Secret Sharing in Multilevel and Compartmented Groups

Hossein Ghodosi, Josef Pieprzyk *, and Rei Safavi–Naini

Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522, AUSTRALIA
hossein/josef/rei@uow.edu.au

Abstract. The paper proposes efficient solutions to two long standing open problems related to secret sharing schemes in multilevel (or hierarchical) and compartmented access structures. The secret sharing scheme in multilevel access structures uses a sequence of related Shamir threshold schemes with overlapping shares and the secret. The secret sharing scheme in compartmented access structures applies Shamir schemes first to recover partial secrets and second to combine them into the requested secret. Both schemes described in the paper are ideal and perfect.

Key words. Secret Sharing, Hierarchical and Compartmented Access Structures, Ideal Schemes, Perfect Security.

1 Introduction

Secret sharing is normally used when either there is a lack of trust in a single person or the responsibility of a single person has to be delegated to a group during the absence of the person. Secret sharing can also be seen as a collective ownership of the secret by participants who hold shares of it. The access structure of a secret sharing defines all subsets of participants who are authorised to recover jointly the secret by pooling together their shares. Needless to say that any subset of unauthorised participants must not gain any knowledge about the secret. There is an important class of secret sharing where each participant holds their share of the same "weight". In other words, all participants are equal in their ability to recover the secret – this is the so-called threshold secret sharing. A t-out-of-n threshold secret sharing scheme, or simply a (t, n) scheme, allows to recover the secret by any t distinct participants while any $(t-1)$ or fewer participants fail to do so. Threshold schemes were independently introduced by Shamir [5] and Blakley [1].

Threshold schemes are suitable for democratic groups where every participant is assigned the same degree of trust. Most of the organisations, however, exhibit

* Support for this project was provided in part by the Australian Research Council under the reference number A49530480.

C. Boyd and E. Dawson (Eds.): ACISP'98, LNCS 1438, pp. 367–378, 1998.

a complex structure where the trust assigned to a given person is directly related to their position in the structure. Simmons [6] introduced *multilevel* t_i*-out-of-*n_i and *compartmented* t_i*-out-of-*n_i secret sharing schemes to model the recovery of secret in some practical situations where the trust is not distributed uniformly over the set of all participants.

In multilevel t_i-out-of-n_i secret sharing schemes, the set of all participants is divided into disjoint levels (classes). The i-th level contains n_i participants. The levels create a hierarchical structure. Any t_i participants on the i-th level can recover the secret. When the number of cooperating participants from the i-th level is smaller than t_i, say r_i, then $t_i - r_i$ participants can be taken from higher levels. For example, a bank may require the concurrence of two vice-presidents or three senior tellers to authenticate an electronic funds transfer (EFT). If there are only two senior tellers available, the missing one can be substituted by a vice president.

In compartmented t_i-out-of-n_i secret sharing schemes, there are several disjoint compartments each consisting of n_i participants. The secret is partitioned in such a way that its reconstruction requires cooperation of at least t_i participants in some (or perhaps all) compartments. Consider the example presented by Simmons in [6]. Let two countries agree to control the recovery of the secret (which may initiate a common action) by a secret sharing scheme. The secret can be recreated only if at least two participants from both compartments pool their shares together.

2 Related Work

The notion of compartmented secret sharing was introduced by Simmons [6]. The concept of multilevel (or hierarchical) secret sharing was considered by several authors (see, for example Shamir [5], Kothari [4] and Ito, Saito and Nishizeki [3]). Shamir [5] suggests that threshold schemes for hierarchical groups can be realized by giving more shares to higher level participants. Kothari [4] considered hierarchical threshold schemes in which a simple (t_i, n_i) threshold scheme is associated with the i-th level of a multilevel group. The obvious drawback of this solution is that it does not provide concurrency among different levels of hierarchical groups. Ito et al [3] discussed secret sharing for general access structures and proved that every access structure can be realized by a perfect secret sharing scheme. Their method, called *multiple assignment scheme*, may assign the same share to many participants. The main drawback of the multiple assignment scheme is that more privileged participants are given longer shares.

Simmons [6] pointed out that solutions for secret sharing in multilevel groups proposed so far were not efficient. He suggested efficient geometrical secret sharing schemes with the required properties. However, his solution is applicable only to a particular case of multilevel and compartmented groups. More precisely, he discussed secret sharing in multilevel and compartmented groups with particular access structures.

Brickell [2] studied general secret sharing in multilevel and compartmented groups and proved that it is possible to construct ideal secret sharing schemes for any multilevel and compartmented access structure. In Brickell's vector space construction, the dealer uses a function to provide publicly known vectors associated with corresponding participants. In general, finding such a function is a matter of trial and error, and therefore the dealer needs to check exponentially many possibilities. Brickell also found some lower bounds on the size of the modulus q (size of the field in which the calculations are being done) for which the construction of ideal secret sharing in general multilevel and compartmented access structures is possible. However, constructing efficient solution to these classes of secret sharing was left as an open problem.

This paper presents efficient solutions for secret sharing in general multilevel and compartmented groups. Our scheme is based on the Shamir scheme and is perfect and ideal. In our schemes, the lower bound on the modulus is significantly smaller than in Brickell's scheme. Indeed, the condition $q > n$ (as in original Shamir's scheme) is sufficient to implement our proposed schemes. Moreover, we do not require public vectors as in Brickell scheme. Although confidentiality of the public vectors is not required, in Brickell's scheme their integrity is nevertheless required.

The organisation of the paper is as follows. In Section 3 we introduce the notations and describe briefly the Shamir scheme. In Section 4 we consider multilevel access structures and describe an implementation of secret sharing in multilevel groups. We also give the lower bound on the modulus. In Section 5 we consider secret sharing in compartmented groups and present a scheme for a general compartmented access structure.

3 Background

The starting point of our method is the Shamir threshold scheme. The Shamir (t, n) threshold scheme uses polynomial interpolation. Let secrets be taken from the set $\mathcal{K} = GF(q)$ where $GF(q)$ is a finite Galois field with q elements. The Shamir scheme uses two algorithms: the dealer and combiner. The dealer sets up the scheme and distributes shares to all participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ via secure channels. The combiner collects shares from collaborating participants and computes the secret only if the set of cooperating participants is of size t or more.

To set up a (t, n) threshold scheme with $q > n$, a dealer chooses n distinct nonzero elements $x_1, \ldots, x_n \in GF(q)$ and publishes them. Next for a secret $K \in \mathcal{K}$, the dealer randomly chooses $t-1$ elements $a_1, \ldots, a_{t-1}$ from $GF(q)$ and forms the following polynomial:

$$f(x) = K + \sum_{i=1}^{t-1} a_i x^i.$$

The share of participant P_i is $s_i = f(x_i)$. The secret $K = f(0)$. Note that a_i are randomly chosen from all elements of $GF(q)$, so in general, $f(x)$ is of degree at most $t-1$.

During the reconstruction phase, the combiner takes shares of at least t participants $s_{i_1}, \ldots, s_{i_t}$, and solves the following system of equations:

$$\begin{aligned} K + a_1 x_{i_1} + \cdots + a_{t-1} x_{i_1}^{t-1} &= s_{i_1} \\ &\vdots \\ K + a_1 x_{i_t} + \cdots + a_{t-1} x_{i_t}^{t-1} &= s_{i_t} \end{aligned}$$

The Lagrange interpolation formula gives the expression for the secret K. It is known (see Stinson [7]) that the Shamir scheme is perfect. That is, if a group of fewer than t participants collaborate, their original uncertainty about K remains unchanged.

4 Secret Sharing in Multilevel Groups

Assume that a multilevel (or hierarchical) group consists of ℓ levels. That is, a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants is partitioned into ℓ disjoint subsets $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$. The subset $\mathcal{P}_1$ is on the highest level of hierarchy while $\mathcal{P}_\ell$ is on the least privileged level. Denote the number of participants on the i-th level as $n_i = |\mathcal{P}_i|$. The threshold t_i indicates the smallest number of participants on the i-th or higher levels, who can cooperate to successfully reconstruct the secret. The number of participants in the scheme is $n = |\mathcal{P}| = \sum_{i=1}^{\ell} |\mathcal{P}_i| = \sum_{i=1}^{\ell} n_i$. Let N_i be the total number of participants on the i-th and higher levels. That is, $N_i = \sum_{j=1}^{i} n_j$, $1 \le i \le \ell$. Clearly, $N_1 = n_1$ and $N_\ell = n$. Of course, we assume that the thresholds on different levels satisfy the following relation $t_1 < t_2 < \cdots < t_\ell$. Note that the reconstruction of secret can be initialised by any hierarchical subgroup of $\mathcal{P}_i$. If their number is smaller than the threshold number t_i, the subgroup can ask some participants from the higher levels to collaborate and pool their shares. The total number of participants has to be at least t_i. The access structure is defined as:

$$\Gamma = \{\mathcal{A} \subseteq \mathcal{P} \;\mid\; \sum_{j=1}^{i} |\mathcal{A} \cap \mathcal{P}_j| \ge t_i \;\text{ for }\; i = 1, \ldots, \ell\}. \tag{1}$$

Consider again the bank example where monetary transactions can be authenticated by three senior tellers or two vice presidents. So there exist two levels of hierarchy. The first (highest) level consists of two vice presidents $\mathcal{P}_1 = \{P_1, P_2\}$ with $n_1 = 2$. The second (lowest) level consists of three senior tellers $\mathcal{P}_2 = \{P_3, P_4, P_5\}$ with $n_2 = 3$. To recover the secret, it is necessary that either two participants on the first level or three participants on the second level or three participants on the both levels pool their shares. Thus, $t_1 = 2$, $t_2 = 3$ and $n = 5$.

Definition 1. *Let A and B be two secret sharing schemes associated with a common secret K. The schemes A and B are (t_a, n_a) and (t_b, n_b) threshold schemes, respectively. We say B is an extension of A if any collection of at least t_b shares from the set of all shares generated in both schemes A and B is sufficient to reconstruct the secret K.*

In other words, the scheme B is an extension of the scheme A if:

(a) both schemes allow to recover the same secret,
(b) the collection of shares defined in A is a subset of shares generated in B, and
(c) any access set in A is an access set in B.

Lemma 1. (transitivity of extension) *If B is an extension of A and C is an extension of B then C is an extension of A.*

We say C is the second extension of A. Similarly, we define the ith extension of a threshold scheme.

4.1 The Model

Secret sharing for multilevel access structures displays some common features with threshold schemes. However, an implementation of multilevel secret sharing based on a sequence of independent (t_i, n_i) threshold schemes on each level $i = 1, \ldots, \ell$ makes the cooperation among participants existing on different levels difficult to achieve. Denote by

$$\mathcal{P}^i = \bigcup_{j=1}^{i} \mathcal{P}_j$$

the set of all participants on the i-th and all higher levels. An alternative implementation of secret sharing for multilevel access structures would involve a sequence of independent threshold schemes (t_i, N_i) for the set $\mathcal{P}^i$ $(i = 1, \ldots, \ell)$ of participants. This solution requires $\ell - i + 1$ shares to be assigned to each participant on the i-th level.

A reasonable implementation of secret sharing for a multilevel access structure can be done as follows. First a (t_1, n_1) threshold scheme (scheme A_1) is designed. It corresponds to the first (highest) level of participants from $\mathcal{P}^1$. Then a (t_2, N_2) threshold scheme (scheme A_2) for $\mathcal{P}^2$ is constructed as an extension of A_1. Next a (t_3, N_3) threshold scheme (scheme A_3) for $\mathcal{P}^3$ is constructed as an extension of A_2. The process continues until a (t_ℓ, N_ℓ) threshold scheme (scheme A_ℓ) for $\mathcal{P}^\ell$ is constructed by extending the threshold scheme $A_{\ell-1}$. In this implementation, each participant will be assigned a single share only.

4.2 The Multilevel Secret Sharing Scheme

Our model utilises a sequence of related Shamir threshold schemes with overlapping shares. Since we require shares corresponding to the basic scheme to be still acceptable in the extended schemes, care needs to be exercised to avoid any information leakage in the system.

Let a Shamir (t_1, N_1) threshold scheme be designed for $\mathcal{P}^1$ (as in original Shamir scheme). That is, a polynomial $f_1(x)$ of degree at most $t_1 - 1$ is associated with this scheme. Let $f_1(x) = K + a_{1,1}x + \cdots + a_{1,T_1}x^{T_1}$, where $T_1 = t_1 - 1$. Let us extend this scheme to a (t_2, N_2) threshold scheme, for the set $\mathcal{P}^2$. In the following we show how to select a polynomial $f_2(x)$ of degree T_2 such that every subset of t_2, or more, participants from the set $\mathcal{P}^2$ can recover the secret, but for every subset of less that t_2 participants the secret remains absolutely undetermined. As we shall see in a moment, in general, $T_2 > t_2 - 1$.

Let $f_2(x) = K + a_{2,1}x \cdots + a_{2,T_2}x^{T_2}$. Since $f_2(x_i) = f_1(x_i)$ for all x_i $(1 \le i \le N_1)$, the following set of $2 \times N_1$ equations are known.

$$\text{From } f_1(x) \begin{cases} K + a_{1,1}x_1 + \cdots + a_{1,T_1}x_1^{T_1} = s_1 \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ K + a_{1,1}x_{N_1} + \cdots + a_{1,T_1}x_{N_1}^{T_1} = s_{N_1} \end{cases}$$

$$\text{From } f_2(x) \begin{cases} K + a_{2,1}x_1 + \cdots + a_{2,T_2}x_1^{T_2} = s_1 \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ K + a_{2,1}x_{N_1} + \cdots + a_{2,T_2}x_{N_1}^{T_2} = s_{N_1} \end{cases}$$

The number of unknowns in this system of equations is $1 + T_1 + T_2 + N_1$. The system has a unique solution if the number of equations is equal to (or greater than) the number of unknowns. However, the requirement is that at least t_2 participants from the set $\mathcal{P}_2$ must collaborate in order to recover the secret. Let a set $\mathcal{A} \subset \mathcal{P}_2$ $(|\mathcal{A}| = t_2)$ of participants includes the set of following t_2 equations into the system (each participant contributes with one equation).

$$\text{From } f_2(x) \begin{cases} K + a_{2,1}x_{j_1} + \cdots + a_{2,T_2}x_{j_1}^{T_2} = s_{j_1} \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ K + a_{2,1}x_{j_{t_2}} + \cdots + a_{2,T_2}x_{j_{t_2}}^{T_2} = s_{j_{t_2}} \end{cases}$$

where $N_1 + 1 \le j_i \le N_2$ $(1 \le i \le t_2)$.

Now, we want that the above set of $2 \times N_1 + t_2$ equations has a unique solution for K. This requires that $2 \times N_1 + t_2 = 1 + T_1 + T_2 + N_1$ (note that the later set of t_2 equations does not increases the number of unknowns). So, the dealer can select a suitable value for T_2 (knowing N_1, T_1, and t_2).

Although we have shown that if t_2 participants from the set $\mathcal{P}_2$ collaborate, then they can determine the secret, we must show that every subset of t_2 participants from the set $\mathcal{P}^2$ (i.e. $\mathcal{P}_1 \cup \mathcal{P}_2$) can also do so. Let j participants $(0 < j < t_2)$ from the set $\mathcal{P}_2$ collaborate in the secret reconstruction process.

Thus, $t_2 - j$ participants from the set $\mathcal{P}_1$ must collaborate in the secret reconstruction. Although this decreases the number of unknown shares $s_1, \ldots, s_{N_1}$ by $t_2 - j$, the number of unknown shares in the system is still N_1 (since $t_2 - j$ shares regarding to the absent participants are now unknown). That is, for every subset of t_2 participants from the set $\mathcal{P}^2$ the above set of equations has N_1 unknown shares.

So, the extended scheme can be constructed if T_2 is chosen such that $t_2 + 2N_1 = 1 + T_1 + T_2 + N_1$, or simply,

$$T_2 = N_1 + (t_2 - t_1). \tag{2}$$

To construct the polynomial $f_2(x)$, the dealer first selects T_2 random coefficients $a_{2,1}, \ldots, a_{2,T_2}$ such that $f_2(x) = K + a_{2,1}x + \cdots + a_{2,T_2}x^{T_2}$ satisfies $f_2(x_i) = f_1(x_i)$, $1 \le i \le N_1$. Next, it selects n_2 distinct and non zero elements x_i $(N_1 + 1 \le i \le N_2)$, such that $x_i \ne x_j$ $(i \ne j,\ 1 \le i, j \le N_2)$ and computes shares $s_i = f_2(x_i)$ $(N_1 + 1 \le i \le N_2)$. Then, the dealer privately sends the shares to the corresponding participants (only to the new n_2 participants of the extended scheme).

The polynomial $f_2(x)$ is constructible if $T_2 \ge T_1 + 2$. Because, the condition $f_2(x_i) = f_1(x_i)$, $1 \le i \le N_1$ is equivalent to:

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{T_2-1} \\ 1 & x_2 & \ldots & x_2^{T_2-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{T_1} & \ldots & x_{T_1}^{T_2-1} \end{pmatrix} \begin{pmatrix} a_{2,1} - a_{1,1} \\ a_{2,2} - a_{1,2} \\ \vdots \\ a_{2,T_1} - a_{1,T_1} \\ a_{2,T_1+1} \\ \vdots \\ a_{2,T_2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

If $T_2 \ge T_1 + 2$, then $T_1 \times T_2$ matrix above has rank $T_1 < T_2 - 1$, and hence the dealer can select $a_{2,1}, \ldots, a_{2,T_2}$ as desired. However, considering equation (2) and the fact that $N_1 \ge t_1$ (this is a basic condition in Shamir scheme), we have, $T_2 \ge t_2$. Since $t_2 > t_1$ (otherwise, the dealer just generates n_2 shares in the constructed scheme (t_1, N_1) scheme and sends them to their correspondence), we have $T_2 > t_1$. On the other hand, $t_1 = T_1 + 1$. Therefore, $T_2 > T_1 + 1$, which implies $T_2 \ge T_1 + 2$. We thus obtain the following theorem.

Theorem 1. *In multilevel structures, there exists a Shamir (t_i, N_i) threshold scheme that realizes the secret sharing for level i and all higher levels.*

That is, our model is applicable for any multilevel (hierarchical) access structure. We use $(t_i, N_i)_{T_i}$ scheme to denote an extended Shamir (t_i, N_i) threshold scheme in which the polynomial associated with the scheme has a degree of at most T_i (in general, $T_i > t_i$).

At level i, the dealer easily can calculate the value T_i, which is the degree of the polynomial associated with a $(t_i, N_i)_{T_i}$ threshold scheme for $\mathcal{P}^i$. The dealer

observes that the available set of equations with the system is as follows: N_1 equations (for level 1) with T_1 (maximum number of coefficients in $f_1(x)$); N_2 equations (for level 2) with T_2 unknowns and, in general, N_{i-1} equations (for level $i-1$) with T_{i-1} unknowns (plus one unknown, corresponding to the secret itself). Since the requirement is that at least t_i participants must collaborate in order to recover the secret, T_i must must satisfy the following equality:

$$t_i + \sum_{j=1}^{i-1} N_j = 1 + \sum_{j=1}^{i} T_j \tag{3}$$

which contains a single unknown value, T_i (all T_j, $1 \leq j \leq i-1$ have been calculated in previous levels).

Hence, a secret sharing for a given multilevel access structure can be implemented according to the following algorithm:

Algorithm 1 – a $(t_i, N_i)_{T_i}$ secret sharing scheme.

1. Select at random a polynomial of degree at most $T_1 = t_1 - 1$ and compute n_1 shares for n_1 participants from $\mathcal{P}_1$. The outcome is a $(t_1, N_1)_{T_1}$ threshold scheme ($N_1 = n_1$).
2. For $i = 2$ to ℓ do:
   - for the given initial $(t_{i-1}, N_{i-1})_{T_{i-1}}$ threshold scheme, construct its extension $(t_i, N_i)_{T_i}$.
   - compute n_i shares for participants on the i-th level,
   - take the next i,
3. Distribute the shares to corresponding participants via secure channels.

4.3 Security

The following theorem demonstrates that secret sharing schemes obtained using Algorithm 1 are perfect.

Theorem 2. *Algorithm 1 produces an ideal and perfect secret sharing scheme for an arbitrary multilevel access structure.*

Proof. (Sketch) Algorithm 1 produces ℓ threshold schemes $A_1, \ldots, A_\ell$, where:

A_1 is defined by polynomial $f_1(x)$ for $\mathcal{P}_1$,
A_i is defined by polynomial $f_i(x)$ for $\mathcal{P}^i = \bigcup_{j=1}^{i} \mathcal{P}_j$, and

$f_i(x) = K + a_{i,1}x + \ldots + a_{i,T_i}x^{T_i}$ for $i = 1, \ldots, \ell$.

Without loss of generality, we can assume $\mathcal{B} = \{P_1, \ldots, P_w\} \notin \Gamma$ are the collaborating participants. For each level, we can determine $\mathcal{B}_i = \mathcal{B} \cap \mathcal{P}^i$ and the number $\beta_i = |\mathcal{B}_i|$. Clearly, $\beta_i < t_i$. So, each system of equations for the i-th level does not produce a unique solution. Indeed, according to the method of generating polynomials associated with Shamir threshold scheme for level i, every subset of all equations available to the set $\mathcal{B}$ has more unknowns than the number of equations, and therefore, has no unique solution. That is, the solution is a space equivalent to $GF(q)$, and thus, the secret remains absolutely undetermined.

4.4 The Lower Bound on the Modulus

Brickell proved [2, Theorem 1] that there exists an ideal secret sharing scheme for a multilevel access structure over $GF(q)$ if:

$$q > (\ell - 1)\binom{n}{\ell - 1}.$$

It is easy to show that in the construction by Algorithm 1, the above condition on size q can be significantly improved.

Corollary 1. *Let Γ be a multilevel access structure with ℓ levels. Given the secret sharing scheme for Γ implemented by the sequence of threshold schemes $A_1, \ldots, A_\ell$, and created according to Algorithm 1. That is, A_i is a $(t_i, N_i)_{T_i}$ threshold scheme. Thus, the lower bound of q in the scheme is given by, $q > T_\ell$*

Now, we give a simple assessment of the required lower bound for q in our scheme. ¿From equation (3), since $t_\ell < N_\ell$, we have $\sum_{j=1}^{i} T_j < \sum_{j=1}^{i} N_j$ $(i = 1, \ldots, \ell)$. That is, in general, $T_i < N_i$, and therefore, $T_\ell < N_\ell$. In other words, the basic condition of the original Shamir scheme, that is,

$$q > n$$

is sufficient to implement our scheme (since $N_\ell = n$).

5 Secret Sharing in Compartmented Groups

Let the set of participants $\mathcal{P}$ be partitioned into ℓ disjoint sets $\mathcal{P}_1, \ldots, \mathcal{P}_\ell$. The compartmented access structure Γ is defined as follows.

Definition 2. *A subset $\mathcal{A} \subset \mathcal{P}$ belongs to the access structure Γ if:*

1. $|\mathcal{A} \cap \mathcal{P}_i| \geq t_i$ *for* $i = 1, \ldots, \ell$, *and*
2. $|\mathcal{A}| = t$ *where* $t \geq \sum_{i=1}^{\ell} t_i$.

The numbers of participants in different compartments and integers $t, t_1, \ldots, t_\ell$ determine an instance of the compartmented access structure.

We consider two distinct cases.

5.1 Case $t = \sum_{i=1}^{\ell} t_i$

In this case the access structure is:

$$\Gamma = \{A \subseteq \mathcal{P} \quad | \quad |A \cap \mathcal{P}_i| \geq t_i \quad \text{for} \quad i = 1, \ldots, \ell\} \tag{4}$$

A trivial solution for the above access structure is as follows. The dealer simply chooses $\ell - 1$ random values $c_1, \ldots, c_{\ell-1}$ from elements of $GF(q)$, and defines a polynomial,

$$\kappa(x) = K + c_1 x + \ldots + c_{\ell-1} x^{\ell-1}.$$

The secret $K = \kappa(0)$ and the partial secrets $k_i = \kappa(i)$ for $i = 1, \ldots, \ell$. The dealer constructs a Shamir (t_i, n_i) scheme for each compartment i. The schemes are independently designed and the scheme in the i-th compartment allows to recover the partial key k_i. The collection of shares for all compartments are later distributed securely to the participants. Obviously, if at least t_i participants of the i-th compartment pool their shares, they can reconstruct the partial secret k_i. A group of fewer than t_i collaborating participants learns absolutely nothing about k_i. Thus, the reconstruction of the secret K needs all partial keys to be reconstructed by at least t_i participants in each compartment i $(i = 1, \ldots, \ell)$.

Similar solution was proposed by Brickell [2]. However, prior to the results described here, no efficient solution has been proposed for a general compartmented access structure in which $t > \sum_{i=1}^{\ell} t_i$.

5.2 Case $t > \sum_{i=1}^{\ell} t_i$

The corresponding access structure is:

$$\Gamma = \{A \subseteq \mathcal{P} \quad | \quad |A| \geq t, \ |A \cap \mathcal{P}_i| \geq t_i \quad \text{for} \quad i = 1, \ldots, \ell\} \tag{5}$$

Let $T = t - \sum_{i=1}^{\ell} t_i$. The secret sharing scheme for a compartmented access structure Γ is designed according to the following algorithm.

Algorithm 2 – a $(t_i, n_i|t; i = 1, \ldots, \ell)$ secret sharing scheme.

1. Choose $\ell - 1$ random values $c_1, \ldots, c_{\ell-1} \in GF(q)$ and define the polynomial,

$$\kappa(x) = K + c_1 x + \ldots + c_{\ell-1} x^{\ell-1}.$$

   The secret $K = \kappa(0)$ and the partial secrets $k_i = \kappa(i)$ for $i = 1, \ldots, \ell$.
2. Select randomly and uniformly $t_i - 1$ values $a_{i,1}, \ldots, a_{i,t_i-1}$ from $GF(q)$ corresponding to each level i, $i = 1, \ldots, \ell$,
3. Choose randomly and uniformly T values $\beta_1, \ldots, \beta_T$ from $GF(q)$,
4. Determine a sequence of ℓ polynomials,

$$f_i(x) = k_i + a_{i,1} x + \cdots + a_{i,t_i-1} x^{t_i-1} + \beta_1 x^{t_i} + \cdots + \beta_T x^{t_i+T-1}$$

   for every level i.
5. Compute shares for all compartments, i.e. $s_{i_j,i} = f_i(x_{i_j,i})$ for $j = 1, \ldots, n_i$ and $i = 1, \ldots, \ell$ $(n_i = |\mathcal{P}_i|)$ and send them securely to the participants.

Theorem 3. *The secret sharing scheme obtained from Algorithm 2 for a compartmented access structure Γ of the form given by equation (5) is ideal and perfect and allows to recreate the secret only if the set of cooperating participants $\mathcal{A} \in \Gamma$.*

Proof. (Sketch) First we prove that if $\mathcal{A} \in \Gamma$, then the participants from $\mathcal{A}$ can recover the secret K. Note that to determine the secret K, each compartment needs to recover its associated partial secret k_i.

Since $\mathcal{A} \in \Gamma$, there must be at least t_i collaborating participants from each compartment. Let the actual numbers of collaborating participants be $\alpha_1, \ldots, \alpha_\ell$, such that $\alpha_i \geq t_i$ and $\sum_{i=1}^{\ell} \alpha_i \geq t$. The combiner who collects all shares from participants in $\mathcal{A}$ can establish the following system of linear equations:

$$
\begin{cases}
k_1 + a_{1,1}x_{i_1,1} + \cdots + a_{1,t_1-1}x_{i_1,1}^{t_1-1} + \beta_1 x_{i_1,1}^{t_1} + \cdots + \beta_T x_{i_1,1}^{t_1+T-1} = s_{i_1,1} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
k_1 + a_{1,1}x_{i_{\alpha_1},1} + \cdots + a_{1,t_1-1}x_{i\alpha_1,1}^{t_1-1} + \beta_1 x_{i_{\alpha_1},1}^{t_1} + \cdots + \beta_T x_{i_{\alpha_1},1}^{t_1+T-1} = s_{i_{\alpha_1},1}
\end{cases}
$$

$$
\vdots
$$

$$
\begin{cases}
k_\ell + a_{\ell,1}x_{i_1,\ell} + \cdots + a_{\ell,t_{\ell-1}}x_{i_1,\ell}^{t_\ell-1} + \beta_1 x_{i_1,\ell}^{t_\ell} + \cdots + \beta_T x_{i_1,\ell}^{t_\ell+T-1} = s_{i_1,\ell} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
k_\ell + a_{\ell,1}x_{i_{\alpha_\ell},1} + \cdots + a_{1,t_\ell-1}x_{i\alpha_\ell,1}^{t_\ell-1} + \beta_1 x_{i_{\alpha_\ell},1}^{t_\ell} + \cdots + \beta_T x_{i_{\alpha_\ell},1}^{t_\ell+T-1} = s_{i_{\alpha_\ell},\ell}
\end{cases}
$$

In the above system of equations, t_i unknown coefficients $k_i, a_{i,j}$ $(j = 1, \ldots, t_i - 1)$ are associated with compartment i, $i = 1, \ldots, \ell$. The T unknown β_i are common in all equations. Since we have at least t equations with t unknowns, the system has a unique solution. Knowing partial secrets k_i, the secret K can be recovered.

Assume that $\mathcal{A} \notin \Gamma$. Then there are two possibilities. The first possibility is that there is a compartment i for which $\alpha_i < t_i$. This immediately implies that the corresponding partial key k_i cannot be found. The second possibility is that all $\alpha_i \geq t_i$, but $\sum_{i=1}^{\ell} \alpha_i < t$. This precludes the existence of the unique solution for $\beta_1, \ldots, \beta_T$.

5.3 The Lower Bound on the Modulus

Brickell showed that [2, Theorem 3] there exists an ideal secret sharing scheme for a compartmented access structure over $GF(q)$ if:

$$q > \binom{n}{t}$$

where n and t are the the same as in our scheme. In our proposed scheme, independent Shamir schemes are constructed for every compartment. Since $t_i + T < n$, it is easy to derive the following corollary.

Corollary 2. *Let Γ be a compartmented access structure with ℓ levels and $n = |\mathcal{P}|$ participants. Then there is an ideal secret sharing scheme for Γ over $GF(q)$ if:*

$$q > n.$$

Acknowledgements

The first author would like to thank the University of Tehran for financial support of his study.

References

1. G. Blakley, "Safeguarding cryptographic keys," in *Proceedings of AFIPS 1979 National Computer Conference*, vol. 48, pp. 313–317, 1979.
2. E. Brickell, "Some Ideal Secret Sharing Schemes," in *Advances in Cryptology - Proceedings of EUROCRYPT '89* (J.-J. Quisquater and J. Vandewalle, eds.), vol. 434 of *Lecture Notes in Computer Science*, pp. 468–475, Springer-Verlag, 1990.
3. M. Ito, A. Saito, and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," in *Proceedings IEEE Global Telecommun. Conf., Globecom '87, Washington*, pp. 99–102, IEEE Communications Soc. Press, 1987.
4. S. Kothari, "Generalized Linear Threshold Scheme," in *Advances in Cryptology - Proceedings of CRYPTO '84* (G. Blakley and D. Chaum, eds.), vol. 196 of *Lecture Notes in Computer Science*, pp. 231–241, Springer-Verlag, 1985.
5. A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, pp. 612–613, Nov. 1979.
6. G. Simmons, "How to (Really) Share a Secret," in *Advances in Cryptology - Proceedings of CRYPTO '88* (S. Goldwasser, ed.), vol. 403 of *Lecture Notes in Computer Science*, pp. 390–448, Springer-Verlag, 1990.
7. D. Stinson, "An Explication of Secret Sharing Schemes," *Designs, Codes and Cryptography*, vol. 2, pp. 357–390, 1992.