{t_i-1} \end{bmatrix}$$

of size $l_i \times t_i - 1$. Since $l_i \leq t_i - 1$, it is always full-rank. Hence, a non-qualified subset will not be able to find the secret. As in the basic scheme, all values in $\mathbb{Z}_p$ will be equally likely for the secret.

We would also like to note that the extended scheme reduces to the Shamir threshold secret sharing scheme when there is only one level, i.e. $m = 1$.

2.3.3 An Efficient Version of the Extended Scheme

The extended scheme is not efficient since the dealer needs to solve a linear system for each participant while sharing the secret. In this section, we will give a special case of the extended scheme such that the dealer can generate the shares easily without solving a linear system.

First of all, note that the participants do not need to know last $m-1$ coordinates of the points X_i and the last $m-1$ coefficients of the hyperplane equations in the extended scheme. A participant $u \in C_i$ actually needs to know $\sum_{k=t_m+1}^{t} a_{u,k}x_{j,k}$ for points X_j, $i \leq j \leq m$. Instead of making the last $m-1$ coeefficients of the hyperplane equations public, the dealer makes $\Delta_u = (\mathit{\Delta}_{u,1}, \mathit{\Delta}_{u,2}, \ldots, \mathit{\Delta}_{u,m})$ public, which are defined as

$$\mathit{\Delta}_{u,j} = \begin{cases} \text{undefined} & \text{if } 1 \leq j \leq i-1 \\ y_u - F_j(u) & \text{if } i \leq j \leq m \end{cases} \tag{2.17}$$

for F_i denoting the degree $t_m - 1$ polynomial

$$F_i(z) = \sum_{j=1}^{t_m} x_{i,j} z^{j-1}.$$

If the dealer finds a valid y_u share for the user u, then the dealer does not need to solve the system in (2.15) for a valid hyperplane (A_u, y_u).

When t_i participants $\{u_1, u_2, \ldots, u_{t_i}\}$ from L_i come together, they will have the linear system

$$\begin{bmatrix} F_i(u_1) \\ F_i(u_2) \\ \vdots \\ F_i(u_{t_i}) \end{bmatrix} X_i'^T = \begin{bmatrix} y_{u_1} - \mathit{\Delta}_{u_1,i} \\ y_{u_2} - \mathit{\Delta}_{u_2,i} \\ \vdots \\ y_{u_{t_i}} - \mathit{\Delta}_{u_{t_i},i} \end{bmatrix}$$

for X_i' denoting the first t_m coordinates of X_i. Remember that only the first t_i coordinates of X_i are private, hence they can find the secret.

We will suggest a special X matrix, defined in (2.13), that allows the dealer to find a valid y_u value easily. Then the dealer will publish Δ_u as defined in (2.17).

For the special $m \times m$ matrix X defined in (2.13), the dealer chooses

$$X = \begin{bmatrix} 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & -1 & -1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & -1 & \dots & -1 & -1 \\ -1 & -1 & \dots & -1 & -1 \end{bmatrix}. \tag{2.18}$$

Note that X is nonsingular, and its inverse is

$$X^{-1} = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 1 & -1 \\ 0 & 0 & 0 & \dots & 1 & -1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & -1 & \dots & 0 & 0 & 0 \\ 1 & -1 & 0 & \dots & 0 & 0 & 0 \\ -1 & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

For a user $u \in C_1$, first t_m coordinates of A_u is set as $a_{u,i} = u^{i-1}$, $1 \leq i \leq t_m$, according to the extended scheme. The last $m-1$ coordinates of A_u, i.e. $A_u^{'}$ in (2.15), and y_u must satisfy

$$X \begin{bmatrix} A_u^{'T} \\ y_u \end{bmatrix} = \begin{bmatrix} -F_1(u) \\ -F_2(u) \\ \vdots \\ -F_m(u) \end{bmatrix}.$$

Then the solution for $A_u^{'}$ and y_u is

$$\begin{bmatrix} a_{u,t_m+1} \\ a_{u,t_m+2} \\ \vdots \\ a_{u,t} \\ y_u \end{bmatrix} = \begin{bmatrix} F_m(u) - F_{m-1}(u) \\ F_{m-1}(u) - F_{m-2}(u) \\ \vdots \\ F_2(u) - F_1(u) \\ F_1(u) \end{bmatrix}.$$

In general, for a user $u \in C_i$, A'_u and y_u must satisfy

$$\overbrace{\begin{bmatrix} 0 & 0 & \dots & 0 & -1 & \dots & -1 \\ 0 & 0 & \dots & -1 & -1 & \dots & -1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -1 & \dots & -1 & -1 & \dots & -1 \\ -1 & -1 & \dots & -1 & -1 & \dots & -1 \end{bmatrix}}^{(m-i+1)\times m} \begin{bmatrix} A'^T_u \\ y_u \end{bmatrix} = \begin{bmatrix} -F_i(u) \\ -F_i + 1(u) \\ \vdots \\ -F_m(u) \end{bmatrix}.$$

The dealer also sets last $i-1$ coordinates of A'_u to 0. Then the system becomes

$$\overbrace{\begin{bmatrix} 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & -1 & -1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & -1 & \dots & -1 & -1 \\ -1 & -1 & \dots & -1 & -1 \end{bmatrix}}^{(m-i+1)\times(m-i+1)} \begin{bmatrix} a_{u,t_m+1} \\ a_{u,t_m+2} \\ \vdots \\ a_{u,t-i+1} \\ y_u \end{bmatrix} = \begin{bmatrix} -F_i(u) \\ -F_i + 1(u) \\ \vdots \\ -F_m(u) \end{bmatrix}$$

which gives the solution

$$\begin{bmatrix} a_{u,t_m+1} \\ a_{u,t_m+2} \\ \vdots \\ a_{u,t-i+1} \\ y_u \end{bmatrix} = \begin{bmatrix} F_m(u) - F_{m-1}(u) \\ F_{m-1}(u) - F_{m-2}(u) \\ \vdots \\ F_{i+1}(u) - F_i(u) \\ F_i(u) \end{bmatrix}.$$

Note that selecting X matrix as in (2.18) always gives $y_u = F_i(u)$ if $u \in C_i$. Then the Δ_u vector defined in (2.17) becomes

$$\mathit{\Delta}_{u,j} = \begin{cases} \text{undefined} & \text{if } 1 \leq j \leq i-1 \\ F_i(u) - F_j(u) & \text{if } i \leq j \leq m \end{cases}$$

In addition to the last $m-1$ coordinates of X_i points that are included in the X matrix, the coordinates $x_{i,t_i+1}, x_{i,t_i+2}, \dots, x_{i,t_m}$ are also public. The dealer can also set these coordinates to 0 for simplicity. Then the F_i polynomials become of degree $t_i - 1$, for $1 \leq i \leq m$.

All these specifications give us the following simple scheme:

The dealer selects m random polynomials $f_i(x)$, $1 \leq i \leq m$, of degree $t_i - 1$ each, such that $f_i(0) = s$ as in Shamir threshold secret sharing for all i, $1 \leq i \leq m$.

For a participant $u \in C_i$, the dealer assigns $y_u = f_i(u)$ as his private share to u, and makes $\varDelta_{u,j} = f_j(u) - f_i(u)$ public for $i \leq j \leq m$. Note that $\varDelta_{u,i} = 0$.

Clearly, when u takes place in a coalition of level $j \geq i$, u has $f_j(u) = y_u + \varDelta_{u,j}$. In this way, a qualified coalition of level j has at least t_j points over a degree $t_j - 1$ polynomial $(f_j(x))$, and recovery of the secret in this scheme becomes equivalent to the recovery of the secret in Shamir threshold secret sharing scheme.

2.4 Comparison to Previous Schemes

Our extended scheme compares favorably to the previous schemes for disjunctive hierarchical secret sharing schemes.

The extended scheme is advantageous over Brickell [3]'s scheme, since his solution needs exponentially many determinant checks to guarantee that the scheme works, while our scheme always works and so does not need any checks of the determinants of the coefficient matrices formed by coalitions.

Ghodosi et al. [4]'s scheme is not dynamic in the sense that a new participant cannot be added to a level without resharing the secret, while new participants can be added to any level in our extended scheme. In addition, the number of unknows that needs to be solved by a qualified coalition is fewer in our scheme than that in Ghodosi et al. 's scheme.

The extended system is equivalent to the scheme proposed by Tassa [11, 12] in terms of the number of unknowns that needs to be solved by a qualified subset. In terms of practicality, our scheme is more advantageous than Tassa's scheme since the selection of the identites are more flexible. To allow new participants to be added, he suggests to leave gaps between the identities: For u_i denoting the maximum identity in C_i and u_{i+1} denoting the minimum identity in C_{i+1}, $u_{i+1} - u_i > g$ allows g more participants to be added later to the ith level. If there are more than g participants to be added to the ith level, then the resulting Birkhoff interpolation may not be well posed. In our scheme, any number of participants can be added to any level given that the total number of participants does not exceed $p - 1$.

2.5 Conclusion

In both schemes, a single hyperplane is assigned to a user $u \in C_i$ which passes through $m - i + 1$ given points. Since there is a single hyperplane equation and a single secret share y_u per user, the scheme is ideal.

In the extended scheme, instead of choosing the points from a t_m dimensional space, we added new dimensions to be used in solving the hyperplane coefficients and increased the number of dimensions to $t_m + m - 1$. By adding these new dimensions, for each user $u \in U$, the dealer can set the first t_m entries of A_u such that the coefficient matrix formed by a qualified subset of participants is always a Vandermonde matrix. This guarantees that the extended scheme is always perfect.

Chapter 3

Joint Compartmented Access Structures

In some cases, it might be desirable that the coalitions are not to be dominated by some participants, and every section of the user population is represented an authorized sets. In such cases, as we have described in Section 1.5.2, the set of participants are partitioned into *compartments*; and in addition to the overall threshold that a coalition's size needs to reach, each compartment is assigned another threshold. A coalition is authorized if and only if the number of participants from each compartment meets its corresponding threshold value, and the size of the overall coalition meets the overall threshold value. Such access structures are called compartmented access structures. They are introduced in [10], and several secret sharing schemes [3, 4, 13] realizing compartmented access structures have been proposed.

In a classical compartmented access structure, the compartments are partitions of the participants set, i.e. they are disjoint. In this chapter, we study the case that the compartments are not necessarily disjoint; i.e. some participants may belong to more than one compartments. We name such an access structure as *joint compartmented access structure*, which contains classical disjoint compartmented access structures and conjunctive hierarchical access structures as special cases. We first discuss under which conditions an ideal perfect secret sharing scheme exists for a joint compartmented access structure, and prove that some joint access structures cannot be realized by an ideal perfect secret sharing scheme. Then we propose an asymptotically perfect and ideal scheme realizing almost all joint compartmented access structures except the ones which are impossible to be realized by an ideal perfect secret sharing scheme.

Before moving on, we will summarize some notable secret sharing schemes from the literature that are related to our work.

Throughout this chapter, the secret is denoted by s, and the share of a participant u is denoted by s_u. We follow the notation introduced in Section 1.5.2 and in Section 1.5.3.

3.1 Background

In this section, we summarize two secret sharing schemes for classical compartmented access structures and one secret sharing scheme for conjunctive hierarchical access structures.

3.1.1 Brickell's Scheme

Brickell [3] proposed the following secret sharing scheme for compartmented access structures: The dealer selects t random values $a_0, a_1, \ldots, a_{t-1}$, where a_0 is the secret. $T = t - \sum_{i=1}^{m} t_i$, $T_i = T + \sum_{j=1}^{i} t_j$ with $T_0 = T$.

For a participant $u \in C_i$, the dealer selects a hyperplane (A_u, y_u) in t dimensional space passing through the point $(a_0, a_1, \ldots, a_{t-1})$, with

$$A_u = (1, x_u, x_u^2, \ldots, x_u^{T-1}, 1, \ldots, 1, \underbrace{x_u^T, \ldots, x_u^{T+t_i-1}}_{\text{coordinates } T_{i-1}+1, \ldots, T_i}, 1, \ldots, 1)$$

for some identity x_u.

This scheme is ideal, but it needs exponentially many checks for perfectness.

3.1.2 Ghodosi et al.'s Scheme

In [4], Ghodosi et al. proposed a Shamir-based secret sharing scheme for the compartmented access structures.

The dealer selects a degree $m-1$ polynomial $f(x)$ with $f(0)=s$, and selects T random values $\beta_0, \beta_1, \ldots, \beta_{T-1}$, where $T = t - \sum_{i=1}^{m} t_i$. The dealer also selects m polynomials $f_i(x)$, $1 \le i \le m$ as

$$f_i(x) = a_{i,0} + a_{i,1}x + \ldots + a_{i,t_i-1}x^{t_i-1} + \beta_0 x^{t_i} + \beta_1 x^{t_i+1} + \ldots + \beta_{T-1}x^{t_i+T-1}$$

with $a_{i,0} = f(i)$. Note that all f_i's have T common coefficients.

This scheme is ideal, but it needs exponentially many checks for perfectness, as in the scheme described in Section 3.1.1.

3.1.3 Selçuk et al.'s Scheme

Selçuk et al. proposed a secret sharing scheme in [7] for conjunctive hierarchical access structures, which is an adaptation of Brickell [3]'s scheme for disjunctive hierarchical access structures, described in Section 2.2.

The dealer selects t_m random values $a_0, a_1, \ldots, a_{t_m-1}$, and sets polynomials $f_i(x)$, $1 \le i \le m$ as

$$f_i(x) = \sum_{j=0}^{t_m-1-t_{i-1}} a_j x^j$$

with $t_0 = 0$ for $f_1(x)$. The secret s is $a_0 + a_1 + \ldots + a_{t_m-1}$.

For a participant $u \in L_i - L_{i-1}$, the dealer selects a random value x_u, and gives $y_u = f_i(x_u)$ as secret share to u.

As previous schemes mentioned here, this scheme is also ideal, but needs exponentially many checks for perfectness.

3.2 Joint Compartmented Access Structures

In this section, we will give the problem and introduce our notation first. Then we will discuss under which conditions an ideal and perfect secret sharing scheme exists. We will see that only some joint compartmented access structures can be realized by an ideal perfect secret sharing scheme. For those kind of access structures, we will propose a linear scheme which is ideal and almost surely perfect. After that, we will include some probabilistic bounds regarding the perfectness of the proposed scheme.

3.2.1 Notation

Let P denote the set of all participants, and let it contain m compartments $C_1, C_2, \ldots, C_m$, not necessarily disjoint. We will call these compartments as *basic compartments*. Each compartment is associated with the threshold t_i.

Let $I^{(m)}$ denote the set of indexes $\{1, 2, \ldots, m\}$. For $I = \{i_1, i_2, \ldots, i_j\} \subset I^{(m)}$, C_I and $C_{i_1,i_2,\ldots,i_j}$ denote the union compartment $\bigcup_{k=1}^{j} C_{i_k}$. Similarly, both t_I and $t_{i_1,i_2,\ldots,i_j}$ denote the threshold for the compartment C_I. Note that a basic compartment is also a union compartment with $|I| = 1$.

Overall, there exists $2^m - 1$ compartments including the union compartments. The threshold may not be specified explicitly for each of these. Given $I = I_1 \cup I_2$, if t_I is not specified, it can be taken as $\max(t_{I_1}, t_{I_2})$ if C_{I_1} and C_{I_2} are not disjoint. If they are disjoint, t_I can be taken as $t_{I_1} + t_{I_2}$. In this way, the dealer can set the thresholds for all $2^m - 1$ compartments and define the access structure as:

$$\Gamma = \{W \subset P : |W \cap C_I| \geq t_I, \forall I \subseteq I^{(m)}, I \neq \emptyset\}.$$

3.2.2 Existence of an Ideal Perfect Solution

In this section, we prove an interesting lemma regarding the existence of an ideal perfect secret sharing scheme when there are two non-nested joint compartments, i.e. C_1 and C_2, and then we will extend this result for arbitrary number of compartments. Before this lemma, we give two definitions and a preposition that will be used in the proof of the lemma.

Definition 1. *Given an unqualified subset W', the participants contained in the set $\{u : u \in P, u \in W - W', \text{for some } W \in \Gamma^-\}$ are critical elements for W'.*

Definition 2. *Two participants u and v are equivalent if $u \in C_i \Leftrightarrow v \in C_i$ for all $1 \leq i \leq m$.*

Assume the secret is shared according to a monotone access structure Γ by an ideal perfect secret sharing scheme. Then the following prepositions hold:

Preposition 1. *Even all of the participants in a subset $W' \notin \Gamma$ pool their shares, all values in $\mathbb{Z}_p$ are possible for the shares of the critical elements for W'.*

Preposition 2. *Assume $W' \notin \Gamma$, but $W' \cup \{u\} \in \Gamma^-$, i.e. u is a critical element for W'. When the participants of W' pool their shares, they can define a bijection f between s_u and the secret s.*

Lemma 8. *For an ideal and perfect secret sharing scheme to exist, the threshold for $C_{1,2}$ needs to satisfy*

$$t_{1,2} \geq t_1 + t_2.$$

given $\max(t_1, t_2) > 1$.

Proof. Assume an ideal perfect secret sharing scheme exists with $t_{1,2} < t_1 + t_2$. WLOG, we can assume $t_1 \geq t_2$. Let $W \in \Gamma^-$ be a subset satisfying

$$\begin{aligned}
|W \cap C_1| &= t_1 \\
|W \cap C_2| &= t_2 \\
W \cap (C_1 - C_2) &\neq \emptyset \\
W \cap (C_1 \cap C_2) &\neq \emptyset \\
(C_1 - C_2) - W &\neq \emptyset \\
(C_2 - C_1) - W &\neq \emptyset
\end{aligned}$$

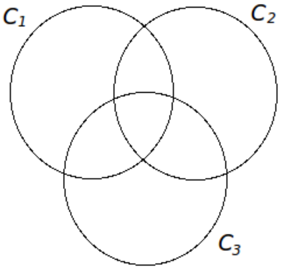

Figure 3.1: A general $m = 3$ case

Let $u_{1,2} \in W \cap C_1 \cap C_2$ and W' denote $W - \{u_{1,2}\}$. When W' is present, they can define a bijection f such that $s_{u_{1,2}} = f(s)$ by Preposition 2.

Let $u_1 \in W \cap (C_1 - C_2)$, and u'_1 be an equivalent participant of u_1 not contained in W, i.e. $u'_1 \in (C_1 - C_2) - W$. Note that W' can define another bijection f_1 such that $s_{u'_1} = f_1(s)$ by Preposition 1 and Preposition 2, since u'_1 is a critical participant for W', and $W_1 = W' \cup \{u_{1,2}\} - \{u_1\} \notin \Gamma$, $W_1 \cup \{u'_1\} \in \Gamma$. That means W' can find the secret by f_1 if u'_1 reveals its share, which means $W' \cup \{u'_1\}$ is qualified. However, $|(W' \cup \{u'_1\}) \cap C_2| = t_2 - 1$: contradiction. □

The proof of the lemma is built on the existence of a proper W: that's satisfying the conditions mentioned in the proof. The existence of u'_1 means $|C_1| > t_1$. $|C_2| > t_2$ is also required for u'_1 to be a critical element for W'. Additionally, in case $t_1 = t_2$, $|C_1 - C_2| > 1$ and $|C_2 - C_1| > 1$ are required for the existence of W. If $t_1 > t_2$, $|C_1 - C_2| > t_1 - t_2$ guarantees the existence of W: the inexistence of an ideal perfect secret sharing scheme. In general, we assume there exists many number of elements in $C_1 - C_2$ and $C_2 - C_1$, that's why Lemma 8 holds.

Let C_1, C_2 and C_3 be three compartments as shown in Figure 3.1. By Lemma 8, it is clear that $t_{1,2}$, $t_{1,3}$ and $t_{2,3}$ needs to be specified for an ideal perfect secret sharing scheme to exist. Since $C_{1,2,3}$ is a union compartment, $t_{1,2,3}$ needs to be specified too. A trivial inequality for $t_{1,2,3}$ is $t_{1,2,3} \geq t_{1,2} + t_3$, but it has a higher bound actually. Since $C_{1,2,3}$ can be expressed as $C_{1,2} \cup C_{1,3}$, Lemma 8 states $t_{1,2,3} \geq t_{1,2} + t_{1,3}$ must hold. If we consider all possible union constructions of $C_{1,2,3}$, we have

$$\begin{aligned} t_{1,2,3} &\geq t_{1,2} + t_{1,3} \\ t_{1,2,3} &\geq t_{1,2} + t_{2,3} \\ t_{1,2,3} &\geq t_{1,3} + t_{2,3} \end{aligned}$$

for an ideal perfect secret sharing scheme to exist.

We have the following lemma for an arbitrary number of compartments regarding the existence of an ideal perfect secret sharing scheme:

Lemma 9. *An ideal perfect secret sharing scheme does not exist if there exists some $I \subseteq I^{(m)}$ such that*

$$t_I < t_{I_1} + t_{I_2}$$

for some I_1 and I_2 satisfying $C_I = C_{I_1} \cup C_{I_2}$, C_{I_1} and C_{I_2} are not nested and $\max(t_{I_1}, t_{I_2}) > 1$.

Proof. We will use the same idea used in Lemma 8: Let $W \in \Gamma^-$ be a subset satisfying

$$\begin{aligned} |W \cap C_{I_1}| &= t_{I_1} \\ |W \cap C_{I_2}| &= t_{I_2} \end{aligned}$$

Let $J = I_1 \cap I_2$, and let $u_{1,2} \in W$ be a participant such that $u_{1,2} \in (C_{I_1} \cap C_{I_2}) - C_J$. When $W' = W - \{u_{1,2}\}$ is present, they can define a bijection f such that $s_{u_{1,2}} = f(s)$.

Let K denote the set of indexes

$$\{i \in I^{(m)} : u_{1,2} \in C_i\}$$

and $K_1 = K - I_2$, $K_2 = K - I_1$. $u_1 \in W$ is a participant such that $u_1 \in C_i \iff i \in K_1$. Note that $u_1 \in W \cap (C_{I_1} - C_{I_2})$. Let $u_1' \notin W$ be an equivalent participant of u_1. u'_1 is a critical participant for W' if there exist $k \leq |K_2|$ participants $v_1, v_2, \ldots, v_k \notin W$ such that

$$\begin{aligned} i \in K_2 &\iff \exists k', v_{k'} \in C_i \\ v_{k_1} \in C_i \text{ and } v_{k_2} \in C_i \text{ for some } i \in K_2 &\implies k_1 = k_2 \end{aligned}$$

which results in the existence of a bijection f_1 such that $s_{u'_1} = f_1(s)$. The contradiction follows as in Lemma 8. □

Note that the proof of Lemma 9 is built on the existence of participants in some special *regions*: the lemma is valid if there are many number of participants in all regions.

3.2.3 Scheme for Joint Compartmented Access Structures

We will introduce the notation and some special functions before giving the scheme. After giving the full scheme, we will provide some examples.

Let t denote the overall threshold, i.e. $t = t_{1,2,\ldots,m}$. The dealer selects t random values a_i, $0 \leq i \leq t-1$ from $\mathbb{Z}_q$ such that the secret $s = \sum_{i=0}^{t-1} a_i$.

In this scheme, the coalitions have linear systems with t unknowns (a_i) when they pool their shares. Each of these t unknowns is associated with a (basic or union) compartment C_I. d_I and $d_{i_1,i_2,\ldots,i_j}$ will denote the number of unknowns associated with the compartment C_I, and its value is defined as

$$d_I = t_I - \sum_{C_J \subset C_I} d_J.$$

The basic values for the above recursive definition come from the basic compartments that do not contain any other compartments as proper subsets, i.e. $d_I = t_I$ for such basic compartments.

Given m basic compartments, there exists $2^m - 1$ nonempty compartments. The dealer decides on an alignment Λ of the set of indexes $I \subseteq I^{(m)}$, and defines the binary bivariate alignment function $a_\Lambda(I, J)$ as

$$a_\Lambda(I, J) = \begin{cases} 1 \text{ if } I \text{ comes after } J \text{ according to } \Lambda \\ 0 \text{ else} \end{cases}$$

After defining $a_\Lambda(I, J)$, the dealer also defines e_I values as

$$e_I = \sum_{a_\Lambda(I,J)=1} d_J$$

For a user $u \in P$, the dealer decides a random identity $x_u \in \mathbb{Z}_q$, calculates

$$y_u = \sum_{u \in C_I} \sum_{i=e_I}^{e_I+d_I-1} a_i x_u^i$$

and assigns y_u as the private share of u.

Note that for each compartment C_I that has a threshold $t_I > 0$, there exist t_I unknowns associated with C_I (or C_J for $C_J \subset C_I$); and equations regarding these t_I unknowns are given to a participant u if and only if $u \in C_I$. In this way, since a qualified coalition W will satisfy $|W \cap C_I| \geq t_I$, there will be at least t_I equations regarding these t_I unknowns. If a coalition W' does not meet the condition $|W' \cap C_I| \geq t_I$, then they will not have enough equations for these t_I unknowns associated with C_I (or C_J for $C_J \subset C_I$).

In the following examples, the participant u will be assigned a point (x_u, y_u) over $f_I(x)$ if $u \in C_i \iff i \in I$.

Example: Let $m = 2$, and they are non-nested joint compartments, with $t_1 = 2$, $t_2 = 3$, $t_{1,2} = 6$. Then d values becomes $d_1 = 2$, $d_2 = 3$, $d_{1,2} = 6-(2+3) = 1$. Let Λ represent the alignment $\{1\}, \{1, 2\}, \{2\}$. For this alignment, $e_1 = 0$, $e_{1,2} = 2$, $e_2 = 3$. The polynomials for the shares are

$$\begin{aligned} f_1(x) &= a_0 + a_1 x + a_2 x^2 \\ f_2(x) &= a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 \\ f_{1,2}(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5. \end{aligned}$$

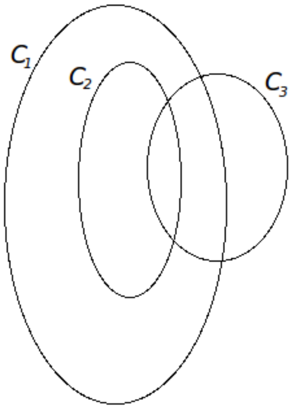

Figure 3.2: A specific $m = 3$ case

Let W be a qualified subset satisfying $|W \cap (C_1 - C_2)| = 1$, $|W \cap (C_1 \cap C_2)| = 1$, $|W \cap (C_2 - C_1)| = 4$. The linear system induced by W is

$$\begin{bmatrix} 1 & x_1 & x_1^2 & 0 & 0 & 0 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 & x_2^5 \\ 0 & 0 & x_3^2 & x_3^3 & x_3^4 & x_3^5 \\ 0 & 0 & x_4^2 & x_4^3 & x_4^4 & x_4^5 \\ 0 & 0 & x_5^2 & x_5^3 & x_5^4 & x_5^5 \\ 0 & 0 & x_6^2 & x_6^3 & x_6^4 & x_6^5 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{bmatrix}$$

where x_i's are public identities, and y_i's are private shares.

Example: $m = 3$, and the compartments are as in Figure 3.2. Let $t_1 = 3$, $t_2 = 2$, $t_3 = 3$, $t_{2,3} = 6$, $t_{1,3} = 10$.

$C_{1,2} = C_1$, so $t_{1,2} = t_1 = 3$. $C_{1,3} = C_{1,2,3}$ so $t_{1,2,3} = t_{1,3} = 10$. Note that $t_{1,3} \geq t_1 + t_{2,3}$.

Given these values, the d values are as following:

$$\begin{aligned}
d_1 &= 3-2=1\\
d_2 &= 2\\
d_3 &= 3\\
d_{1,2} &= 3-(1+2)=0\\
d_{2,3} &= 6-(2+3)=1\\
d_{1,3} &= 10-(1+2+3+1)=3\\
d_{1,2,3} &= 10-(1+2+3+1+3)=0
\end{aligned}$$

For the alignment $\{1\}$, $\{2\}$, $\{3\}$, $\{1,2\}$, $\{2,3\}$, $\{1,3\}$, $\{1,2,3\}$; the e values becomes

$$\begin{aligned}
e_1 &= 0\\
e_2 &= 1\\
e_3 &= 3\\
e_{2,3} &= 6\\
e_{1,3} &= 7
\end{aligned}$$

Note that we omit the e_I values for the compartments C_I if $d_I = 0$, since they are not necessary. After all, the polynomials for the users become as following:

$$\begin{aligned}
f_1(x) &= a_0 + a_7x^7 + a_8x^8 + a_9x^9\\
f_{1,2}(x) &= a_0 + a_1x + a_2x^2 + a_7x^7 + a_8x^8 + a_9x^9\\
f_{1,2,3}(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 + a_9x^9\\
f_{1,3}(x) &= a_0 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 + a_9x^9\\
f_3(x) &= a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 + a_9x^9.
\end{aligned}$$

3.2.4 Perfectness

As discussed in Section 1.4 a secret sharing scheme is said to be perfect if

- qualified coalitions find the secret uniquely,
- and unqualified coalitions gain no information about the secret.

We will give the necessary lemmas regarding the perfectness of the scheme. For the proofs of the lemmas, we will only give the sketch since they are very similar to the proofs of Theorem 1 and Theorem 2 in [14].

Lemma 10 (Schwartz-Zippel Lemma [6, 15])**.** *Let $G(x_1, x_2, \ldots, x_k)$ be a nonzero k-variate polynomial over $\mathbb{Z}_p$. Given d is the highest degree of each variable of G, the number of zeros of G over $\mathbb{Z}_p^k$ is bounded from above by kdp^{k-1}.*

Proof of the lemma can be found in [13, 14].

Lemma 11. *A qualified subset W finds the secret s with probability at least $1 - t(t-1)/p$, where t is the overall threshold.*

Proof. For M_W denoting the coefficient matrix of the linear system induced by the shares of W, W finds the secret if M_W is nonsingular. The determinant of M_W $\det(M_W)$ is a polynomial of t variables $\{x_1, x_2, \ldots, x_t\}$ of degree $t-1$, where x_i's are the public identities of the participants in W. By Lemma 10, $\det(M_W)$ can be zero for at most $t(t-1)p^{t-1}$ values in Z_p^t. A random selection of identities may lead to a singular M_W with probability at most $t(t-1)p^{t-1}/p^t = t(t-1)/p$, which means M_W is nonsingular with probability at least $1 - t(t-1)/p$. Hence the result follows. □

Lemma 12. *An unqualified subset W gains no information about the secret s with probability at least $1 - (t-1)^2/p$, where t is the overall threshold.*

Proof. If $|W| < t$, then M_W has fewer rows than columns. If $|W| \geq t$ but $|W \cap C_I| < t_I$ for some C_I, they have at least $t - t_I + 1$ equations regarding $t - t_I$ unknowns, which means some of them are redundant: W can ignore the shares of the *extra* participants. In both case, the coefficient matrix M_W has less rows than columns. Let's assume M_W has $t-1$ rows. Let M'_W be the augmented matrix $[\mathbf{1}^T M_W^T]^T$ for $\mathbf{1}$ denoting the row vector of length t with all entries equal to 1. If

$\det(M'_W) \neq 0$, we can say that W can not find the secret. Since all equations are linear in unknowns, “not finding the secret” is equivalent to “gaining no information about the secret”. The probability of $\det(M'_W)$ to be nonzero can be bounded by using Lemma 10 as in Lemma 11. □

3.3 Conclusion

In this work, we extended the idea of comparmented access structures and introduced joint compartmented access structures. We marked some joint compartmented access structures as *unrealizable* by any ideal perfect secret sharing scheme. For those joint compartmented access structures not marked as *unrealizable*, we proposed an ideal secret sharing scheme that is perfect with an overwhelming probability.

We would like to note that the classical compartmented access structures and conjunctive hierarchical access structures are special cases of joint comparmented access structures: When the compartments are disjoint, our scheme is very similar to the ones proposed in [3, 4, 14]. When the compartments are all nested, i.e. $C_i \subset C_j$ if $i < j$ with thresholds $0 < t_1 < t_2 < \ldots < t_m$, the access structure becomes a conjunctive hierarchical access structure, and our scheme reduces to the scheme proposed in [7].

Chapter 4

Spherical Secret Sharing

In this chapter, a new threshold secret sharing scheme will be introduced. We will also use this new scheme for constructing disjunctive multilevel secret sharing schemes.

In our new threshold scheme, we use the idea that t points in $t-1$ dimensional space uniquely determines a hypersphere in $t-1$ dimensional space. The dealer will select a random centre and a random radius for the hyphersphere, and assign points on that hypersphere to the participants. The secret is a particular coordinate of the center point. When less than t participants come together, they will not be able to find the centre of the hypersphere.

4.1 Preliminary

In this section, we will provide some preliminary information related to our new scheme.

4.1.1 Perpendicular Bisector Hyperplane Equation

Given two points $A = (a_1, a_2, \ldots, a_d), B = (b_1, b_2, \ldots, b_d)$ in d dimensional space, assume H is the perpendicular bisector hyperplane of $[AB]$, and M is the midpoint of $[AB]$. Then we have

$$M = (A + B)/2 = ((a_1 + b_1)/2, (a_2 + b_2)/2, \ldots, (a_d + b_d)/2).$$

Assume $X = (x_1, x_2, \ldots, x_d)$ is an arbitrary point on H. The vector $X - M$ is perpendicular to $A - B$. So

$$\begin{aligned}
(X - M)(A - B)^T &= 0 \\
\sum_{i=1}^{d} \left(x_i - \frac{a_i + b_i}{2} \right) (a_i - b_i) &= 0 \\
\sum_{i=1}^{d} (a_i - b_i) x_i &= \sum_{i=1}^{d} \frac{(a_i - b_i)(a_i + b_i)}{2} \\
\sum_{i=1}^{d} (a_i - b_i) x_i &= \frac{1}{2} \sum_{i=1}^{d} (a_i^2 - b_i^2)
\end{aligned}$$

Then the hyperplane equation of H becomes

$$(A - B)X^T = \frac{1}{2} \left(AA^T - BB^T \right)$$

where x_i's are the variables.

4.1.2 Hypersphere

For a given point C in d dimensional space and a scalar r, a hypersphere is the set of all points that are r unit euclidean distance away from C. If the center C is $(c_1, c_2, \ldots, c_d)$, then the equation of the hypersphere becomes

$$\sum_{i=1}^{d} (x_i - c_i)^2 = r^2$$

where x_i's are variables.

4.1.3 Finding the Hypersphere Center from Given Points on the Hypersphere

Given two points P_i, P_j on the sphere, we know that the perpendicular bisector of $[P_iP_j]$ passes through the center of the hypersphere. Assume the set of points $P = \{P_1, P_2, \ldots, P_t\}$ are given such that they lie on a hypersphere in $d = t - 1$ dimensional space. Let $H_{i,j}$ is the perpendicular bisector hyperplane of $[P_iP_j]$. The center C lies on all $H_{1,j}$ for $2 \leq j \leq t$. Then we know that

$$(P_1 - P_j)\, C^T = \frac{1}{2}\left(P_1P_1^T - P_jP_j^T\right)$$

for all j, $2 \leq j \leq t$. We have $d = t - 1$ unknowns –the coordinates of C, and d equations. C can be completely computed if the coefficient matrix

$$\begin{bmatrix} P_1 - P_2 \\ P_1 - P_3 \\ \vdots \\ P_1 - P_t \end{bmatrix} \tag{4.1}$$

is nonsingular.

4.2 Spherical Threshold Secret Sharing

Given the threshold t, the dealer selects a random point C over $\mathbb{Z}_p^d$ where $d = t-1$, and a scalar r as the center and the radius of the hypersphere, respectively. The secret to be shared is the last coordinate of C. For each participant $u \in P$, the dealer assigns a random point P_u lying on the hypersphere to u. If $P_u = (p_{u,1}, p_{u,2}, \ldots, p_{u,d})$, the dealer makes the first $d - 1$ coordinates public. The private share of u is only the last coordinate of P_u, i.e. $p_{u,d}$.

When any coalition of size t is present, they can find C as it is described in Section 4.1.3, in this way they have the secret, which is the last coordinate of C.

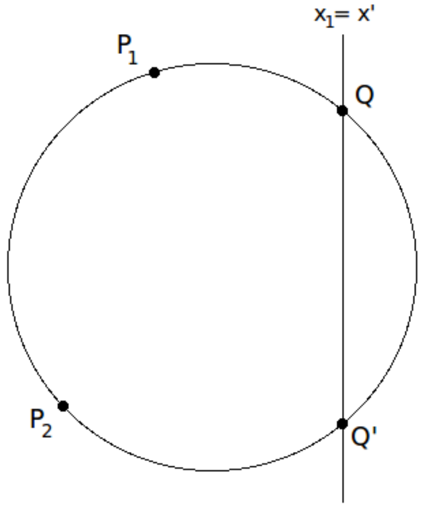

Figure 4.1: A possible circle for P_1 and P_2

4.2.1 Perfectness of the Scheme

Assume a qualified coalition is present, then the secret may not be recoverable if and only if the coefficient matrix given in (4.1) is singular. This is the case when the points of the participants in the coalition are at the intersection of the d dimensional hypersphere with a d dimensional hyperplane. If the selection of the points is well-randomized during the share generation phase, this is very unlikely.

Assume an unqualified coalition is present. The secret may be compromised if and only if the coefficient matrix given in (4.1) spans the unit vector $(0, 0, \ldots, 0, 1)$, which is very unlikely for an arbitrary selection of the points by the dealer.

When an unqualified subset is present, even if they cannot obtain the exact value of the secret, they may gain some information about it, and eliminate some possible values from the domain that the secret is taken from: Assume $t = 3$, and 2 participants came together. Let their points be P_1, P_2, and the point of some another participant is P_3, where the first coordinate of P_3 is known to be x'. For a perfect secret sharing scheme, there must be one-to-one matching between possibilities of P_3 and the secret. As it is shown in Figure 4.1, both of $P_3 = Q$

and $P_3 = Q'$ suggests the same circle, i.e. the same secret. If we call Q' and Q as the dual of each other, then all points —except the point where the circle is tangent to the $x_1 = x'$ line— have a dual. In this way, a coalition of size 2 can eliminate almost half of the possibilities for the secret, i.e. one bit of the secret is compromised.

4.2.2 Hierarchical Secret Sharing

Before starting spherical hierarchical secret sharing, note that the intersection of a d dimensional hyperplane with a d dimensional hypersphere is exactly a $d-1$ dimensional hypersphere. Additionally, if that hyperplane is in form $x_j = x'$ for some dimension x_j and some scalar x', then the coordinates of the centre of the $d-1$ dimensional hypersphere is equal to the coordinates of the d dimensional hypersphere except the jth coordinate, which is equal to x' for the $d-1$ dimensional hypersphere. We will call the $d-1$ dimensional hypersphere as the sub-hypersphere of the d dimensional hypersphere induced by the hyperplane $x_j = x'$.

We will use the notation introduced in Section 1.5.3: We have m levels, and the thresholds for the levels are t_i for $1 \leq i \leq m$. For L_i denoting the participants contained in the ith level, C_i represents the set difference $L_i - L_{i-1}$ for $1 \leq i \leq m$, with $L_0 = \emptyset$.

The dealer selects a random hypersphere S_m with the center

$$C = (c_1, c_2, \ldots, c_{t_m - 1})$$

and the radius r. Additionally, the dealer selects random values r_i from interval $(c_i - r, c_i + r)$ for $1 \leq i \leq t_m - t_1$, and makes them public. Let H_i denote the hyperplane $x_i = r_i$ for $1 \leq i \leq t_m - t_1$. Then the hypersphere S_i for $1 \leq i < m$ is defined as the sub-hypersphere of S_m induced by the hyperplanes H_j's satisfying $1 \leq j \leq t_m - t_i$. Note that S_i is a $(t_m - 1) - (t_m - t_i) = t_i - 1$ dimensional hypersphere.

For a participant $u \in C_i$, the dealer selects a point lying on S_i and assigns the last coordinate of that point as the private share to u. The first $t_m - 1$ coordinates of the point is public, as it was in spherical threshold secret sharing.

When t_i participants from L_i come togerher, since S_i is a $t_i - 1$ dimensional hypersphere, they can find the center as it is described in Section 4.1.3. Note that S_i is a sub-hypersphere of S_j for $i < j$. That's why a point assigned to a participant $u \in C_i$ also lies on the hypersphere S_j. In this way, a participant from C_i can take place in a coalition of the level L_j, for $i \leq j \leq m$.

Chapter 5

Conclusion

In this work, we studied several access structures including threshold access structures, compartmented access structures and multilevel access structures. All solutions we proposed are linear and ideal.

In Chapter 2, we suggested two ideal secret sharing schemes realizing disjunctive multilevel access structures. The first scheme (basic scheme) is almost surely perfect, and the second scheme (extended scheme) is always perfect. Multilevel access structures are introduced in 1988 by Simmons [10], without a secret sharing scheme for it. As far as we know, the only ideal, dynamic and always perfect secret sharing scheme realizing multilevel access structures was published in 2004 by Tassa [11]. Although many schemes have been proposed in the literature, the scheme described in [11] and our extended scheme are the only ideal schemes that always work, and allow new users to be added to any level.

In Chapter 3, we introduced a new access structure named as joint compartmented access structures. All previous research about compartmented access structures assumed the compartments to be disjoint. We examined the existence of an ideal perfect secret sharing scheme if the compartments have some common participants. We showed that some joint compartmented access structures cannot be realized by an ideal perfect secret sharing scheme. For the other joint compartmented access structures, we have proposed an ideal and almost surely perfect secret sharing scheme.

In Chapter 4, we suggested an interesting threshold secret sharing scheme that uses hyperspheres, so we called this scheme as spherical threshold secret sharing scheme. Moreover, we used this threshold secret sharing scheme and provided another secret sharing scheme that realizes disjunctive multilevel access structures. Although the idea used in the scheme is novel, it is not completely perfect: Unqualified coalitions gain one-bit of information about the secret.

As a future work, we will look for an always perfect secret sharing scheme realizing joint compartmented access structures. We think such a scheme would be quite significant, since it will also cover compartmented access structures and conjunctive multilevel access structures as special cases.

Bibliography

[1] M. Belenkiy. Disjunctive multi-level secret sharing. Cryptology ePrint Archive, Report 2008/018, 2008.

[2] G. Blakley. Safeguarding cryptographic keys. In *AFIPS National Computer Conference*, 1979.

[3] E. Brickell. Some ideal secret sharing schemes. In *EUROCRYPT'89*, volume 434 of *LNCS*, pages 468–475. Springer-Verlag, 1990.

[4] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini. Secret sharing in multilevel and compartmented groups. In *ACISP'98*, volume 1438 of *LNCS*, pages 367–378, London, UK, 1998. Springer-Verlag.

[5] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *GLOBECOM'87*, pages 99–102. IEEE Press, 1987.

[6] J. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. volume 27 of *Journal of the ACM*, pages 701–717. ACM, 1980.

[7] A. A. Selçuk, K. Kaşkaloğlu, and F. Özbudak. On hierarchical threshold secret sharing. Cryptology ePrint Archive, Report 2009/450, 2009.

[8] A. A. Selçuk and R. Yılmaz. Linear hierarchical secret sharing. In *ISC Turkey 2010*, pages 160–164, 2010.

[9] A. Shamir. How to share a secret? *Communications of the ACM*, 22(11):612–613, 1979.

[10] G. J. Simmons. How to (really) share a secret. In *CRYPTO'88*, volume 403 of *LNCS*, pages 390–448, London, UK, 1988. Springer-Verlag.

[11] T. Tassa. Hierarchical threshold secret sharing. In *TCC 2004*, pages 473–490, 2004.

[12] T. Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264, 2007.

[13] T. Tassa and N. Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology*, 22(2):227–258, 2009.

[14] Y. Yu and M. Wang. A probabilistic secret sharing scheme for a compartmented access structure. Cryptology ePrint Archive, Report 2009/301, 2009.

[15] R. Zippel. Probabilistic algorithms for spare polynomials. In *EUROSAM'79*, pages 216–226, Marseille, 1979.