Ideal Hierarchical (t, n) Secret Sharing Schemes

Changlu Lin[*,a,c], Lein Harn[b], Dingfeng Ye[a]

[a] *State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing, 10049, P.R.China*
[b] *Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, MO 64110, USA*
[c] *Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fujian, 35007, P.R.China*

Abstract

A secret sharing scheme divides a secret into multiple shares by a dealer and shared among shareholders in such a way that any authorized subset of shareholders can reconstruct the secret; whereas any un-authorized subset of shareholders cannot recover the secret. If the maximal length of shares is equal to the length of the secret in a secret sharing scheme, the scheme is called *ideal*. If the shares corresponding to each un-authorized subset provide absolutely no information, in the information-theoretic sense, the scheme is called *perfect*. Shamir proposed the first (t, n) threshold secret sharing scheme and it is ideal and perfect. In this paper, we propose two modifications of Shamir's secret sharing scheme. In our first modification, each shareholder keeps both x-coordinate and y-coordinate of a polynomial as private share. In our second modification, dealer uses polynomial with degree *larger* than the threshold value t to generate shares for a (t, n) threshold scheme. We show that these

[*]Corresponding author. Tel: +86-134-6672-0505, Fax: +86-10-88258713.
Email addresses: lincl@is.ac.cn (Changlu Lin), harnl@umkc.edu (Lein Harn), ydf@is.ac.cn (Dingfeng Ye)

two modified schemes are ideal and perfect. Using these two modifications, we design two hierarchical secret sharing schemes: *multilevel threshold secret sharing* (MTSS), and *compartmented threshold secret sharing* (CTSS). We prove that these two schemes are secure.
Key words: Secret sharing, threshold secret sharing, hierarchical secret sharing, multilevel secret sharing, compartmented secret sharing

---

1. Introduction

A secret sharing scheme divides a secret s into n shares by a *dealer* D and shared among a set of of n *shareholders*, $\mathcal{P} = \{P_1, \ldots, P_n\}$, in such a way that any authorized subset can reconstruct the secret; whereas any unauthorized subset cannot recover the secret s. The (t, n) threshold secret sharing schemes were introduced by Shamir [11] and Blakley [2] independently in 1979. A (t, n) threshold secret sharing scheme allows any t or more than t shareholders to reconstruct the secret s; while any fewer than t shareholders cannot reconstruct the secret s. In Shamir's (t, n) threshold scheme, a dealer generates n shares based on a $(t-1)$-th degree polynomial. Secret reconstruction is based on Lagrange interpolating polynomial of any t private shares.

The length of shares in a secret sharing should be as small as possible. Smaller shares are easier to store and manage. Brickell and Davenport [4] claimed that the length of any share is larger than or equal to the length of the secret. The secret sharing scheme is called *ideal* if the maximal length of shares and the length of the secret are identical. There exists a relationship between ideal secret sharing scheme and matroids [4]. It is easy to know that

Shamir's threshold secret sharing scheme is ideal.

A threshold scheme is *perfect* if any $(t-1)$ or fewer than $(t-1)$ shareholders who work together with their corresponding shares cannot get any information, in the information-theoretic sense, about the secret. Karnin *et al.* [7] have shown that in all perfect schemes, the minimal length of shares must be no less than the length of the secret. Shamir's threshold secret sharing scheme is perfect.

Hierarchical threshold secret sharing scheme is a generalization of simple threshold secret sharing scheme, and it has been studied extensively in the literature [1; 3; 5; 6; 8; 10; 12; 13; 14]. In a hierarchical threshold secret sharing scheme, all shareholders play different roles; while in a simple threshold secret sharing scheme all shareholders play the same role. In this paper, we will focus on the following two types of hierarchical threshold secret sharing schemes: *multilevel threshold secret sharing* (MTSS), and *compartmented threshold secret sharing* (CTSS).

Simmons [10] considered a setting where all shareholders are partitioned into different levels, $L_1, \ldots, L_m$, and each level L_i is assigned with a threshold value t_i, for $i = 1, \ldots, m$. He further defined two secret sharing schemes: MTSS scheme and CTSS scheme. In MTSS scheme, when there are at least t_i shareholders belonging to levels smaller than or equal to L_i, this subset of shareholders can reconstruct the secret. For example, when thresholds are $t_1 = 2$ at level $L_1$and $t_2 = 3$ at level L_2, then two shareholders at L_1, or three shareholders at L_2 can reconstruct the secret. In addition, when there are one shareholder at L_1 and two shareholders at L_2, this combination of shareholders can also reconstruct the secret. In CTSS scheme, when there

are $t \geq \sum_{j=1}^{m} t_j$ shareholders in total and these shareholders also satisfy the requirements that at least t_i shareholders for each compartment C_i, for $i = 1, \ldots, m$, this combination of shareholders can reconstruct the secret.

Brickell [3] proposed an ideal MTSS scheme and an ideal CTSS scheme. However, both schemes are inefficient since dealer is required to compute exponentially to ensure non-singular matrices. Ghodosi *et al.* [6] proposed an ideal MTSS scheme and an ideal CTSS scheme based on Shamir's threshold scheme; but their schemes only work for small number of shareholders. Recently, Tassa [12] considered a special case of CTSS scheme (also called *conjunctive threshold secret sharing*) using polynomial derivative based on Birkhoff interpolation, and that scheme is ideal.

In this paper, we propose two modifications of Shamir's secret sharing scheme. In our first modification, each shareholder keeps both x-coordinate and y-coordinate of a polynomial as private share. In our second modification, dealer uses a polynomial with degree *larger* than the threshold value t to generate shares for a (t, n) threshold scheme. Secret reconstruction is based on any t private shares along with some public shares. We show that these two modified secret sharing schemes are ideal and perfect. Using these two modifications, we design an ideal MTSS scheme and an ideal CTSS scheme. Our proposed schemes will use a polynomial to generate shares for shareholders and use Lagrange interpolating polynomial to reconstruct the secret. We prove that these two schemes are secure.

Organization of the paper: In the next section, we provide some fundamental definitions and notations. In Section 3, we introduce two modifications of Shamir's threshold scheme. In Section 4, we propose our MTSS

scheme and CTSS scheme. We conclude in Section 5.

2. Definitions and Notations

In this section, we first review Shamir's threshold secret sharing scheme. Then, we give some fundamental definitions of hierarchical threshold secret sharing schemes.

In Shamir's (t, n) scheme based on Lagrange interpolating polynomial, there are n shareholders, $\mathcal{P} = \{P_1, \ldots, P_n\}$, and a dealer D. The scheme consists of two steps:

1. Share generation: dealer D first picks a polynomial $f(x)$ of degree $(t-1)$ randomly: $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$, in which the secret $s = a_0$ and all coefficients $a_0, a_1, \ldots, a_{t-1}$ are in a finite field $\mathbb{F}_p = GF(p)$ with p elements, where $s < p$, and D computes:

$$s_1 = f(1), s_2 = f(2), \ldots, s_n = f(n).$$

   Then, D outputs a list of n shares, $(s_1, s_2, \ldots, s_n)$, and distributes each share s_i to corresponding shareholder P_i privately.

2. Secret reconstruction: with any t shares, $(s_{i_1}, \ldots, s_{i_t})$, where $A = \{i_1, \ldots, i_t\} \subseteq \{1, 2, \ldots, n\}$ can reconstruct the secret s as follows.

$$\begin{aligned} s = f(0) &= \sum_{i \in A} s_i \beta_i \\ &= \sum_{i \in A} s_i \Big(\prod_{j \in A - \{i\}} \frac{x_j}{x_j - x_i} \Big), \end{aligned}$$

   where β_i for $i \in A$ are Lagrange coefficients.

We note that the above scheme satisfies basic requirements of secret sharing scheme as follows: 1) with knowledge of any t or more than t shares, it can reconstruct the secret s; and 2) with knowledge of any fewer than t shares, it cannot reconstruct the secret s. Shamir's scheme is *information-theoretically secure* since the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, readers can refer to the original paper [11].

Definition 1 (Information rate)**.** *Information rate of a secret sharing scheme is the ratio between the length, in bits, of the secret and the maximal length of shares distributed to shareholders. Let a be the number of bits of the secret and $b = \max_{i\in\{1,\ldots,n\}}\{b_i\}$ be the number of bits of maximal share. The information rate is defined as*

$$\rho = \frac{a}{b}.$$

The secret sharing scheme is ideal *if $\rho = 1$.*

Definition 2 (Perfect threshold secret sharing [9])**.** *We say that a (t, n) threshold secret sharing scheme is* perfect *if any $(t-1)$ or fewer than $(t-1)$ shareholders who work together with their corresponding shares cannot get any information, in the information-theoretic sense, about the secret.*

Shamir's secret sharing scheme is perfect. If we use entropy to describe this perfect secret property of threshold secret sharing scheme, Karnin *et al.* [7] have shown that in all perfect schemes, the length of share must be larger than or equal to the length of the secret s. In other words, the information rate, (length of the secret)/(maximal length of shares), of all perfect schemes is no more than 1.

Definition 3 (Multilevel threshold secret sharing). *Let* $\mathcal{L} = \{L_1, \ldots, L_m\}$ *denote a partition of shareholders* $\{P_1, \ldots, P_n\}$ *into multiple security levels,* i.e., $\mathcal{P} = \{P_1, \ldots, P_n\} = \cup_{j=1}^{m} L_j$. *Let* $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$ *denote a sequence of threshold values where* $1 \leq t_j \leq |L_1| + \cdots + |L_j|$ *for* $1 \leq j \leq m$ *and* $t_1 < t_2 < \cdots < t_m$. *The authorized set* $\mathcal{MA}$ *of* n *shareholders in a* $(\mathcal{L}, \mathcal{T})$ *multilevel threshold secret sharing (MTSS) scheme is defined as*

$$\mathcal{MA} = \{A \subseteq \{P_1, \ldots, P_n\} | \ \exists i \in \{1, \ldots, m\}$$

$$and \ \ |A \cap (\cup_{j=1}^{i} L_j)| \geq t_i\},$$

where $A = \{P_{i_1}, \ldots, P_{i_t}\}$ *and* $P_{i_k} \neq P_{i_l}$ *if* $k \neq l$ *for any subset* $\{i_1, \ldots, i_t\}$ *of* $\{1, \ldots, n\}$.

Definition 4 (Compartmented threshold secret sharing). *Let* $\mathcal{C} = \{C_1, \ldots, C_m\}$ *denote a partition of shareholders* $\{P_1, \ldots, P_n\}$ *into multiple security compartments,* i.e., $\mathcal{P} = \{P_1, \ldots, P_n\} = \cup_{j=1}^{m} C_j$. *Let* $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$ *denote a sequence of compartmented threshold values, where* $1 \leq t_j \leq |C_j|$ *for* $1 \leq j \leq m$, *and* t *denote the total threshold value with* $\sum_{j=1}^{m} t_j \leq t \leq n$. *The authorized set* $\mathcal{CA}$ *of* n *shareholders in a* $(\mathcal{C}, \mathcal{T})$ *compartmented threshold secret sharing (CTSS) scheme is defined as*

$$\mathcal{CA} = \{A \subseteq \{P_1, \ldots, P_n\} | \ |A| \geq t$$

$$and \ \ \forall \ j = 1, \ldots, m, |A \cap C_j| \geq t_j\},$$

where $A = \{P_{i_1}, \ldots, P_{i_t}\}$ *and* $P_{i_k} \neq P_{i_l}$ *if* $k \neq l$ *for any subset* $\{i_1, \ldots, i_t\}$ *of* $\{1, \ldots, n\}$.

A special case of CTSS is called *conjunctive threshold secret sharing scheme* if the total threshold is $t = \sum_{j=1}^{m} t_j$.

3. Two Modifications of Shamir's Scheme

In this section, we describe two modifications of Shamir's scheme. We will use these two modifications to construct two ideal hierarchical threshold secret sharing schemes in the next section.

Modification 1 (ideal secret sharing scheme with both x_i and y_i as private share). In Shamir's (t, n) scheme, dealer first selects a secret s, and chooses a random $(t-1)$-th degree polynomial $f(x)$ over a finite $\mathbb{F}_p$ where $s < p$, p is a large prime and $s \in \mathbb{F}_p$. The private share of each shareholder is just the y-coordinate of the polynomial and the corresponding x-coordinate is made publicly known. In this modified scheme, we need to keep both x-coordinate and y-coordinate as private share. Obviously, Shamir's secret sharing scheme is no longer ideal if both x-coordinate and y-coordinate are private shares. Since the size of the secret $s \in \mathbb{F}_p$ is p and the size of share $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ is $2p$, the information rate of this approach is $p/2p = 1/2$.

However, to construct an ideal secret sharing scheme with both x_i and y_i as private share, we need to make some modifications. Let the master secret s be k bits and it can be divided into two sub-secrets as s_1 and s_2, where $s = s_1||s_2$, $|s_1| = |s_2| = k/2$ bits and "||" denotes concatenation of s_1 and s_2. Dealer selects a k bits secret s and a modulus p with $|p| = k/2$ bits and $s_1, s_2 < p$, and then chooses a random polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ over $\mathbb{F}_p$ such that the coefficients $a_0 = s_1$ and $a_1 = s_2$, where $a_i \in \mathbb{F}_p$ for $i = 0, 1, \ldots, t-1$. At the same time, the share (x_i, y_i) of each shareholder P_i is computed in the same way as Shamir's scheme, where x_i is a random value from $\mathbb{F}_p$ for $i = 1, \ldots, n$. Note that the size of secret s is k bits and the size of each share is $|x_i| + |y_i| = k/2 + k/2 = k$ bits. Thus, the information

rate of our modified scheme is $k/k = 1$, that is, this modified scheme is ideal. Furthermore, for any t shareholders who work together, they can reconstruct the secret s; but they cannot obtain the x-coordinates of other shareholders. This modified scheme is also information-theoretically secure.

There has a main difference between Shamir's (t, n) scheme and this modified scheme. In Shamir's (t, n) scheme, any t shareholders can reconstruct the polynomial and they also can compute private share of other shareholder since the x-coordinate of other shareholder is publicly known. In our modified scheme, any t shareholders can reconstruct the polynomial; but they cannot compute private share of any other shareholder since they have no information about the x-coordinate of other shareholder. This property will be utilized to construct a compartmented threshold secret sharing scheme (see Sec. 4.2).

Modification 2 (secret sharing scheme with both private and public shares). In Shamir's (t, n) secret sharing scheme, dealer uses a $(t-1)$-th degree polynomial to generate all private shares. Secret reconstruction is based on Lagrange interpolating polynomial of any t private shares. In this modified scheme, for a (t, n) scheme, dealer uses a polynomial with degree $(l-1)$, where l is *larger* than the threshold value t , to generate all shares, including n *private* shares and $(l-t)$ *public* shares. Dealer makes all public shares publicly known. Secret reconstruction is based on Lagrange interpolating polynomial with any t private shares along with $(l-t)$ public shares. For example, for a $(2, 4)$ scheme, dealer may select a 2-nd degree polynomial $f(x)$ to generate 4 private shares and 1 public share accordingly. Dealer publishes the public share. Later, with any 2 private shares and 1 public share can

reconstruct the secret.

We claim that all security properties in Shamir's scheme are maintained in this modified scheme. For example, it satisfies basic security requirements mentioned in Sec. 2, that is, the secret can be reconstructed by any t private shares along with some public shares and the secret cannot be reconstructed by any fewer than t private shares along with public shares. It is information-theoretically secure. This modified scheme is also ideal since the maximal length of shares is the same as the length of secret.

This modified scheme can be used in some applications, e.g. to construct a multilevel threshold secret sharing scheme (see Sec. 4.1). In Shamir's (t, n) scheme, dealer selects a secret and a random polynomial $f(x)$ over a finite $\mathbb{F}_p$ with degree $(t-1)$ such that the polynomial passes through one given point $(0, s)$. In some applications, dealer may need to select a polynomial such that this polynomial needs to pass through a set of given points. In this case, the degree of polynomial may be larger than the threshold value t.

4. Proposed Ideal Perfect Hierarchical Threshold Secret Sharing Schemes

In this section, we propose two schemes: an ideal perfect MTSS scheme and an ideal perfect CTSS scheme, based on our modified schemes described in Sec. 3, and give security analysis for the proposed schemes.

4.1. Ideal Perfect MTSS scheme

Let $\mathcal{L} = \{L_1, \ldots, L_m\}$ denote a partition of shareholders $\{P_1, \ldots, P_n\}$ into multiple security levels, and let n_i denote the number of shareholders at levels lower than or equal to L_i . Thus, we have $n_m = n$. Let $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$

denote a sequence of threshold values where $1 \leq t_j \leq j_i$ for $1 \leq j \leq m$ and $t_1 < t_2 < \cdots < t_m$.

We describe our $(\mathcal{L}, \mathcal{T})$ MTSS scheme based on **Modifications 1** and **2** described in Sec. 3 as follows.

Algorithm 1. Our $(\mathcal{L}, \mathcal{T})$ MTSS scheme.

---

1. According to **Modification 1** in Sec. 3, dealer selects the master secret s to be k bits and divides s into two sub-secrets as s_1 and s_2, where $s = s_1||s_2$, $|s_1| = |s_2| = k/2$ bits and "||" denotes concatenation of s_1 and s_2. Dealer selects a modulus p with $|p| = k/2$ bits and $s_1, s_2 < p$.
2. Dealer picks a random polynomial $g_1(x) = a_{10} + a_{11}x + \cdots + a_{1(t_1-1)}x^{t_1-1}$ with degree $(t_1 - 1)$, and computes n_1 private shares (x_{1i}, y_{1i}) for shareholders at level L_1 where $s_1 = a_{10} = g_1(0)$, $s_2 = a_{11}$ and $i = 1, \ldots, n_1$. This is a simple modified (t_1, n_1) threshold scheme.
3. According to **Modification 2** in Sec. 3, dealer computes a polynomial $g_2(x) = a_{20} + a_{21}x + \cdots + a_{2(n_1+2)}x^{n_1+2}$ to pass through all private share points at level(s) lower than L_2. More specifically, $g_2(x)$ is with degree (n_1+2) that satisfies $s_1 = g_2(0) = a_{20}$ and $s_2 = a_{21}$, and passes through n_1 private share points of step 2 and one random point from domain B. We need to consider two different cases as follows.
    - If $n_1 + 2 \geq t_2 - 1$, dealer computes private shares using $g_2(x)$ for all shareholders at level L_2. Dealer computes additional $(n_1 - t_2 + 3)$ public shares. This is a simple modified (t_2, n_2) threshold scheme using polynomial $g_2(x)$. Dealer distributes each private share

(x_{2i}, y_{2i}) for $i = 1, \ldots, n_2$ to corresponding shareholder privately. Also, dealer makes all public shares publicly known.

- If $n_1 + 2 < t_2 - 1$, dealer needs to modify $g_2(x)$ to pass through additional $(t_2 - n_1 - 3)$ points and obtains another polynomial $g_2'(x)$ with $(t_2 - 1)$-th degree. Dealer computes private shares using polynomial $g_2'(x)$ for all shareholders at level L_2. This is a simple modified (t_2, n_2) threshold scheme using polynomial $g_2'(x)$. Dealer distributes each private share (x_{2i}, y_{2i}) for $i = 1, \ldots, n_2$ to corresponding shareholder privately.

4. For each level L_j, $j = 3, \ldots, m$, dealer can repeat the same process as described in step 3 to construct a simple (t_j, n_j) threshold scheme for generating shares at level L_j. Dealer distributes each private share to corresponding shareholder privately. Also, dealer makes all public shares publicly known.
5. For any authorized subset $A = \{P_{i_1}, \ldots, P_{i_t}\}$ in $\mathcal{MA}$, there exists an integer $i \in \{1, \ldots, m\}$ such that $|A \cap (\cup_{j=1}^{i} L_j)| \geq t_i$. Thus, all shareholders in A can reconstruct the secret based on either t_i private shares of shareholders and $(n_{i-1} - t_i + 3)$ public shares if $n_{i-1} + 2 \geq t_i - 1$, or t_i private shares of shareholders if $n_{i-1} + 2 < t_i - 1$.

Remark 1. *In step 3, dealer computes a polynomial $g_2(x)$ to pass through n_1 private share points of step 2. This condition is to ensure that private shares at level L_1 can be used at level L_2. This design ensures ideal property. In addition, polynomial $g_2(x)$ needs to pass through one random point from*

domain B. This condition is to ensure that the polynomials $g_1(x)$ and $g_2(x)$ are different because n_1 private share points of step 2 are generated from polynomial $g_1(x)$.

Theorem 1. *Our $(\mathcal{L}, \mathcal{T})$ MTSS scheme constructed using Algorithm 1 is ideal, perfect and secure.*

Proof. Our proposed scheme constructed using **Modifications 1** and **2** is ideal since in Algorithm 1 dealer computes polynomial $g_i(x)$ at level L_i to pass through all private share points at level(s) lower than L_i. This condition is to ensure that private shares at lower levels can be used at higher levels. The information rate is 1. Thus, it is ideal. For any authorized subset A which is in $\mathcal{MA}$, the secret can be reconstructed by all shareholders in A based on Algorithm 1. For any un-authorized subset A' which is not in $\mathcal{MA}$, it must satisfy $|A' \cap (\cup_{j=1}^{i} L_j)| < t_i$ for all $i \in \{1, \ldots, m\}$. Since the number of private shares at each level is smaller than the threshold value, the secret cannot be reconstructed. Furthermore, our proposed scheme is perfect since this scheme is based on our first modification in previous section. The security of our proposed scheme is the same as Shamir's scheme. □

4.2. Ideal Perfect CTSS scheme

Let $\mathcal{C} = \{C_1, \ldots, C_m\}$ denote a partition of shareholders $\{P_1, \ldots, P_n\}$ into multiple security compartments, n_i denote the number of shareholders at compartment C_i, and $n_i = |C_i|$. Let $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$ denote a sequence of compartmented threshold values, where $1 \leq t_j \leq n_j$ for $1 \leq j \leq m$, and t denote the total threshold value with $\sum_{j=1}^{m} t_j \leq t \leq n$, and $n = \sum_{j=1}^{m} n_j$.

We first consider a special case when $t = \sum_{j=1}^{m} t_j$. This special case of CTSS scheme is called *conjunctive threshold secret sharing scheme*. The solution for this special $(\mathcal{C}, \mathcal{T})$ CTSS scheme is trivial. Dealer first picks $(m-1)$ random numbers, $s^1, \ldots, s^{m-1}$, from domain S of secrets and computes $s^m = s - \sum_{j=1}^{m-1} s^j$. Then, dealer constructs Shamir's (t_j, n_j) threshold schemes for each compartment C_j such that $s^j = f_j(0)$ where $f_j(x)$ is a random polynomial over $\mathbb{F}_p$ selected by dealer for C_j, $j = 1, \ldots, m$. Thus, for any authorized subset $A = \{P_{i_1}, \ldots, P_{i_t}\}$ in $\mathcal{CA}$, where $|A| = t = \sum_{j=1}^{m} t_j$, each partial secret s^i can be reconstructed by shareholders in $A \cap C_j$ for $j = 1, \ldots, m$. It is obvious that this scheme is ideal.

We now consider the general case when $t > \sum_{j=1}^{m} t_j$. We propose our $(\mathcal{C}, \mathcal{T})$ CTSS scheme based on two modifications described in Sec. 3.

Algorithm 2. Our $(\mathcal{C}, \mathcal{T})$ CTSS scheme.

---

1. Dealer picks m random numbers $s^1, \ldots, s^m$ from domain S of secrets and computes $s^{m+1} = s - \sum_{j=1}^{m} s^j$. Here, $s, s^1, \ldots, s^{m+1}$ are k bits and the prime modulus p is $k/2$ bits.
2. Dealer constructs a modified Shamir's (t_j, n_j) threshold scheme according to **Modification 1** in Sec. 3 for each compartment C_j such that $s_1^j = a_{j0} = f_j(0)$ and $s_2^j = a_{j1}$, where $f_j(x) = a_{j0} + a_{j1}x + \cdots + a_{t_j-1}x^{t_j-1}$ is a random polynomial over $\mathbb{F}_p$ selected by dealer for C_j and s_1^j, s_2^j are the sub-secrets of the master secret s^j, for $j = 1, \ldots, m$. Dealer distributes each private share (x_{jl}, y_{jl}) where $l = 1, \ldots, n_j$ to corresponding shareholder privately.

3. Dealer constructs a modified Shamir's (t_{m+1}, n_{m+1}) threshold scheme according to **Modifications 1** and **2** in Sec. 3. Dealer generates a random polynomial $f_{m+1}(x)$ over $\mathbb{F}_p$ such that this polynomial passes through all private share points (x_{jl}, y_{jl}), for $l = 1, \ldots, n_j$ and $j = 1, \ldots, m$, where $s_1^{m+1} = a_{(m+1)0} = f_{m+1}(0)$ and $s_2^{m+1} = a_{(m+1)1}$ are the sub-secrets of the master secret s^{m+1}. The degree of $f_{m+1}(x)$ is $d = n$. Since $d > t - 1$, dealer needs to compute $(d - t + 1)$ public shares and makes them publicly known.
4. For any authorized subset $A = \{P_{i_1}, \ldots, P_{i_t}\}$ in $\mathcal{CA}$, it must satisfy $|A \cap C_j| \geq t_j$ for all $j \in \{1, \ldots, m\}$ and $t > \sum_{j=1}^{m} t_j$. Thus, shareholders in A can reconstruct all partial secrets $s^1, \ldots, s^m$ and reconstruct the partial secret s^{m+1} using t private shares and $(d - t + 1)$ public shares. The secret s can be reconstructed as $s = s^1 + \cdots + s^m + s^{m+1}$.

Remark 2. *In Algorithm 2, we use the two modifications of Shamir's threshold scheme. This ensures that any t_j private shares used to reconstruct partial secrets s^j of compartments C_j, for $j = 1, \ldots, m$, and any t private shares along with $(d - t + 1)$ public shares can also be used to reconstruct s^{m+1}. In addition, this design ensures ideal and perfect property of our proposed scheme.*

Theorem 2. *Our $(\mathcal{L}, \mathcal{T})$ CTSS scheme constructed using algorithm 2 is ideal, perfect and secure.*

Proof. Our proposed scheme is ideal since the information rate is 1 as mentioned in **Modifications 1** and **2**. For any authorized subset A which is

in $\mathcal{CA}$, the secret can be reconstructed by all shareholders in A based on Algorithm 2. For any un-authorized subset A' which is not in $\mathcal{CA}$, it must satisfy $|A' \cap C_j| < t_j$ for some $j \in \{1, \ldots, m\}$ or $|A'| < t$. We analyze un-authorized subset A' into three different cases: a) $|A' \cap C_j| < t_j$ for some $j \in \{1, \ldots, m\}$ and $|A'| < t$. This is a trivial case since all shareholders in A' cannot reconstruct the complete list of $s^1, \ldots, s^{m+1}$. Thus, they cannot reconstruct the secret s. b) $|A' \cap C_j| \geq t_j$ for all $j \in \{1, \ldots, m\}$ and $|A'| < t$. It is obvious that all shareholders in A' can reconstruct the partial secrets, $s^1, \ldots, s^m$. However, they cannot reconstruct the partial secret s^{m+1}. As mentioned in **Modification 2**, all shareholders in compartment C_j only can get $|A' \cap C_j|$ shares of their own; but cannot obtain any additional share of other shareholder in the same compartment since they have no information on the x-coordinate of any other shareholder. Thus, the partial secret s^{m+1} is protected from A', that is, the secret s is protected from A'. c) $|A' \cap C_j| < t_j$ for some $j \in \{1, \ldots, m\}$ and $|A'| \geq t$. Assume that there is a set $J = \{j_1, \cdots, j_v\} \subseteq \{1, \ldots, m\}$ such that $|A' \cap C_j| < t_j$ for each $j \in J$. It is obvious that all shareholder in A' who work together along with $(d - t + 1)$ public shares can reconstruct the partial secrets s^{m+1} and s^j for $j \in \{1, \ldots, m\} - J$. However, they still cannot obtain any additional share of other shareholder for each compartment C_j for $j \in J$. The reason is that they have no information on the x-coordinate of any other shareholder. Thus, for any compartment C_j for $j \in J$, the partial secret s^j cannot be reconstructed. Therefore, the secret s is protected from A'. Thus, we have showed that our proposed scheme is information-theoretically secure. Furthermore, our proposed scheme is perfect since this scheme is based on our two modifications

in previous section. □

5. Conclusions

In this paper, we propose two modifications of Shamir's (t, n) secret sharing scheme. These two modified schemes are ideal and perfect. Two ideal hierarchical threshold secret sharing schemes: multilevel threshold secret sharing and compartmented threshold secret sharing, are constructed based on these two modifications. We have proved that our proposed schemes are secure.

References

[1] E. Ballico, G. Boato, C. Fontanari, F. Granelli, Hierarchical secret sharing in ad hoc networks through birkhoff interpolation, in: Proc. the IEEE International Conference on Telecommunications and Networking, Springer-Verlag, 2006, pp. 157–164.

[2] G. R. Blakley, Safeguarding cryptographickeys, in: Proc. AFIPS'79 Nat. Computer Conf., AFIPS Press, vol. 48, Montvale, New York, 1979, pp. 313–317.

[3] E. F. Brickell, Some ideal secret sharing schemes, J. Combinatorial Mathematics and Combinatorial Computing, 6 (1989) 105–113.

[4] E. F. Brickell, D. M. Davenport, On the classification of ideal secret sharing schemes, J. Cryptology, 4(2) (1991) 123–134.

[5] O. Farrás, J. Martí-Farré, C. Padró, Ideal multipartite secret sharing schemes, in: Proc. EUROCRYPT 2007, LNCS, vol. 4515, Springer-Verlag, 2007, pp. 448–465.

[6] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, Secret sharing in multilevel and compartmented groups, in: Proc. ACISP 1998, LNCS, vol. 1438, Springer-Verlag, 1998, pp. 367–378.

[7] E. D. Karnin, J. W. Greene, M. E. Hellman, On Secret Sharing Systems, IEEE Trans. on Information Theory., 29(1) (1983) 35–40.

[8] C. Ma, R. Cheng, Key management based on hierarchical secret sharing in Ad-hoc networks, in: Prof. Inscrypt 2007, LNCS, vol. 4990, Springer-Verlag, 2007, pp. 182–191.

[9] A. J. Menezes, P. C. Oorschot, S. A. Vanstone, Handbook of applied cryptography. CRC Press, Oct. 1996.

[10] G. J. Simmons, How to (really) share a secret, in Proc. CRYPTO 1988, LNCS, vol. 403, 1988, pp. 390–448.

[11] A. Shamir How to share a secret, Commun. ACM, 22(11) (1979) 612–613.

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

[13] T. Tassa, N. Dyn, Multipartite secret sharing by bivariate interpolation, J. Cryptology, 22(2) (2008) 227-258.

[14] Y. Zhang, Z. Liu, G. Huang, Sure interpolation and its application to hierarchical threshold secret sharing scheme, in: International Symposium on Computer Science and Computational Technology(ISCSCT'08), 2008, pp. 447–450.