Joint Compartmented Threshold Access Structures

Ali Aydın Selçuk[1], **Ramazan Yılmaz**[2]

[1] *Bilkent University, Turkey* selcuk@cs.bilkent.edu.tr
[2] *Bilkent University, Turkey* ryilmaz@cs.bilkent.edu.tr

■ **Extended Abstract** ■

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 *compartmented* threshold access structure, where the user set is partitioned into compartments, 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 [6], and several secret sharing schemes realizing such access structures were proposed in [1, 3, 7].

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 [4]. 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 [6, 1, 3, 7]. 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 is as follows: In the rest of this section, we give a brief overview of compartmented access structures. In Section 2, we define JCTASes and introduce our notation. In Section 3 and Section 4, 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 in Section 5. We analyze the perfectness of the proposed construction in Section 6.

Definition 1. *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*

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

1.1 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 almost surely perfect secret sharing scheme for those JCTASes that satisfy the necessary conditions.

In this extended abstract, we give the main results of our study in lemmas and theorems. The proofs will be given in the full paper.

2 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 [6, 1, 3, 7]. 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

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

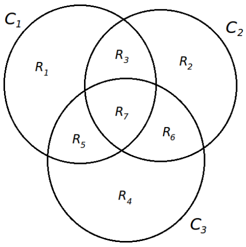

Figure 1: Simple regions for $m = 3$

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

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 3, we will first study the case of two compartments; then, in Section 4, 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.

3 Existence of Ideal Perfect Schemes for $m = 2$

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.

First, we will assume in Lemma 1 that there are at least t_1 and t_2 participants in R_1 and R_2, respectively. Then in Lemma 2, we will study the cases without this restriction.

Lemma 1. *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*

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

The next lemma is an extension of Lemma 1. 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 2. *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*

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

Note that our two-compartment JCTAS here is a special case of tripartite access structures, which have been studied in detail in [2]. The results in this section are significant because they lay the foundation for the results in Section 4 for arbitrary values of m and facilitate their comprehension.

4 Existence of Ideal Perfect Schemes for $m \geq 3$

In Section 3, 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 1 and Lemma 2 and show which JCTAS can be realized by an ideal and perfect secret sharing scheme.

Definition 2. *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 3. *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*

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

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 4. *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*

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

5 An Ideal Perfect Scheme

T is the set of regions that have a threshold, and note that all regions in T satisfy the necessary condition proposed in Lemma 3. 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 3 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 $s_u = f_i(u)$.

When the compartments are all disjoint, the scheme becomes identical to the one presented in [8]. When they are nested, the scheme corresponds to the one proposed in [5] for conjunctive hierarchical access structures.

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.

6 Perfectness of the Proposed Scheme

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.

Lemma 5. *A qualified subset W finds the secret s with probability at least $1 - t(t-1)/q$, where t is the overall threshold $t(U)$.*

Lemma 6. *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 $t(U)$.*

References

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

[2] Oriol Farrás, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. In *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 448–465, 2007.

[3] 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.

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

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

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

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

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