Joint Compartmented Threshold Access Structures

Ali Aydın Selçuk, Ramazan Yılmaz*

Department of Computer Engineering, Bilkent University, Ankara, 06800, Turkey

Abstract

In this paper, we introduce the notion of a joint compartmented threshold access structure (JCTAS). We study the necessary conditions for the existence of an ideal and perfect secret sharing scheme and give a characterization of almost all ideal JCTASes. Then we give an ideal and almost surely perfect construction that realizes such access structures. We prove the asymptotic perfectness of this construction by the Schwartz-Zippel Lemma.

Keywords: cryptography, secret sharing, general access structures, compartmented access structures, Shamir secret sharing

1. Introduction

A secret sharing scheme is a method of distributing a secret value among members of a group such that only certain coalitions of these participants can find the secret. A subset of users that can recover the secret is called a *qualified coalition*, and the set of all qualified coalitions is called the *access structure*. An access structure is called *monotone* if every coalition containing a qualified coalition as a subset is also a qualified coalition.

An important class of access structures is the *threshold* access structure, where a coalition is qualified if and only if it has at least t members for some specified threshold t. Threshold access structures were introduced and the first solutions were proposed by Shamir [1] and Blakley [2].

Another important class of access structures is the *compartmented* threshold access structure, where the user set is partitioned into compartments,

*Corresponding author

Email addresses: selcuk@cs.bilkent.edu.tr (Ali Aydın Selçuk), ryilmaz@cs.bilkent.edu.tr (Ramazan Yılmaz)

and a qualified subset has to satisfy a certain threshold at each compartment as well as the overall threshold. Such access structures may be desirable to guarantee fair representation across different sections of a community. Compartmented access structures were introduced in [3], and several secret sharing schemes realizing such access structures were proposed in [4, 5, 6].

Ideality and *perfectness* are two important criteria for a secret sharing scheme in terms of efficiency and security, respectively. A secret sharing scheme is said to be *ideal* if the size of the share assigned to each participant is no larger than the size of the secret; and it is said to be *perfect* if an unqualified coalition can gain no information about the secret. It is shown that all monotone access structures can be realized by a perfect secret sharing scheme [7]. Thus, an important question for an access structure is whether it is possible to find a secret sharing scheme that is both ideal and perfect.

Traditionally, a compartmented access structure is assumed to consist of disjoint compartments [3, 4, 5, 6]. We generalize this concept such that the compartments are not necessarily disjoint, and refer to such an access structures as a *joint compartmented threshold access structure* (JCTAS). In this paper, we give necessary conditions for the existence of an ideal and perfect scheme for JCTASes. Then we propose an ideal and almost surely perfect construction for these access structures.

The organization of this paper is as follows: In the rest of this section, we give a brief overview of compartmented access structures. In Section 2, we prove a fundamental result regarding the existence of an ideal and perfect secret sharing scheme for a given access structure. In Section 3, we define JCTASes and introduce our notation. In Section 4 and Section 5, we give the necessary conditions for the existence of an ideal and perfect secret sharing scheme for a JCTAS. We also include a construction for those JCTASes satisfying the necessary conditions given. We analyze the perfectness of the proposed construction in Section 6. Finally, we conclude the paper in Section 7.

Throughout this work, we will represent the set of participants with U, and denote the access structure defined on U with Γ. The access structures that we deal with are all monotone. Unless otherwise stated, all values and computations are defined over $\mathbb{Z}_q$, where q is a large prime. The secret is denoted by s, and the share of a participant u is denoted by s_u.

1.1. Minimal Access Structure

The access structure Γ defined on U is the set of all qualified coalitions $W \subset U$. Given that Γ is monotone, some subsets included in Γ are actually unnecessary: If a particular W is marked as qualified, then all of its supersets are also qualified. Therefore, including just the minimal qualified sets is sufficient for defining a monotone access structure.

Definition 1. Given a monotone access structure Γ, its *minimal access structure* is defined as

$$\Gamma^- = \{W \in \Gamma : W' \subset W \Rightarrow W' \notin \Gamma\}.$$

1.2. Compartmented Access Structures

In a compartmented access structure, the set of participants U contains a number of compartments $C_1, C_2, \ldots, C_m$. In addition to the overall threshold t, each compartment C_i has another threshold t_i. A coalition is qualified if and only if the threshold for each compartment as well as the overall threshold is satisfied.

Definition 2. For a user set U partitioned into m compartments $C_1, C_2, \ldots, C_m$ and given the thresholds $t_1, t_2, \ldots, t_m, t$, the *compartmented access structure* is defined as

$$\Gamma = \{W : |W| \geq t \text{ and } |W \cap C_i| \geq t_i \text{ for } 1 \leq i \leq m\}.$$

Compartmented access structures can be used in settings where each section of the user space is to be fairly represented in authorized coalitions.

1.3. Our Contribution

We introduce the concept of the JCTAS, which allows intersections between compartments in a compartmented access structure, i.e. a user is allowed to be in more than one compartment. We identify the necessary conditions for the existence of ideal and perfect schemes for almost all JCTASes, and give an ideal and perfect secret sharing scheme for those JCTASes that satisfy the necessary conditions.

Besides being an interesting generalization, a JCTAS is interesting also because any access structure can be seen as a JCTAS by selecting the compartments appropriately: Let Γ be an arbitrary access structure on a set U of participants, and let $\Gamma^* = \{A \subseteq U : U - A \notin \Gamma\}$ be the *dual access structure*.

Let the minimal sets of Γ^* be $(\Gamma^*)^- = \{C_1, C_2, \ldots, C_j\}$. Then a coalition W is qualified according to Γ if and only if $|W \cap C_i| \geq 1$ for every $i = 1, \ldots, j$; hence, Γ is a JCTAS with compartments $C_1, C_2, \ldots, C_j$, with a threshold of 1 for each compartment.

Although any access structure can be seen as a JCTAS, we would like to note that we do not claim to solve the longstanding open problem of giving a complete characterization of all ideal access structures. This is due to the fact that our analysis does not cover certain cases of JCTASes where the thresholds of the compartments are equal to 1.

2. Inexistence of Ideal and Perfect Schemes

In this section, we will give a necessary condition about existence of an ideal and perfect secret sharing scheme for a given access structure. The given result is general but it will also serve as the fundamental tool for our results on ideal and perfect secret sharing schemes for JCTASes.

Lemma 1. *Let τ be an ideal and perfect secret sharing scheme realizing a monotone access structure Γ, $W \notin \Gamma$, and $W \cup \{u\} \in \Gamma$. The shares of W together induce a bijection between s_u and the secret s.*

Proof. Since τ is perfect, all values in $\mathbb{Z}_q$ are possible for s. Given that $W \cup \{u\}$ is qualified but W is not, each value of s_u uniquely identifies the value of s. Since τ is ideal, this relation is also onto. Hence, the values of W together induce a bijection between s and s_u.

Definition 3. For W being an unqualified subset, its qualified extension $V \in \Gamma$, and $V \supset W$ is said to be a minimal qualified extension of W if any W' satisfying $W \subset W' \subset V$ is unqualified.

Definition 4. Given an unqualified subset W, the participants contained in the set

$$\{u \notin W : u \text{ is in some minimal qualified extension of } W\}$$

are *critical extenders* for W.

Lemma 2. *Let τ be an ideal and perfect secret sharing scheme realizing a monotone access structure Γ. An unqualified subset W' cannot obtain any information about s_u if u is a critical extender for W'.*

PROOF. The result follows from Lemma 1 by a suitable selection of a qualified minimal extension V of $W' \cup \{u\}$ and $W = V - \{u\}$.

Definition 5. Two participants u and v are equivalent, i.e. $u \equiv v$, if their roles are identical in Γ (i.e. $W' = W - \{u\} \cup \{v\}$ is qualified for all qualified coalitions W containing u but not v, and $V' = V - \{v\} \cup \{u\}$ is qualified for all qualified coalitions V containing v but not u).

Lemma 3 (Fundamental Lemma). *Let Γ be an access structure, W be an unqualified subset, and $v, u, u' \in U$ such that*

1. *$v \notin W$, $W \cup \{v\} \in \Gamma^-$,*
2. *$u \notin W$ is a critical extender for W, but $W \cup \{u\} \notin \Gamma$, and*
3. *$\exists u' \in W$ such that $u' \equiv u$.*

Then, Γ cannot be realized by an ideal and perfect secret sharing scheme.

PROOF. Assume that there exists an ideal and perfect secret sharing scheme τ realizing Γ. When the participants in W pool their shares, they can find a bijection $f_v(s_v) = s$, by Lemma 1.

Since u is a critical extender for W, W cannot gain any information about s_u, by Lemma 2. Since $W \cup \{v\} \in \Gamma^-$, $W' = W \cup \{v\} - \{u'\}$ is not a qualified coalition, but $W' \cup \{u\} \in \Gamma$. By f_v, W has s in terms of s_v, so W can find another bijection f_u such that $f_u(s_u) = s$: Given W, the pair (s, s_v) has q possible values in $\mathbb{Z}_q^2$ instead of q^2, by Lemma 1. Each possibility corresponds to a single value for s_u since $\{u\} \cup W' \in \Gamma$. That leads to the existence of the bijection f_u.

The existence of f_u means that W can find s if u reveals his share, i.e. $W \cup \{u\} \in \Gamma$. However, that contradicts our prior assumption that $W \cup \{u\} \notin \Gamma$.

3. Joint Compartmented Threshold Access Structures

We define a JCTAS to mean a compartmented access structure where the compartments are not necessarily disjoint and where there may be elements at the intersection of two compartments. Traditionally, compartments are assumed to be disjoint [3, 4, 5, 6]. We hereby generalize this structure and allow a participant to be in more than one compartment. We also allow additional thresholds to be defined for intersections and unions of compartments, i.e. a threshold can be defined for $(C_i \cup C_j) \cap C_k$.

For indexing compartments and their intersections, we use the following notation: Let $b(N, i)$ denote the ith right-most bit of N for its binary representation, $b_1(N, n)$ denote the set of integers $1 \leq i \leq n$ such that $b(N, i) = 1$, and $b_0(N, n)$ denote the set of integers $1 \leq i \leq n$ such that $b(N, i) = 0$. For example, $b(2, 1) = 0$, $b(5, 3) = 1$, $b(5, 4) = 0$, $b_0(2, 3) = \{1, 3\}, b_1(6, 3) = \{2, 3\}$.

For m denoting the number of compartments, R_c denotes the cth *simple region*, defined as

$$R_c = \bigcap_{i \in b_1(c,m)} C_i \; - \bigcup_{i \in b_0(c,m)} C_i$$

for $1 \leq c \leq 2^m - 1$. As an example, the simple regions for $m = 3$ are shown in Figure 1.

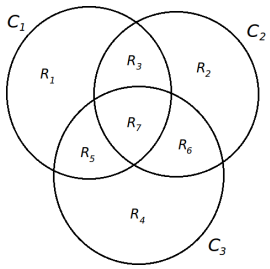

Figure 1: Simple regions for $m = 3$

If we consider all possible regions that can be unions of simple regions, we have $2^{2^m-1} - 1$ non-empty regions. For $1 \leq c \leq 2^{2^m-1} - 1$, U_c is defined as

$$U_c = \bigcup_{i \in b_1(c, 2^m-1)} R_i.$$

In classical compartmented access structures, thresholds are specified for only disjoint compartments and the set of participants U. In joint compartmented threshold access structures, a threshold may be specified for any region U_c. Let T denote the set of regions for which a threshold is specified. For $t(U_c)$ denoting the threshold specified for U_c, a JCTAS is defined as

$$\Gamma = \{W \subseteq U : |W \cap U_c| \geq t(U_c) \text{ for all } U_c \in T\}.$$

We will stick to the classical notation in the literature and denote $t(C_i)$ with t_i.

In the following sections, we will first discuss the conditions for an ideal and perfect secret sharing scheme to exist for a JCTAS. Then we will propose a linear scheme for those joint access structures that can be realized by an ideal and perfect secret sharing scheme. For the sake of simplicity, in Section 4, we will first study the case of two compartments; then, in Section 5, we will generalize our results to an arbitrary number of compartments. Finally, in Section 6, we will give some probabilistic bounds regarding the perfectness of the proposed scheme.

4. Existence of Ideal Perfect Schemes for $m = 2$

Before we give our general results and construction in Section 5, we first consider the special case of two compartments ($m = 2$) with thresholds $t_1 = t(C_1), t_2 = t(C_2)$, and $t(U_7) = t(U)$.

With only two compartments C_1 and C_2, there are three possible cases regarding their relation:

- $C_1 \cap C_2 = \emptyset$, which corresponds to the classical compartmented access structures; ideal and perfect schemes for such access structures have been proposed in [4, 5, 6].
- $C_1 \subset C_2$ (or vice versa), which corresponds to the conjunctive hierarchical access structures, and which is also well studied; ideal and perfect schemes for such access structures appear in [8, 6, 9].
- $C_1 \cap C_2 \neq \emptyset$, and they are not nested.

We will deal with the third scenario and show, by Lemma 3, which access structures can be realized by an ideal and perfect secret sharing scheme. Then we will propose a construction, which will also cover the first two cases as special cases.

Note that our two-compartment JCTAS here is a special case of tripartite access structures, which have been studied in detail in [10]. The results in this section are significant because they lay the foundation for the results in Section 5 for arbitrary values of m and facilitate their comprehension.

In the following lemmas, we assume $|C_i| > t_i$ for $i = 1, 2$. If $|C_i| = t_i$ for some i, the access structure can be thought of as a classical disjoint compartmented access structure with C_i being one compartment and $C_{3-i} - C_i$ (i.e. $C_2 - C_1$ if $i = 1$, and $C_1 - C_2$ if $i = 2$) being the other compartment.

Note that some important regions for $m = 2$ are as follows:

$$\begin{array}{rcccl} U_1 & = & R_1 & = & C_1 - C_2, \\ U_2 & = & R_2 & = & C_2 - C_1, \\ U_4 & = & R_3 & = & C_1 \cap C_2, \\ U_7 & = & R_1 \cup R_2 \cup R_3 & = & U. \end{array}$$

First, we will assume in Lemma 4 that there are at least t_1 and t_2 participants in R_1 and R_2, respectively. Then in Lemma 5, we will study the cases without this restriction.

Lemma 4. *Given* $\max(t_1, t_2) > 1$, $|R_1| \geq t_1$, $|R_2| \geq t_2$ *and* $|R_3| \geq 1$*; an ideal and perfect secret sharing scheme exists only if a threshold for* U_7 *is defined and satisfies*

$$t(U_7) \geq t_1 + t_2.$$

PROOF. Assume $t(U_7) < t_1 + t_2$, or $t(U_7)$ is not specified (which is equivalent to $t(U_7) = \max(t_1, t_2)$). Without loss of generality, we can assume $t_1 \geq t_2$. By Lemma 3, and with suitable selections of u, u', v, and W, we can see that an ideal and perfect secret sharing scheme cannot exist: Take W to be a subset of size $t_1 + t_2 - 2$, satisfying

$$\begin{array}{rcl} |W \cap R_1| & = & t_1 - 1, \\ |W \cap R_2| & = & t_2 - 1, \text{ and} \\ |W \cap R_3| & = & 0. \end{array}$$

Participants u, v are selected as $u \in R_1 - W$ and $v \in R_3$. Note that u' can be any participant in $W \cap R_1$. The result follows from Lemma 3.

Remark 1. Note that the proof of this lemma relies on the existence of a coalition W satisfying $|W \cap R_1| \geq t_1 - 1$ and $\exists u' \in W \cap R_1$, i.e. $t_1 = \max(t_1, t_2) > 1$, in order to use the Fundamental Lemma. Hence we have the restriction $\max(t_1, t_2) > 1$ in the statement of Lemma 4; as we have similar restrictions in the lemmas that will follow.

The next lemma is an extension of Lemma 4. It gives a lower bound for $t(U_7)$, where we do not necessarily have $|R_1| \geq t_1$ or $|R_2| \geq t_2$.

Before moving on, let $n_i = |R_i|$ and k_i be defined as

$$k_i = \begin{cases} t_i - n_i & \text{if } n_i < t_i \\ 0 & \text{otherwise} \end{cases}$$

for $i \in \{1, 2\}$.

Lemma 5. *Let $k = \max(k_1, k_2)$, and $n = n_i$ for i satisfying $k = k_i$. Given $n > 1$ and $\max(t_1, t_2) > 1$, an ideal and perfect secret sharing scheme exists only if a threshold for U_7 is defined and it satisfies*

$$t(U_7) \geq t_1 + t_2 - k.$$

PROOF. Let r be the integer satisfying $k = k_r$ for $r \in \{1, 2\}$. Let W be a subset of size $t_1 + t_2 - k - 2$ satisfying

$$\begin{aligned} |W \cap R_1| &= t_1 - k - 1, \\ |W \cap R_2| &= t_2 - k - 1, \\ |W \cap R_3| &= k. \end{aligned}$$

The argument above assumes $t_{3-r} - k - 1 \geq 0$, since $t_{3-r} - k - 1 < 0$ requires $t_{3-r} \leq k$, which makes the compartment C_{3-r} redundant: Any coalition that has t_r members from C_r will also have at least $k \geq t_{3-r}$ members from $R_3 \subset C_{3-r}$.

$|C_i| > t_i$ ensures there exists some $v \in R_3 - W$.

$n > 1$ and $\max(t_1, t_2) > 1$ ensure there exists some $u \in R_r - W$ and there exists some $u' \in W \cap R_r$. Note that $t_{3-r} - k - 1 < n_{3-r}$, so u is critical for W. The result follows from Lemma 3.

Note that Lemma 4 is a special case of Lemma 5, with $k = 0$.

Without a threshold for $U = U_7$, the size of a minimal qualified subset W satisfies $\max(t_1, t_2) \leq |W| \leq t_1 + t_2 - k$. For an ideal and perfect scheme to exist, we showed that $t(U_7)$ must be defined and must satisfy $t(U_7) \geq t_1 + t_2 - k$, which means that the size of all minimal qualified coalitions are the same and equal to $t_1 + t_2 - k$. This result suggests using a Shamir-like scheme with polynomials of degree $t_1 + t_2 - k - 1$ for secret sharing in such access structures. We give such a construction in the following subsection.

4.1. An Ideal Perfect Scheme for $m = 2$

Let U contain two compartments C_1, C_2, and the thresholds for these compartments be t_1 and t_2. We also have an overall threshold, $t(U_7)$, that satisfies the condition in Lemma 5.

The secret sharing scheme we propose will be a Shamir-like polynomial construction. The degree of the polynomial will be $t(U_7) - 1$, i.e. $f(x) = \sum_{i=0}^{t(U_7)-1} a_i x^i$, and each member will be associated with certain terms of the polynomial according to its position. The secret is $f(1)$.

We define the *dimension* of a region U_i as

$$d_i = t(U_i) - \sum_{U_j \subset U_i} d_j,$$

with $d_i = t(U_i)$ for a region U_i that does not have any sub-regions with a specified threshold.

Note that $T = \{U_4, U_5, U_6, U_7\}$, where

$$\begin{aligned} U_4 &= C_1 \cap C_2, \\ U_5 &= C_1, \\ U_6 &= C_2, \\ U_7 &= C_1 \cup C_2. \end{aligned}$$

That is why we are interested in only d_4, d_5, d_6 and d_7. In particular, given t_1, t_2, k and $t(U_7)$, we have the following dimension values for a system of two compartments C_1, C_2:

$$\begin{aligned} d_4 &= k, \\ d_5 &= t_1 - d_4 = t_1 - k, \\ d_6 &= t_2 - d_4 = t_2 - k, \\ d_7 &= t(U_7) - (d_4 + d_5 + d_6) = t(U_7) - t_1 - t_2 + k. \end{aligned}$$

Although there is no explicit threshold for $U_4 = C_1 \cap C_2$, we assign k dimensions to it since a minimal qualified subset cannot meet the thresholds of $C_1 = U_5$ and $C_2 = U_6$ without having at least $k \geq 0$ participants from U_4, i.e. there is an implicit threshold for U_4.

Intuitively, d_i corresponds to the number of dimensions associated with U_i. For instance, if

$$\begin{aligned} d_4 &= 1, \\ d_5 &= 2, \\ d_6 &= 3, \text{ and} \\ d_7 &= 2, \end{aligned}$$

then the association between the regions and the terms of the polynomial is as follows.

$$\overbrace{1}^{U_4} \quad \overbrace{x \quad x^2}^{U_5} \quad \overbrace{x^3 \quad x^4 \quad x^5}^{U_6} \quad \overbrace{x^6 \quad x^7}^{U_7}$$

A participant $u \in R_1 = C_1 - C_2$ (with the ID $u \in \mathbb{Z}_q$) will have $f_1(u)$ as his private share, where $f_1(x)$ is defined as

$$f_1(x) = a_1 x + a_2 x^2 + a_6 x^6 + a_7 x^7,$$

where the coefficients of the terms $1, x^3, x^4$, and x^5 are zero since they are associated with U_4 and U_6, and $u \notin U_4$ and $u \notin U_6$, while $u \in U_5$ and $u \in U_7$.

Similarly, participants in $R_2 = C_2 - C_1$ and $R_3 = C_1 \cap C_2$ will be given shares according to the polynomials $f_2(x)$ and $f_3(x)$, respectively, which are defined as

$$\begin{aligned} f_2(x) &= a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7, \text{ and} \\ f_3(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 \\ &\quad + a_7 x^7. \end{aligned}$$

Let e_i denote the smallest exponent of the terms associated with U_i, i.e. the terms associated with U_i are $x^{e_i}, x^{e_i+1}, \ldots, x^{e_i+d_i-1}$. We have

$$e_i = \sum_{j<i} d_j.$$

Then, the general definition of the polynomials f_1, f_2, and f_3 mentioned in the example above becomes

$$\begin{aligned} f_1(x) &= \sum_{i=e_5}^{e_5+d_5-1} a_i x^i + \sum_{i=e_7}^{e_7+d_7-1} a_i x^i, \\ f_2(x) &= \sum_{i=e_6}^{e_6+d_6-1} a_i x^i + \sum_{i=e_7}^{e_7+d_7-1} a_i x^i, \text{ and} \\ f_3(x) &= \sum_{i=e_4}^{e_4+d_4-1} a_i x^i + \sum_{i=e_5}^{e_5+d_5-1} a_i x^i \\ &\quad + \sum_{i=e_6}^{e_6+d_6-1} a_i x^i + \sum_{i=e_7}^{e_7+d_7-1} a_i x^i. \end{aligned}$$

For a participant with the ID $u \in \mathbb{Z}_q$, the dealer computes his share s_u as:

$$s_u = \begin{cases} f_1(u) & \text{if } u \in R_1 = C_1 - C_2 \\ f_2(u) & \text{if } u \in R_2 = C_2 - C_1 \\ f_3(u) & \text{if } u \in R_3 = C_1 \cap C_2 \end{cases}$$

As stated in Section 4, there are three possible cases for the compartments when $m = 2$. Our scheme is applicable not only for the last case but also the first two cases: When the compartments C_1, C_2 are disjoint, k is always equal to 0, $d_5 = t_1$, $d_6 = t_2$, $d_7 = t(U_7) - (t_1 + t_2)$ and the secret is shared according to the polynomials

$$\begin{aligned} f_1(x) &= \sum_{i=0}^{t_1-1} a_i x^i + \sum_{i=t_1+t_2}^{t(U_7)-1} a_i x^i \text{ and} \\ f_2(x) &= \sum_{i=t_1}^{t_1+t_2-1} a_i x^i + \sum_{i=t_1+t_2}^{t(U_7)-1} a_i x^i, \end{aligned}$$

which is identical to the scheme presented in [11]. When they are nested, i.e. $C_1 \subset C_2$, the polynomials are

$$\begin{aligned} f_2(x) &= \sum_{i=t_1}^{t_2-1} a_i x^i \text{ and} \\ f_3(x) &= \sum_{i=0}^{t_1-1} a_i x^i + \sum_{i=t_1}^{t_2-1} a_i x^i, \end{aligned}$$

and the scheme corresponds to the one proposed in [9] for conjunctive hierarchical access structures.

5. Existence of Ideal Perfect Schemes for $m \geq 3$

In Section 4, we proved two lemmas regarding the existence of an ideal and perfect scheme when there are exactly two compartments in the user domain. In this section, we will generalize Lemma 4 and Lemma 5 and show which JCTAS can be realized by an ideal and perfect secret sharing scheme.

Definition 6. A JCTAS Γ is said to be *sufficiently populated* if $|U_i - U_j| \geq t(U_i)$ for all $U_i, U_j \in T$ that are neither nested nor disjoint.

Lemma 6. *Let Γ be a sufficiently populated JCTAS, with $\max(t(U_i), t(U_j)) > 1$ for all $U_i, U_j \in T$ that are neither nested nor disjoint. An ideal and perfect secret sharing scheme exists for Γ only if, for any two regions $U_i, U_j \in T$ that are neither nested nor disjoint, we have $U_i \cup U_j \in T$ and*

$$t(U_i \cup U_j) \geq t(U_i) + t(U_j).$$

PROOF. Let $r \in \{i, j\}$ be an integer such that $t(U_r) > 1$, and $r' \in \{i, j\}$ be the integer such that $r' \neq r$. Let V be a qualified coalition such that $V \cap U_i \cap U_j = \{v\}$. Let u be some participant in $U_r - V$ and u' be some participant in $V \cap (U_r - U_{r'})$. The result follows from Lemma 3 by selecting $W = V - \{v\}$.

Let C_1, C_2, and C_3 be three compartments, as shown in Figure 1. Some important regions are

$$\begin{array}{rcccl} U_{119} & = & R_1 \cup R_2 \cup R_3 \cup R_5 \cup R_6 \cup R_7 & = & C_1 \cup C_2, \\ U_{125} & = & R_1 \cup R_3 \cup R_4 \cup R_5 \cup R_6 \cup R_7 & = & C_1 \cup C_3, \\ U_{126} & = & R_2 \cup R_3 \cup R_4 \cup R_5 \cup R_6 \cup R_7 & = & C_2 \cup C_3. \end{array}$$

By Lemma 6, it is clear that $t(U_{119})$, $t(U_{125})$, and $t(U_{126})$ need to be specified for an ideal and perfect secret sharing scheme to exist, and they must satisfy

$$\begin{array}{rcl} t(U_{119}) & \geq & t_1 + t_2, \\ t(U_{125}) & \geq & t_1 + t_3, \text{ and} \\ t(U_{126}) & \geq & t_2 + t_3. \end{array}$$

Obviously, a threshold for $U = U_{127}$ must be specified too. A trivial inequality for $t(U_{127})$ is $t(U_{127}) \geq t(U_{119}) + t_3$, but it actually has a higher bound. Since U_{127} can be expressed as $U_{119} \cup U_{125}$, Lemma 6 states $t(U_{127}) \geq t(U_{119}) + t(U_{125})$ must hold. If we consider all possible union constructions of U_{127}, we have

$$\begin{array}{rcl} t(U_{127}) & \geq & t(U_{119}) + t(U_{125}), \\ t(U_{127}) & \geq & t(U_{119}) + t(U_{126}), \text{ and} \\ t(U_{127}) & \geq & t(U_{125}) + t(U_{126}) \end{array}$$

for an ideal and perfect secret sharing scheme to exist.

We will now extend Lemma 6 to the JCTASes that are not sufficiently populated. Since the transition from Lemma 6 to Lemma 7 is very similar to that from Lemma 4 to Lemma 5, we will not include the proof.

We have the following notation for the forthcoming lemma:

$$k_{ij} = \begin{cases} t(U_i) - |U_i - U_j| & \text{if } |U_i - U_j| < t(U_i) \\ 0 & \text{otherwise,} \end{cases}$$

where U_i, U_j are two regions that are neither nested nor disjoint. Also, we define

$$K_{ij} = \max(k_{ij}, k_{ji}).$$

Lemma 7. *Let Γ be a JCTAS with $\max(t(U_i), t(U_j)) > 1$ for all $U_i, U_j \in T$ that are neither nested nor disjoint. An ideal and perfect secret sharing scheme exists for Γ only if, for any two regions $U_i, U_j \in T$ that are neither nested nor disjoint, we have $U_i \cup U_j \in T$, and*

$$t(U_i \cup U_j) \geq t(U_i) + t(U_j) - K_{ij}.$$

Note that the necessary conditions given in this section are applicable to access structures that do not contain any two regions U_i, U_j that are neither nested nor disjoint and $t(U_i) = t(U_j) = 1$, as we have the constraint $\max(t_1, t_2) > 1$ in Lemma 4 and Lemma 5, by Remark 1. Recall that any access structure Γ can be seen as a JCTAS with the compartments being the minimal sets of the dual access structure Γ^* and with the thresholds being all equal to 1. Since we need $\max(t(U_i), t(U_j)) > 1$ for all regions U_i, U_j that are neither nested nor disjoint, our results do not claim to solve the problem of fully characterizing the ideal access structures in the general case.

5.1. An Ideal Perfect Scheme for $m \geq 3$

We will extend the scheme proposed in Section 4.1 for an arbitrary number of compartments, i.e. $m \geq 3$.

Note that T is the set of regions that have a threshold, and all regions in T satisfy the necessary condition proposed in Lemma 6. As in Section 4.1, the dimension of a region $U_i \in T$ is defined as

$$d_i = t(U_i) - \sum_{U_j \subset U_i} d_j,$$

and the smallest exponent of a region U_i is

$$e_i = \sum_{j<i} d_j.$$

Note that Lemma 6 guarantees that the dimension of a region is always non-negative.

The dealer selects a polynomial $f(x)$ of degree $t(U)-1$ such that $f(1) = s$. For f being represented as

$$f(x) = a_0 + a_1 x + \ldots + a_{t(U)-1} x^{t(U)-1},$$

the polynomial $f_i, 1 \leq i \leq 2^m - 1$ is

$$f_i(x) = \sum_{R_i \subseteq U_k} \sum_{j=e_k}^{e_k+d_k-1} a_j x^j,$$

which is a *masked* version of f. The share of a participant u in R_i is simply $s_u = f_i(u)$.

Let W' be an unqualified coalition. If $|W'| < t(U)$ and thus W' is unqualified, then they will have fewer equations than unknowns, hence they will not be able to find $s = f(1)$ with an overwhelming probability, as we show in Section 6.

Assume W' is of size $t(U)$ but does not meet the threshold for some region U_i. Since $t(U_i)$ of $t(U)$ dimensions are associated with regions U_j such that $U_j \subseteq U_i$, and equations regarding these dimensions (or unknowns) are given only to the participants that are contained in U_i, W' has more than $t(U) - t(U_i)$ equations regarding $t(U) - t(U_i)$ unknowns, which means some of the equations are redundant. Hence, this case is equivalent to the case $|W'| < t(U)$, i.e. W' gains no information about s with an overwhelming probability.

Example: Suppose $m = 3$, and the compartments are as in Figure 2. Let $t_1 = 3$, $t_2 = 2$, $t_3 = 2$, $t(U_{126}) = 5$, and $t(U_{127}) = 9$. Note that $t(U_{127}) \geq t_1 + t(U_{126})$.

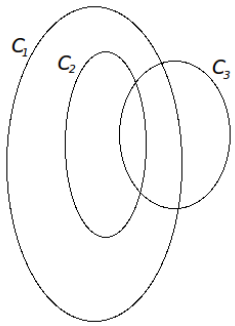

Figure 2: An example of $m = 3$

Given these values, the dimensions are as follows:

$$\begin{array}{lcll} d_{102} & = & 2 & (U_{102} = C_2), \\ d_{119} & = & 3 - 2 = 1 & (U_{119} = C_1 \cup C_2), \\ d_{120} & = & 2 & (U_{120} = C_3), \\ d_{126} & = & 5 - (2 + 2) = 1 & (U_{126} = C_2 \cup C_3), \\ d_{127} & = & 9 - (2 + 1 + 2 + 1) = 3 & (U_{127} = \bigcup_{i=1}^{3} C_i). \end{array}$$

The exponents of the regions are

$$\begin{array}{lcl} e_{102} & = & 0, \\ e_{119} & = & 2, \\ e_{120} & = & 3, \\ e_{126} & = & 5, \text{ and} \\ e_{127} & = & 6. \end{array}$$

Finally, the polynomials become as follows:

$$\begin{array}{lcl} f_1(x) & = & a_2x^2 + a_6x^6 + a_7x^7 + a_8x^8, \\ f_3(x) & = & a_0 + a_1x + a_2x^2 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8, \\ f_4(x) & = & a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8, \\ f_5(x) & = & a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8, \\ f_7(x) & = & a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 \\ & & + a_7x^7 + a_8x^8. \end{array}$$

6. Perfectness of the Proposed Scheme

Let us first state the Schwartz-Zippel Lemma, which will be used in the proofs of the perfectness of our scheme.

Lemma 8 (Schwartz-Zippel Lemma [12, 13]). *Let $G(x_1, x_2, \ldots, x_k)$ be a nonzero k-variate polynomial over $\mathbb{Z}_q$. Given that d is the highest degree of each variable of G, the number of zeros of G over $\mathbb{Z}_q^k$ is bounded from above by kdq^{k-1}.*

Recall that a secret sharing scheme is said to be perfect if

1. qualified coalitions find the secret uniquely and

2. unqualified coalitions gain no information about the secret.

We will analyze the perfectness of our scheme in Lemma 9 and Lemma 10. We will just give the sketches of the proofs since they are very similar to the proofs of Theorem 1 and Theorem 2 in [11].

Lemma 9. *A qualified subset W finds the secret s with probability at least $1 - t(t-1)/q$, where t is the overall threshold $t(U)$.*

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 $\{u_1, u_2, \ldots, u_t\}$ of degree $t-1$, where u_i's are the public identities of the participants in W. By Lemma 8, $\det(M_W)$ can be 0 for at most $t(t-1)q^{t-1}$ values in Z_q^t. A random selection of identities may lead to a singular M_W with probability at most $t(t-1)q^{t-1}/q^t = t(t-1)/q$, which means M_W is nonsingular with probability at least $1 - t(t-1)/q$. Hence, the result follows.

Lemma 10. *An unqualified subset W' gains no information about the secret s with probability at least $1-(t-1)^2/q$, where t is the overall threshold $t(U)$.*

PROOF. If $|W'| < t$, then $M_{W'}$ has fewer rows than columns. If $|W'| \geq t$ but $|W' \cap U_i| < t(U_i)$ for some U_i, they have at least $t - t(U_i) + 1$ equations regarding $t - t(U_i)$ unknowns, which means some of them are redundant: W' can ignore the shares of the *extra* participants. In both cases, the coefficient matrix $M_{W'}$ has fewer rows than columns.

Let's assume $M_{W'}$ has $t-1$ rows. Let $M'_{W'}$ be the augmented matrix $[\mathbf{1}^T M_{W'}^T]^T$ with $\mathbf{1}$ 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 8, as in Lemma 9.

7. Conclusion

In this work, we introduced joint compartmented threshold access structures which include conjunctive hierarchical threshold access structures and disjoint compartmented access structures as special cases. We gave necessary conditions regarding the existence of an ideal and perfect scheme for almost

all JCTASes. We also gave an ideal and perfect construction for the access structures that satisfy these necessary conditions.

There are still open problems not covered by our results: If a JCTAS contains two compartments that are neither nested nor disjoint with both having a threshold equal to 1, our results do not suggest anything about the existence of an ideal and perfect scheme. These cases are open problems for future research.

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

[2] G. Blakley, Safeguarding cryptographic keys, in: AFIPS National Computer Conference, 1979.

[3] G. J. Simmons, How to (really) share a secret, in: CRYPTO'88, Vol. 403 of LNCS, Springer-Verlag, London, UK, 1988, pp. 390–448.

[4] E. Brickell, Some ideal secret sharing schemes, in: EUROCRYPT'89, Vol. 434 of LNCS, Springer-Verlag, 1990, pp. 468–475.

[5] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, Secret sharing in multilevel and compartmented groups, in: ACISP'98, Vol. 1438 of LNCS, Springer-Verlag, London, UK, 1998, pp. 367–378.

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

[7] M. Ito, A. Saito, T. Nishizeki, Secret sharing scheme realizing general access structure, in: GLOBECOM'87, IEEE Press, 1987, pp. 99–102.

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

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

[10] O. Farrás, J. Martí-Farré, C. Padró, Ideal multipartite secret sharing schemes, in: EUROCRYPT 2007, Vol. 4515 of LNCS, pp. 448–465.

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

[12] J. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, Journal of the ACM 27 (4) (1980) 701–717.

[13] R. Zippel, Probabilistic algorithms for spare polynomials, in: EUROSAM'79, Marseille, 1979, pp. 216–226.