Ideal Social Secret Sharing Using Birkhoff Interpolation Method

Nasrollah Pakniat [a], Ziba Eslami [a,b,*], Mehrdad Nojoumian [c]

[a] *Department of Computer Sciences, Shahid Beheshti University, G.C., Tehran, Iran*

[b] *Cyberspace Research Center, Shahid Beheshti University, G.C., Tehran, Iran*

[c] *Department of Computer Science, Southern Illinois University, Carbondale, Illinois, USA*

Abstract

The concept of *social secret sharing* (SSS) was introduced in 2010 by Nojoumian et al. [1,2]. In this scheme, the number of shares allocated to each party depends on the players reputation and the way he interacts with other parties. In other words, weights of the players are periodically adjusted such that cooperative participants receive more shares compared to non-cooperative parties. As our contribution, we propose an *ideal social secret sharing* (Ideal-SSS) in which the size of each player's share is equal to the size of the secret. This property will be achieved using hierarchical threshold secret sharing rather than weighted secret sharing. We show that the proposed scheme is secure in a passive adversary model. Compared to SSS, our proposed scheme is more efficient in terms of the share size, communication complexity and computational complexity of the "sharing" protocol. However, the "social tuning" and "reconstruction" protocols of SSS are computationally more efficient than those of the proposed scheme. Depending on the number of execution of social tuning protocol, this might be a reasonable compromise because the reconstruction protocol is executed only once throughout the secret's lifetime.

Key words: Secret Sharing, Social Secret Sharing, Hierarchical Threshold Access Structure, Trust Modeling, Birkhoff Interpolation.

* Corresponding author. Tel:+98 2129903007; fax: +98 2122431655
Email addresses: n_pakniat@sbu.ac.ir (Nasrollah Pakniat), z_eslami@sbu.ac.ir (Ziba Eslami), nojoumian@cs.siu.edu (Mehrdad Nojoumian).

1 Introduction

In secret sharing schemes, a secret is divided into different pieces, named "secret shadows". These shadows are then shared among a group of participants such that any authorized subset of players can reconstruct the secret but any unauthorized subset of players gain no information about the secret. A subset is called authorized if it belongs to a predetermined access structure. The first secret sharing scheme, a.k.a *threshold secret sharing* (TSS), was proposed independently by Shamir and Blakley [3,4]. In (t, n)-threshold secret sharing, the authorized subsets of participants are those with at least t members, where t is the threshold of the scheme.

We now briefly explain some secret sharing schemes that are used in our technical discussions. In *verifiable secret sharing* (VSS) [5], participants are able to verify the consistency of their shares in both sharing and recovery phases. There exist many verifiable secret sharing schemes in the literature with different properties and security models [6–9]. In *proactive secret sharing* (PSS) [10], the scheme is equipped with an extra ability to renew participants' shares without changing the secret in order to deal with "mobile adversary", i.e., the adversary who is active while the protocols are executing. To change other parameters of a threshold secret sharing scheme (such as the threshold t and the number of players n), *dynamic secret sharing* (DSS) [11] can be used. In a *weighted secret sharing* (WSS) scheme [12], participants are assigned different number of shares based on their levels of authority, i.e., players with a higher level of authority receive more shares compared to the other parties. Finally, in *social secret sharing* (SSS) [1,2], the number of shares allocated to each party depends on the players reputation and the way he interacts with other parties. In other words, weights of the players are periodically adjusted such that cooperative participants receive more shares compared to non-cooperative parties. It is worth mentioning that SSS is constructed using VSS, PSS, DSS and WSS schemes. We can refer to [13–15] as applications of SSS in the context of cloud computing, rational cryptography and multiparty computation.

The initial social secret sharing construction is shown to be secure in both passive and active adversary models. For the later case, the authors use the verifiable proactive secret sharing scheme of [6] in their protocols. In SSS, reputation of each participant is re-evaluated periodically based on his availability and subsequently, the player's authority (i.e., player's weight or number of shares) will be adjusted. To make participants' old shares (from previous time period) invalid in the next time interval, each player's shares are proactively renewed at the beginning of each period while the secret remains unchanged. Finally, to provide various number of shares for different players, Nojoumian et al. use Shamir's weighted threshold secret sharing scheme [3]. As a result,

the size of the share that each player receives is proportional to his assigned weight (which is determined based on his reputation/availability).

To the best of our knowledge, two types of hierarchical threshold secret sharing exist in the literature, i.e., *disjunctive hierarchical threshold secret sharing* [16–19] and *conjunctive hierarchical threshold secret sharing* [18,20–22]. In a hierarchical threshold secret sharing scheme, the secret is shared among a set of participants $\mathcal{U} = \{P_1, P_2, \cdots, P_n\}$ who are divided into m hierarchical non-overlapping subsets according to their authorities, i.e., $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$ and $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ where $i \neq j$. In other words, players in $\mathcal{U}_i$ have more authority to recover the secret than those in $\mathcal{U}_j$ for $1 \leq j < i \leq m$. The access structure of a hierarchical threshold secret sharing scheme is determined by a strictly decreasing sequence of threshold parameters $t_1 > t_2 > \cdots > t_m$.

In conjunctive hierarchical threshold secret sharing, a subset A of players is able to recover the secret if it satisfies a sequence of threshold requirements, i.e., $\left|A \cap \left(\bigcup_{i=0}^{j} \mathcal{U}_{m-i}\right)\right| \geq t_{m-j}$ for $j = 0, \cdots, m-1$. The scheme is called disjunctive if the satisfaction of one of the threshold requirements is sufficient to reconstruct the secret. In other words, in disjunctive hierarchical threshold secret sharing, a subset of participants A is authorized if there exists some $0 \leq j \leq m-1$ such that $\left|A \cap \left(\bigcup_{i=0}^{j} \mathcal{U}_{m-i}\right)\right| \geq t_{m-j}$. It is clear that, in the later scheme, players in the higher level have more power for the secret recovery.

In this article, we employ disjunctive hierarchical threshold secret sharing instead of weighted secret sharing that results in an *ideal social secret sharing* scheme. Our proposed construction is based on Tassa's scheme (second scheme in [18]). The number of communication rounds in our construction is less than that of Nojoumian et al.'s scheme. Therefore, our scheme outperforms Nojoumian et al.'s scheme in terms of the share size as well as communication complexity. Furthermore, we will show that the "sharing" protocol of the proposed scheme is computationally more efficient than that of Nojoumian et al.'s scheme, whereas, "social tuning" and "reconstruction" protocols of SSS are computationally more efficient than ours. Depending on the number of execution of social tuning protocol, this might be a reasonable compromise because the reconstruction protocol is executed only once throughout the secret's lifetime.

The rest of this article is organized as follows. Section 2 explains preliminary concepts including Birkhoff interpolation, social secret sharing and Tassa's disjunctive hierarchical threshold secret sharing scheme. In Section 3, we illustrate our proposed ideal social secret sharing scheme. Section 4 provides security and efficiency analysis of ideal SSS and SSS. Finally, concluding remarks are presented in Section 5.

2 Preliminaries

In this section, we first review the Birkhoff interpolation problem and then we illustrate the SSS and disjunctive hierarchical TSS schemes.

2.1 Birkhoff Interpolation

Definition 1. Let X, E and C be defined as follows:

- $X = \{x_1, \cdots, x_k\}$ is a given set of points in R, where $x_1 < x_2 < \cdots < x_k$.
- $E = (e_{i,j})_{1 \le i \le k, 0 \le j \le l}$ is a matrix with binary entries, $I(E) = \{(i,j) : e_{i,j} = 1\}$ and $N = |I(E)|$; we assume the right-most column in E is nonzero.
- $C = \{c_{i,j} : (i,j) \in I(E)\}$ is a set of N real values.

Then, the ***Birkhoff interpolation problem*** that corresponds to the triplet $< X, E, C >$ is the problem of finding a polynomial $P(x) \in R_{N-1}[x]$ that satisfies the N equalities

$$P^{(j)}(x_i) = c_{i,j}, \ (i,j) \in I(E), \tag{1}$$

where $P^{(j)}(\cdot)$ is the j-th derivative of $P(x)$ and $R_{N-1}[x]$ is the set of all possible polynomials with degree at most $N-1$. The matrix E is called the *interpolation matrix* [18].

Unlike Lagrange and Hermite interpolation methods that are unconditionally well posed, the Birkhoff interpolation problem may not result in a unique solution. The following lemma provides a necessary condition for interpolation matrix E; the corresponding Birkhoff interpolation problem would be well posed for all X.

Lemma (Pólya's Condition [23]). Let the Birkhoff interpolation problem that corresponds to the triplet $< X, E, C >$ be well posed. Then, the entries of E satisfy the following relation:

$$\forall t, (0 \le t \le l) : \sum_{j=0}^{t} \sum_{i=1}^{k} e_{i,j} \ge (t+1), \tag{2}$$

where l is the highest derivative order in the data and k is the number of interpolating points.

In order to obtain a sufficient condition, we provide the following definition.

Definition 2. A 1-***sequence*** in the interpolation matrix E is a maximal run of consecutive 1-s in a row of the matrix E; namely, it is a triplet of the

form (i, j_0, j_1) where $1 \leq i \leq k$, $0 \leq j_0 \leq j_1 \leq l$, such that $e_{i,j} = 1$ for all $j_0 \leq j \leq j_1$ while $e_{i,j_0-1} = e_{i,j_1+1} = 0$ (letting $e_{i,-1} = e_{i,l+1} = 0$). A 1-sequence (i, j_0, j_1) is called *supported* if E has 1-s both to the northwest and southwest of the leading entry in the sequence; i.e., there exist indexes nw and sw, where $i_{nw} < i < i_{sw}$ and $j_{nw}, j_{sw} < j_0$ such that $e_{i_{nw},j_{nw}} = e_{i_{sw},j_{sw}} = 1$ [18].

The following theorem provides a sufficient condition for Birkhoff interpolation to be well posed [24].

Theorem 1. The interpolation problem (Definition 1) has a unique solution if the interpolation matrix E satisfies Pólya's condition and contains no supported 1-sequences of odd length.

In this paper, we use Birkhoff interpolation over finite fields. The following theorem provides sufficient (not necessarily optimal) conditions for Birkhoff interpolation problem to be well posed over finite fields [18].

Theorem 2. The Birkhoff interpolation problem (Definition 1) has a unique solution over the finite field $GF(q)$ if, besides the conditions of Theorem 1, the following condition is satisfied:

$$q > 2^{-l+2} \cdot (l-1)^{(l-1)/2} \cdot (l-1)! \cdot x_k^{(l-1)(l-2)/2}, \tag{3}$$

where l is the highest derivative order in the data.

Next, we provide further clarification and also an example regarding the Birkhoff interpolation method.

Let $\varphi = \{g_0, g_1, \ldots, g_N\}$ be a system of linearly independent, N times continuously differentiable real-valued, functions and $I'(E) = \{\alpha_i : i = 1, \cdots, N+1\}$ be a vector that is obtained by lexicographically ordering of entries of $I(E)$ (in $I'(E)$ the pair (i, k) precedes (i', k') if and only if $i < i'$ or $i = i'$ and $k < k'$). Furthermore, let $\alpha_i(1)$ and $\alpha_i(2)$ denote the first and second elements of the pair $\alpha_i \in I'(E)$. Finally, let $C' = \{c_i^{'} : i = 1, \cdots, N+1\}$ be another vector that is obtained by lexicographically ordering of entries of C (the ordering procedure is done based on indexes of elements in C).

Now, by using the elements E, X and φ, we are able to solve the Birkhoff interpolation problem as follows:

$$P(x) = \sum_{j=0}^{N} \frac{|A(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x), \tag{4}$$

where

$$A(E,X,\varphi)=\begin{bmatrix} g_0^{(\alpha_1(2))}(x_{\alpha_1(1)}) & g_1^{(\alpha_1(2))}(x_{\alpha_1(1)}) & \cdots & g_N^{(\alpha_1(2))}(x_{\alpha_1(1)}) \\ g_0^{(\alpha_2(2))}(x_{\alpha_2(1)}) & g_1^{(\alpha_2(2))}(x_{\alpha_2(1)}) & \cdots & g_N^{(\alpha_2(2))}(x_{\alpha_2(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(\alpha_{N+1}(2))}(x_{\alpha_{N+1}(1)}) & g_1^{(\alpha_{N+1}(2))}(x_{\alpha_{N+1}(1)}) & \cdots & g_N^{(\alpha_{N+1}(2))}(x_{\alpha_{N+1}(1)}) \end{bmatrix} \tag{5}$$

$|\cdot|$ is the determinant operation and $A(E,X,\varphi_j)$ can be computed by replacing $(j+1)$-th column of matrix (5) with C'.

By reformulating (4) (i.e., by expanding $|A(E,X,\varphi_j)|$ down to its $(j+1)$-th column), we have the following equation for the Birkhoff interpolating procedure Eq.(1):

$$P(x)=\sum_{j=0}^{N}\sum_{i=0}^{N}(-1)^{(i+j)}\,c'_{i+1}\frac{|A_i(E,X,\varphi_j)|}{|A(E,X,\varphi)|}g_j(x), \tag{6}$$

where $A_i(E,X,\varphi_j)$ can be computed from $A(E,X,\varphi_j)$ by removing $(i+1)$-th row and $(j+1)$-th column.

Example 1. (Birkhoff Interpolation) Let assume $X=\{1,2,3,4\}$, $C=C'=\{c_1=10,c_2=28,c_3=24,c_4=6\}$ and matrix E be as follows:

$$E=\begin{pmatrix}1&0&0&0\\1&0&0&1\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

As a result, we have $N=3$ and $I(E)=I'(E)=\{\alpha_1=(1,1),\alpha_2=(2,1),\alpha_3=(3,3),\alpha_4=(4,4)\}$. It is easy to check that the Birkhoff interpolation problem that corresponds to these parameters is well posed. Let $\varphi=\{1,x,x^2,x^3\}$. By using the provided parameters, we have

$$|A(E,X,\varphi)|=\begin{vmatrix}1&1&1&1\\1&2&4&8\\0&0&2&18\\0&0&0&6\end{vmatrix}=12,\ |A(E,X,\varphi_0)|=\begin{vmatrix}10&1&1&1\\28&2&4&8\\24&0&2&18\\6&0&0&6\end{vmatrix}=48,$$

$$|A(E,X,\varphi_1)|=\begin{vmatrix}1&10&1&1\\1&28&4&8\\0&24&2&18\\0&6&0&6\end{vmatrix}=24,\ |A(E,X,\varphi_2)|=\begin{vmatrix}1&1&10&1\\1&2&28&8\\0&0&24&18\\0&0&6&6\end{vmatrix}=36,$$

$$|A(E,X,\varphi_3)|=\begin{vmatrix}1&1&1&10\\1&2&4&28\\0&0&2&24\\0&0&0&6\end{vmatrix}=12.$$

Using Eq.(4), the result of Birkhoff interpolation would be:

$$\begin{aligned}P(x)=\sum_{j=0}^{3}\frac{|A(E,X,\varphi_j)|}{|A(E,X,\varphi)|}g_j(x)&=\frac{48(1)+24(x)+36(x^2)+12(x^3)}{12}\\&=4+2x+3x^2+x^3.\end{aligned}$$

2.2 Social Secret Sharing

A social secret sharing scheme is defined by three protocols; "sharing" (*Sha*), "social tuning" (*Tun*) and "reconstruction" (*Rec*) protocols. In *Sha*, the dealer shares a secret among a group of participants with different authorities and then he leaves the scheme. *Tun* is periodically performed after the sharing phase. Its aim is to adjust the participants' authorities based on their behavior (cooperation/availability) over time using a trust function [25]. Newcomers are always able to join the scheme and receive shares of the secret. There would be no necessity for the presence of the dealer and authorized subsets of participants can execute *Tun* protocol without revealing the secret. When all participants, in an authorized subset, decide to reconstruct the secret, they can use *Rec* protocol to recover the secret. For further clarification and detail, see [1,2].

2.3 Disjunctive Hierarchical Threshold Secret Sharing

We briefly review Tassa's disjunctive hierarchical threshold secret sharing scheme (the second scheme of [18]). Suppose that there is a group $\mathcal{U}$ of n players $P_1, P_2, \cdots, P_n$ partitioned into m levels $\mathcal{U}_1, \mathcal{U}_2, \cdots, \mathcal{U}_m$. Also, assume that the sequence of threshold requirements $t_1 > t_2 > \cdots > t_m$ determines the hierarchical threshold access structure. Let q be a prime power such that $q > max\{2^{-t_1+2} \cdot (t_1-1)^{(t_1-1)/2} \cdot (t_1-1)! \cdot n^{(t_1-1)(t_1-2)/2}, n\}$. Same as Shamir's secret sharing scheme, Tassa's scheme is a polynomial-based secret sharing, i.e., the share of each participant is obtained from a polynomial. The reconstruction of the secret is based on Birkhoff interpolation method. The Tassa's scheme is demonstrated in Figure 1.

3 Ideal Social Secret Sharing

Let $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$ denote m authority levels such that players in the higher levels have more power than those in the lower ones. Therefore, if a player is in i-th authority level, it is in $\mathcal{U}_i$. Moreover, assume that there is a threshold t_i for each level of authority $\mathcal{U}_i$ $(i = 1, \cdots, m)$. This threshold determines the required number of parties for secret recovery (from that level or higher ones). In other words, this sequence of thresholds determines the access structure of the scheme. Since we do not give the ability of secret recovery only to one participant, we require that $t_m > 1$. Furthermore, since we would like to give more authorities to the players in the higher levels, $t_i < t_j$ for $1 \leq j < i \leq m$.

The sharing protocol

To share the secret S, the dealer proceeds as follows:

(1) Generates polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t_1-2}x^{t_1-2} + Sx^{t_1-1}$ over $GF(q)$, where $\{a_i\}_{i=0}^{t_1-2}$ are random numbers.

(2) For each participant $P_i \in \mathcal{U}$, computes $sh_i = f^{(t_1-t_j)}(i)$ as his share from the secret S, where $f^{(t_1-t_j)}(\cdot)$ is the (t_1-t_j)-th derivative of $f(\cdot)$ and j is such that $P_i \in \mathcal{U}_j$.

The reconstruction protocol

Let $Autsub = \{P_{\alpha_0}, P_{\alpha_1}, \cdots, P_{\alpha_{t_j-1}}\}$ be an authorized subset of participants. Then, on input the set of shares corresponding to the members of $Autsub$, a trusted party proceeds as follows to recover the secret:

(1) Applies Birkhoff interpolation on the provided shares and reconstructs $(t_1 - t_j)$-th derivative of $f(\cdot)$, i.e., $f^{(t_1-t_j)}(\cdot)$.

(2) Let S' be the last coefficient of $f^{(t_1-t_j)}(\cdot)$. Then, retrieves the secret as $S = \frac{(t_j-1)!}{(t_1-1)!}S' \ (mod\ q)$.

Fig. 1. Tassa's Disjunctive Hierarchical Threshold Secret Sharing Scheme.

In a social secret sharing scheme, new parties are able to join the scheme and have secret shadows. Therefore, the size of $\mathcal{U}$ can be changed over time. Let n be the maximum cardinality of $\mathcal{U}$ (i.e., the maximum number of players) and let $q > n$ be a prime number such that:

$$q > 2^{t_m-t_1+2} \cdot (t_1 - t_m - 1)^{(t_1-t_m-1)/2} \cdot (t_1 - t_m - 1)! \cdot n^{(t_1-t_m-1)(t_1-t_m-2)/2}$$

This is a necessary assumption for the well-posedness of the interpolation problem. We also require a trust function to compute each participant's trust value at the beginning of each period. For example, we can use the proposed function in [25], which is also used in [1,2,13]. Assume that this trust function returns real values in the interval (ξ_1, ξ_2). We divide the interval (ξ_1, ξ_2) into m subintervals

$$I_1 = \left(\xi_1, \xi_1 + \frac{(\xi_2 - \xi_1)}{m}\right), I_2 = \left[\xi_1 + \frac{(\xi_2 - \xi_1)}{m}, \xi_1 + \frac{2(\xi_2 - \xi_1)}{m}\right), \cdots,$$
$$I_m = \left[\xi_2 - \frac{(\xi_2 - \xi_1)}{m}, \xi_2\right).$$

We associate the subinterval I_i to the authority level $\mathcal{U}_i$, for $i = 1, \cdots, m$. Similarly, our proposed scheme consists of sharing (Sha), social tuning (Tun) and reconstruction (Rec) protocols.

3.1 Sharing Protocol (Sha)

The sharing protocol of our proposed scheme is the same as Tassa's scheme, except that all participants belong to the same authority level. The details of this protocol are presented in Figure 2.

The sharing protocol

On input the secret S, the dealer proceeds as follows:

(1) With the assumption of equal authority for all the participants at the beginning of the sharing, gives all of them the same initial trust value $\xi_I = \xi_1 + (\xi_2 - \xi_1)/2$.

(2) Let I_c be the subinterval that the initial trust value ξ_I belongs to and let $\mathcal{U}_c$ be the corresponding authority level. Places all the participants in $\mathcal{U}_c$, i.e., it is assumed that $\mathcal{U} = \mathcal{U}_c$ at the beginning of the sharing.

(3) Generates a polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t_1-2} x^{t_1-2} + S x^{t_1-1}$ over $GF(q)$, where $\{a_i\}_{i=0}^{t_1-2}$ are random values.

(4) Computes the share corresponding to each participant $P_i \in \mathcal{U}$ as $sh_i = f^{(t_1-t_c)}(i)$, where $f^{(t_1-t_c)}(\cdot)$ is (t_1-t_c)-th derivative of $f(\cdot)$.

(5) Sends P_i's share to him via a secure channel.

Fig. 2. Sharing Protocol of the Ideal Social Secret Sharing Scheme.

Note that, in step-3 of the sharing protocol, a polynomial of degree $t_c - 1$ would be sufficient, however, choosing a polynomial of degree $(t_1 - 1)$ would simplify our notations in social tuning and reconstruction protocols. After executing protocol *Sha*, the dealer leaves the scheme and participants can execute *Tun* and *Rec* protocols on their own.

3.2 Social Tuning Protocol (Tun)

The social tuning protocol of the proposed scheme consists of two phases: 1) "adjusting" phase and 2) "share renewal" phase. In the adjusting phase, the trust value of each participant is reevaluated. The newcomers can also join the scheme through this phase. The details of this phase are presented in Figure 3. Note that step 4 of Figure 3 is necessary in order to ensure that authorized subsets of participants are able to run the social tuning as well as the secret recovery protocols whenever it is required.

In the following, we provide an example to show how the new identities would be given to the participants in step 4 of Figure 3:

The adjusting phase

The participants in an authorized subset:

(1) Reevaluate the trust value of each participant based on his previous trust value and his behavior in the past time period.
(2) Assign the initial trust value ξ_I to each newcomer.
(3) Rearrange the set of participants into subsets $\mathcal{U}_1, \mathcal{U}_2, \cdots, \mathcal{U}_m$ according to the new computed trust values. The rearrangement is done in such a way that if a participant's new trust value is in the subinterval I_k, then he would be moved to $\mathcal{U}_k$.
(4) To make sure that the interpolation matrices that correspond to authorized subsets of participants do not contain supported 1-sequences, reassign the identities of participants in the following way:
    (a) For $j = 1, \cdots, m$:
        (i) For each $P_i \in \mathcal{U}_j$ $(1 \leq i \leq |\mathcal{U}_j|)$: assign the least possible non-zero (non-occupied) number from $GF(q)$ as P_i's (new) identity (ID_{P_i}).

Fig. 3. Adjusting Phase of the Ideal Social Secret Sharing Scheme.

Example 2. (Identity Allocation) Suppose there exist three authority levels and ten players in our scheme. Let the division of the participants to the authority levels be as follows: (division is done based on step 3 of Figure 3) $\mathcal{U}_1 = \{P_1, P_5, P_6\}$, $\mathcal{U}_2 = \{P_3, P_4, P_8\}$, $\mathcal{U}_3 = \{P_2, P_7, P_9, P_{10}\}$. To ensure that the Birkhoff interpolation problem is well-posed, the identity of the players in the lower levels must be less than those in the higher ones. For instance, we can assign $ID_{P_1} = 1, ID_{P_5} = 2, ID_{P_6} = 3, ID_{P_3} = 4, ID_{P_4} = 5, ID_{P_8} = 6, ID_{P_2} = 7, ID_{P_7} = 8, ID_{P_9} = 9, ID_{P_{10}} = 10$ as players' identities, however, we cannot consider the following allocation, since it might causes the corresponding Birkhoff interpolation problem to be unsolvable: $ID_{P_1} = 10, ID_{P_5} = 1, ID_{P_6} = 8, ID_{P_3} = 7, ID_{P_4} = 6, ID_{P_8} = 5, ID_{P_2} = 4, ID_{P_7} = 3, ID_{P_9} = 2, ID_{P_{10}} = 9$.

After reevaluating participants' trust values, the share of each participant is reevaluated in the share renewal phase. Any authorized subset of participants can execute this protocol. The detail of this phase is presented in Figure 4.

Example 3. (Share Renewal) Let $f_i(\cdot)$ be the polynomial that is shared among players in i-th time period T_i. Let P_β be a party who belongs to $\mathcal{U}_k$ in T_i considering his trust value. Therefore, the share that P_β receives in T_i is $sh_\beta = f_i^{(t_1 - t_k)}(ID_{P_\beta})$, where ID_{P_β} is the identity that is assigned to P_β in T_i. Furthermore, suppose P_β's trust value is equal to $\zeta_{P_\beta} \in I_l$ at the beginning of T_{i+1} and also let his new identity be ID'_{P_β}. As a result, the share that P_β receives in T_{i+1} would be equal to $sh_\beta = f_{i+1}^{(t_1 - t_l)}(ID'_{P_\beta})$.

The share renewal phase

Let $Autsub = \{P_{\alpha_0}, \cdots, P_{\alpha_{t_k-1}}\}$ be an authorized subset of participants such that $ID_{P_{\alpha_i}} < ID_{P_{\alpha_{i+1}}}$ for $i = 0, \cdots, t_k - 2$. Then, in order to renew the share of each participant $P_\beta \in \mathcal{U}$:

(1) Each participant $P_{\alpha_i} \in Autsub$:
   (a) Constructs a polynomial $f_{1\alpha_i}(x) = a_{0\alpha_i} + a_{1\alpha_i}x + \cdots + a_{(t_1-3)\alpha_i}x^{t_1-3} + a_{(t_1-2)\alpha_i}x^{t_1-2}$ over $GF(q)$, where $\{a_{j\alpha_i}\}_{j=0}^{t_1-2}$ are random values. Note that the degree of $f_{1\alpha_i}(\cdot)$ is $t_1 - 2$.
   (b) Uses his share from the previous time period and constructs a polynomial $f_{2\alpha_i}(x) = \sum_{j=0}^{t_k-1}\left[(-1)^{(i+j)}sh_{\alpha_i}\left(\frac{|A_i(E,X,\varphi_j)|}{|A(E,X,\varphi)|}\right)\left(\frac{(j)!}{(j+t_1-t_k)!}\right)x^{j+t_1-t_k}\right]$, where E is the interpolation matrix corresponding to the participants in $Autsub$ and their former authorities, i.e., $e_{i,t_k-t_j+1} = 1 \Leftrightarrow P_{\alpha_i} \in \mathcal{U}_j$, the other entries of E are all 0, $X = \{ID_{P_{\alpha_0}}, ID_{P_{\alpha_1}}, \cdots, ID_{P_{\alpha_{t_k-1}}}\}$, ID_{P_i} is the former identity of P_i and $\varphi = \{1, x, x^2, \cdots, x^{t_k-1}\}$.
   (c) Computes $f_{\alpha_i}(x) = f_{1\alpha_i}(x) + f_{2\alpha_i}(x)$.
   (d) For each $P_\beta \in \mathcal{U}$:
      (i) Computes a subshare of P_β's new share from the secret S as $sh_{P_{\alpha_i}\to P_\beta} = f_{\alpha_i}^{(t_1-t_l)}(ID'_\beta)$, where l is such that $P_\beta \in \mathcal{U}_l$ according to P_β's new authority obtained from adjusting phase and ID'_β is P_β's new identity.
      (ii) Sends $sh_{P_{\alpha_i}\to P_\beta}$ to P_β via a secure channel.

(2) After receiving the subshares from all P_{α_i}, $(0 \le i \le t_k - 1)$, each participant $P_\beta \in \mathcal{U}$:
   (a) Erases his share from the previous time period.
   (b) Computes his final new share from the secret S as $sh_\beta = \sum_{i=0}^{t_k-1} sh_{P_{\alpha_i}\to P_\beta}$.

Fig. 4. Share Renewal Phase of the Ideal Social Secret Sharing Scheme.

3.3 Reconstruction Protocol (Rec)

If an authorized subset of players decide to recover the secret at any time, they can execute the *Rec* protocol in order to recover the secret. The details of this protocol are presented in Figure 5.

The reconstruction protocol

Let $Autsub = \{P_{\alpha_0}, P_{\alpha_1}, \cdots, P_{\alpha_{t_j-1}}\}$ be an authorized subset of participants. Then, on input the set of shares corresponding to the members of $Autsub$, a trusted party proceeds as follows to recover the secret:

(1) Applies Birkhoff interpolation on the provided shares and reconstructs $(t_1 - t_j)$-th derivative of $f(\cdot)$, i.e., $f^{(t_1-t_j)}(\cdot)$.
(2) Let S' be the last coefficient of $f^{(t_1-t_j)}$. Then, retrieves the secret as $S = \frac{(t_j-1)!}{(t_1-1)!}S' \ (mod\ q)$.

Fig. 5. Reconstruction Protocol of the Ideal Social Secret Sharing Scheme.

4 Security Analysis and Comparison

In this section, the security proof of ideal social secret sharing, in a passive adversary model, is presented. Afterwards, our proposed construction is compared with Nojoumian et al.'s scheme.

4.1 Security analysis

Theorem 3. The share renewal phase of our proposed Ideal SSS is correct and unconditionally secure under the passive adversary model.

Proof. Let T_h denote the h-th time period and let $f_h(x) = \sum_{i=0}^{t_1-1} a_{ih}x^i$ be the polynomial that is shared among the players in T_h. At the beginning of T_{h+1}, the set of shares belonging to any authorized subset of participants $Autsub = \{P_{\alpha_0}, \cdots, P_{\alpha_{t_k-1}}\}$ can be used to retrieve the following polynomial:

$$\begin{aligned} F(x) &= \sum_{i=t_1-t_k}^{t_1-1} b_i x^i \\ &= \sum_{j=0}^{t_k-1} \sum_{i=0}^{t_k-1} (-1)^{(i+j)}\, sh_{\alpha_i} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} \frac{(j)!}{(j + t_1 - t_k)!} (x^{j+t_1-t_k}). \end{aligned} \tag{7}$$

By using the Birkhoff interpolation method, it can be easily verified that $\{a_{ih} = b_i\}_{i=t_1-t_k}^{t_1-1}$ and the last coefficient of $F(\cdot)$ is equal to the secret S. It is also clear that $(t_1 - t_l)$-th derivative of $F(\cdot)$, for some $1 \leq l \leq m$, is equal to:

$$F^{(t_1-t_l)}(x) = \sum_{j=max\{0,(t_k-t_l)\}}^{t_k-1} \sum_{i=0}^{t_k-1} (-1)^{(i+j)} sh_{\alpha_i} \frac{|A_i(E,X,\varphi_j)|}{|A(E,X,\varphi)|} \frac{(j)!}{(j+t_1-t_k)!} \frac{(j+t_1-t_k)!}{(j-t_k+t_l)!} (x^{j-t_k+t_l}). \quad (8)$$

We now show that the final share of each player $P_\beta \in \mathcal{U}$ in T_{h+1} is equal to $sh_\beta = f_{h+1}^{(t_1-t_l)}(ID'_{P_\beta}) = F^{(t_1-t_l)}(ID'_{P_\beta}) + \sum_{j=0}^{t_k-1} f_{2\alpha_i}^{(t_1-t_l)}(ID'_{P_\beta})$, where ID'_{P_β} is the identity of P_β in T_{h+1} and $P_\beta \in \mathcal{U}_l$ according to P_β's new trust value:

$$\begin{aligned}
sh_\beta &= \sum_{i=0}^{t_k-1} [sh_{P_{\alpha_i} \to P_\beta}] = \sum_{i=0}^{t_k-1} [f_{\alpha_i}^{(t_1-t_l)}(ID'_{P_\beta})] \\
&= \sum_{i=0}^{t_k-1} [f_{1\alpha_i}^{(t_1-t_l)}(ID'_{P_\beta})] + \sum_{i=0}^{t_k-1} [f_{2\alpha_i}^{(t_1-t_l)}(ID'_{P_\beta})] \\
&= \sum_{i=0}^{t_k-1} \sum_{j=max\{0,(t_k-t_l)\}}^{t_k-1} \\
&\quad \left[(-1)^{(i+j)} sh_{\alpha_i} \frac{|A_i(E,X,\varphi_j)|}{|A(E,X,\varphi)|} \frac{(j)!}{(j+t_1-t_k)!} \frac{(j+t_1-t_l)!}{((j+t_l-t_k))!} (ID'_{P_\beta})^{(j-(t_k-t_l))} \right] \\
&\quad + \sum_{i=0}^{t_k-1} [f_{2\alpha_i}^{(t_1-t_l)}(ID'_{P_\beta})] \\
&= F^{(t_1-t_l)}(ID'_\beta) + \sum_{i=0}^{t_k-1} [f_{2\alpha_i}^{(t_1-t_l)}(ID'_{P_\beta})] = f_{h+1}^{(t_1-t_l)}(ID'_{P_\beta}).
\end{aligned}$$

Now, we show that the share renewal phase is unconditionally secure. Let $UnAutsub = \{P_{\beta_1}, \cdots, P_{\beta_{t_k-1}}\}$ $(1 \le k \le m)$ be an unauthorized subset of the players in period T_h. We first show that the members of $UnAutsub$ obtain no information about the old shares of $Autsub$'s members from the subshares that they receive from $Autsub$'s members. In T_h, $sh_{P_{\alpha_i} \to P_{\beta_r}} = f_{\alpha_i}^{(t_1-t_l)}(ID'_{P_{\beta_r}})$ is the subshare that each player $P_{\beta_r} \in UnAutsub$ receives from each player $P_{\alpha_i} \in Autsub$, where $P_{\beta_r} \in \mathcal{U}_l$ due to P_β's trust value in T_h and $ID'_{P_{\beta_r}}$ is the identity of P_{β_r} in T_h. The polynomial $f_{\alpha_i}(\cdot)$ can be recomputed as follows:

$$
\begin{aligned}
f_{\alpha_i}(x) &= f_{1\alpha_i}(x) + f_{2\alpha_i}(x) \\
&= \sum_{j=0}^{t_1-2} a_{j\alpha_i} x^j + \sum_{j=0}^{t_k-1} \left[(-1)^{i+j} sh_{\alpha_i} \frac{|A_i(E,X,\varphi_j)|}{|A(E,X,\varphi)|} \frac{(j)!}{(j+t_1-t_k)!} x^{j+t_1-t_k} \right] \\
&= \sum_{j=0}^{t_1-t_k-1} a_{j\alpha_i} x^j \\
&+ \sum_{j=t_1-t_k}^{t_1-2} \left[\left(a_{j\alpha_i} + (-1)^{i+j-t_1+t_k} sh_{\alpha_i} \frac{|A_i(E,X,\varphi_{j-t_1+t_k})|}{|A(E,X,\varphi)|} \frac{(j-t_1+t_k)!}{(j)!} \right) x^j \right] \\
&+ \left[(-1)^{i+t_k-1} sh_{\alpha_i} \frac{|A_i(E,X,\varphi_{t_k-1})|}{|A(E,X,\varphi)|} \frac{(t_k-1)!}{(t_1-1)!} \right] x^{t_1-1} \\
&= \sum_{j=0}^{t_1-t_k-1} a_{j\alpha_i} x^j + \sum_{j=t_1-t_k}^{t_1-2} \left[(a_{j\alpha_i} + sh_{\alpha_i} b_j)\, x^j \right] + sh_{\alpha_i} b_{t_1-1} x^{t_1-1},
\end{aligned}
$$

where

$$
b_j = (-1)^{i+j-t_1+t_k} \left(\frac{|A_i(E,X,\varphi_{j-t_1+t_k})|}{|A(E,X,\varphi)|} \right) \left(\frac{(j-t_1+t_k)!}{(j)!} \right),
$$

for $j = (t_1 - t_k), \cdots, (t_1 - 1)$. Denoting $a_{j\alpha_i}$ by c_j for $j = 0, \cdots, (t_1 - t_k - 1)$ and $a_{j\alpha_i} + sh_{\alpha_i} b_j$ by c_j for $j = (t_1 - t_k), \cdots, (t_1 - 2)$, we have:

$$
f_{\alpha_i}(x) = \sum_{j=0}^{t_1-2} c_j x^j + sh_{\alpha_i} b_{t_1-1} x^{t_1-1}.
$$

Therefore, the procedure that each player follows in the share renewal phase is the same as the sharing of the secret $S = sh_{\alpha_i} b_{t_1-1}$ using Tassa's secret sharing scheme. The unconditional security of Tassa's scheme makes it impossible to obtain any information on $b_{t_1-1} sh_{\alpha_i}$ from the subshares belonging to the members of $UnAutsub$. Moreover, $b_{t_1-1} = \left[(-1)^{i+t_k-1} \left(\frac{|A_i(E,X,\varphi_{t_k-1})|}{|A(E,X,\varphi)|} \right) \left(\frac{(t_k-1)!}{(t_1-1)!} \right) \right]$ can be computed publicly. Hence, obtaining any information on sh_{α_i} from the subshares computed by P_{α_i} is equal to obtaining the same information on $b_{t_1-1} sh_{\alpha_i}$. As a result, an unauthorized subset of players in T_h can not obtain any information about the old shares of $Autsub$'s members.

Without obtaining any information about other players' shares, an unauthorized subset of players have only access to their shares from different periods. Furthermore, we show that an unauthorized subsets of players obtain no information about the secret by having access to their own shares belonging to different time periods. Let $f_h(\cdot)$ denote the polynomial that is shared among the set of participants in T_h for $h = 1, 2, \cdots$. Note that the only thing $f_h(\cdot)$-s have in common is their last coefficient. To simplify the proof without loss of generality, we consider the case when unauthorized subsets of players have

only access to their own shares from two consecutive time periods T_h and T_{h+1}. It is not hard to show that the proof can be simply generalized.

Suppose $UnAutsub$ is authorized neither in T_h nor in T_{h+1} and, that it only requires one player from $\mathcal{U}_k$ or higher levels to become an authorized subset in either of T_h or T_{h+1}, i.e., $|UnAutsub \cap \mathcal{U}_i| = t_i - 1$ $(i = k, \cdots, m)$ in either of T_h or T_{h+1}. Let $\mathcal{U}_{m+1}$ be an imaginary authority level with threshold $t_{m+1} = 1$ which has a phantom player P_0. Let $ImaginAutsub = UnAutsub \cup \{P_0\}$ and also S' be an arbitrary element of $GF(q)$. By assigning $sh_{P_0} = \frac{S'}{(t_1-1)!}$ (note that P_0's share is fixed in all periods), the Birkhoff interpolation problem that corresponds to the shares of $ImaginAutsub$ would be well-posed in all periods. As a result, the shares of $ImaginAutsub$'s members can be used to recover polynomials:

$$f_j(x) = b_{j(t_1-t_k)}x^{t_1-t_k} + b_{j(t_1-t_k+1}x^{t_1-t_k+1} + \cdots + b_{j(t_1-2)}x^{t_1-2} + S'x^{t_1-1}$$

at T_j for $j = h$ or $h + 1$. The well-posedness of the corresponding Birkhoff interpolation problems implies that the shares of the $ImaginAutsub$'s players are consistent with the recovered polynomials. As a consequence, the last coefficient of each recovered polynomial would be equal to S'. Therefore, by having the shares of an unauthorized subset of players, the secret could be any $S' \in GF(q)$. This means that without obtaining any information about the other players' shares, participants of an unauthorized subset can not obtain any information about the secret. □

Theorem 4. Our proposed Ideal SSS scheme is unconditionally secure in a passive adversary setting.

Proof. The unconditional security of the social tuning protocol depends on the security of the share renewal phase, which is shown to be secure in Theorem 3. The unconditional security of the sharing and reconstruction protocols is the same as the unconditional security of Tassa's scheme [18], however, we provide a brief clarification here. In these protocols, players of an unauthorized subset have only access to their own shares (possibly belonging to different time periods). As we stated in Theorem 3, these players obtain no information about the actual secret and the secret, recovered by these parties, can be any element of $GF(q)$. This completes the proof. Therefore, our proposed Ideal SSS scheme is unconditionally secure in a passive adversary setting. □

4.2 Comparing Ideal SSS with Standard SSS

In this section, our proposed construction is compared with the first scheme of Nojoumian et al. (i.e., the one which is secure in a passive adversary model) in terms of the share size, communication and computational complexities.

The analysis shows that our proposed scheme outperforms Nojoumian et al.'s scheme in terms of the share size, communication complexity and computational complexity of the "sharing" protocol, however, the "social tuning" and "reconstruction" protocols of Nojoumian et al.'s scheme are computationally more efficient than those in our scheme. Depending on the number of execution of social tuning protocol, this might be a reasonable compromise because the reconstruction protocol is executed only once throughout the secret's lifetime.

Note that all computations are perform in finite field $GF(q)$. Furthermore, in standard social secret sharing, the total number of shares that a single player P_i receives is less that the threshold, i.e., $w_i < t$, meaning that an individual player cannot recover the secret. For the sake of simplicity in our complexity analysis, we assume $w = t$. The results are summarized in Table 1.

4.2.1 Share Size

In Nojoumian et al.'s scheme, the size of the share that each party receives is proportional to his weight, i.e., the size of P_i's share is equal to $w_i|q|$, where w_i is the weight of player P_i and $|q|$ is the bit length of q. As we stated earlier, the share size is approximated to $t|q|$, where t is the threshold of the scheme. Compared to Nojoumian et al.'s scheme, in our proposed scheme, the size of each participant's share is a fixed value equal to $|q|$. In other words, our proposed scheme is an ideal social secret sharing scheme.

4.2.2 Communication Complexity

In this section, our proposed scheme is compared with Nojoumian et al.'s scheme in terms of the communication complexity. We compute the number of communication rounds that is required in each construction. In both schemes, the sharing and reconstruction protocols require only 1 round of communication. However, the social tuning protocol of the proposed scheme requires only 1 round of communication (step-1.d.ii of Figure 4) whereas, that of Nojoumian et al.'s scheme requires 3 rounds of communication (2 communication rounds are required in step-3 of Phase-(I) for the enrollment protocol and 1 communication round is required in step-2 of Phase-(II) for the proactive share update; for details, see [1,2]). Therefore, the proposed scheme outperforms Nojoumian et al.'s scheme in terms of the communication complexity.

4.2.3 Computational Complexity

Next, our proposed construction is compared with Nojoumian et al.'s scheme in terms of the computational complexity. The comparison is based on the number of multiplication operations performed in each protocol.

Let n denote the maximum number of parties who can join the scheme and let t be the threshold of the scheme; note that $n > t$. Also, let w (for the sake of simplicity $w = t$) be the maximum weight of each player in Nojoumian et al.'s scheme. In our construction, the number of players in authorized subsets are not fixed (i.e., there can be authorized subsets with the size of t_1, t_2, $\cdots$, or t_m). As a result, the computational complexity of the social tuning and reconstruction protocols of our scheme depends on the number of parties who execute these protocols. Therefore, we consider the worst case scenario where the size of the subset of players is equal to t_1. Furthermore, it would be realistic to assume that, in our scheme, the authority of each player belonging to the lowest level is equal to the authority of a player who possesses only one share in Nojoumian et al.'s scheme, that is, $t_1 = t$.

In the sharing protocol of our scheme, the dealer computes the derivatives of a polynomial of degree $t - 1$, which can be done in $O(t^2)$. Furthermore, he performs, at most, n polynomial evaluations. The computational complexity of a polynomial evaluation (for a polynomial of degree t) is $O(t)$. As a result, the sharing protocol of our scheme has a complexity of $O(t^2 + tn) \in O(tn)$. In Nojoumian et al.'s scheme, the dealer performs, at most, wn polynomial evaluations where degrees of polynomials are t. Therefore, the sharing protocol of Nojoumian et al.'s scheme has a complexity of $O(wtn) \in O(t^2 n)$.

In both constructions, the share renewal phase is the time consuming part of the social tuning protocol. In our scheme, each player requires to compute a polynomial using his old share and parts of the Birkhoff interpolation method (Item 1.b of Figure 4). Furthermore, he computes different derivatives of a polynomial of degree $t - 1$ at n points (Item 1.d of Figure 4). The former procedure has a complexity of $O(t^4)$ using the naive approach, i.e., computing $t + 1$ determinants of size $t \times t$ according to Eq.(4). However, it is known that the determinant of an $t \times t$ matrix can be computed in $O(M(t))$ time, where $M(t)$ is the minimum time required to multiply any two $t \times t$ matrices [26]. The best known solution for matrix multiplication requires $O(t^{2.373})$ operations [27], therefore, the generation of $f_{1\alpha_i}(\cdot)$ in step 1.b of Figure 4 and the Birkhoff interpolation method have complexities of $O(t^{3.373})$. The latter procedure has a complexity of $O(tn)$. Therefore, the social tuning phase of our scheme requires $O(t^{3.373} + tn)$ operations. However, in the social tuning phase of Nojoumian et al.'s scheme, each player evaluates a polynomial of degree $t - 1$ at wn points, i.e., proactive share update. Assuming $w = t$, this takes $O(t^2 n)$ operations.

Finally, in the reconstruction protocol of our scheme, a trusted party who has access to the shares of an authorized subset of players can recover the secret by solving the corresponding Birkhoff interpolation problem. As we stated earlier, this takes $O(t^{3.373})$ operations. However, the reconstruction protocol of Nojoumian et al.'s scheme uses the Lagrange interpolation method that takes $O(t \log t)$ operations via the Vandermonde matrix.

Table 1
Comparison of Our Ideal SSS with Standard SSS.

Protocol	Share	Communication Complexity			Computational Complexity		
(passive)	Size	*Sha*	*Tun*	*Rec*	*Sha*	*Tun*	*Rec*
Ideal SSS	$\|q\|$	1	1	1	$O(tn)$	$O(t^{3.373} + tn)$	$O(t^{3.373})$
Standard SSS	$t\|q\|$	1	3	1	$O(t^2 n)$	$O(t^2 n)$	$O(t \log t)$

5 Concluding Remarks

We proposed an ideal social secret sharing scheme using a hierarchical TSS scheme. We illustrated that our construction is more efficient in terms of the share size, communication complexity and computational complexity of the "sharing" protocol compared to the standard social secret sharing scheme. We also showed that the "social tuning" and "reconstruction" protocols of standard social secret sharing are computationally more efficient than those of our proposed scheme. This seems a reasonable compromise because the number of execution of social tuning protocol can be predetermined ahead of time. Furthermore, the reconstruction protocol is executed only once throughout the secret's lifetime. Finally, protecting a single share is less costly and easier than protecting a set of shares.

Based on the similarity of the Birkhoff interpolation procedure and that of the Lagrange interpolation method, it's not hard to combine Tassa's scheme [18] with a commitment scheme used in polynomial-based VSS schemes (such as Feldman's scheme [7], Pedersen's scheme [8] and Peng's scheme [9]) in order to obtain computationally or unconditionally secure verifiable hierarchical TSS schemes. After constructing such a scheme, it would be straightforward to improve the proposed scheme to be secure in an active adversary setting.

Note that the sharing protocol of our scheme is the same as Tassa's sharing protocol. Also, as explained in Theorem 3, in the share renewal phase of the social tuning protocol, each player (who participates in the share renewal phase) executes the sharing protocol of Tassa's scheme. Therefore, by constructing a verifiable hierarchical TSS scheme, the only required modifications are: (a) executing the sharing protocol of the constructed verifiable hierarchical TSS scheme instead of Tassa's sharing protocol, and (b) verifying the validity of the shares whenever it is required.

References

[1] M. Nojoumian, D. R. Stinson, M. Grainger, Unconditionally secure social secret sharing scheme, IET Information Security (IFS), Special Issue on Multi-Agent and Distributed Information Security 4 (4) (2010) 202–211.

[2] M. Nojoumian, D. R. Stinson, Brief announcement: Secret sharing based on the social behaviors of players, in: 29th ACM Symposium on Principles of Distributed Computing (PODC), 2010, pp. 239–240.

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

[4] G. R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, Vol. 48, 1979, pp. 313–317.

[5] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, in: 26th Annual IEEE Symposium on Foundations of Computer Science FOCS, 1985, pp. 383–395.

[6] D. R. Stinson, R. Wei, Unconditionally secure proactive secret sharing scheme with combinatorial structures, in: Selected Areas in Cryptography, Vol. 1758 of Lecture Notes in Computer Science, Springer, 2000, pp. 200–214.

[7] P. Feldman, A Practical Scheme for Non-interactive Verifiable Secret Sharing, in: Proceedings of the 28th Annual Symposium on Foundations of Computer Science, SFCS '87, 1987, pp. 427–438.

[8] T. P. Pedersen, Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing, in: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '91, 1992, pp. 129–140.

[9] K. Peng, Efficient VSS free of computational assumption, Journal of Parallel and Distributed Computing 71 (12) (2011) 1592 – 1597.

[10] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, Proactive secret sharing or: How to cope with perpetual leakage, in: Advances in Cryptology CRYPT0 95, Vol. 963 of Lecture Notes in Computer Science, Springer, 1995, pp. 339–352.

[11] M. Nojoumian, D. R. Stinson, On dealer-free dynamic threshold schemes, Advances in Mathematics of Communications (AMC) 7 (1) (2013) 39–56.

[12] J. C. Benaloh, J. Leichter, Generalized secret sharing and monotone functions, in: 8th Annual International Cryptology Conference CRYPTO, Vol. 403 of LNCS, Springer, 1988, pp. 27–35.

[13] M. Nojoumian, D. R. Stinson, Social secret sharing in coud computing using a new trust function, in: 10th IEEE Annual International Conference on Privacy, Security and Trust (PST), 2012, pp. 161–167.

[14] M. Nojoumian, D. R. Stinson, Socio-rational secret sharing as a new direction in rational cryptography, in: 3rd International Conference on Decision and Game Theory for Security (GameSec), Vol. 7638 of LNCS, Springer, 2012, pp. 18–37.

[15] Y. Wang, Z. Liu, H. Wang, Q. Xu, Social rational secure multi-party computation, Concurrency and Computation: Practice and Experience 26 (5) (2014) 1067–1083.

[16] E. F. Brickell, Some ideal secret sharing schemes, in: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology, EUROCRYPT '89, 1990, pp. 468–475.

[17] G. J. Simmons, How to (really) share a secret, in: Proceedings on Advances in cryptology, CRYPTO '88, 1990, pp. 390–448.

[18] T. Tassa, Hierarchical Threshold Secret Sharing, Journal of Cryptology 20 (2) (2007) 237–264.

[19] C. Lin, L. Harn, D. Ye, Ideal perfect multilevel threshold secret sharing scheme, in: Information Assurance and Security, 2009. IAS '09. Fifth International Conference on, Vol. 2, 2009, pp. 118–121.

[20] T. Tassa, N. Dyn, Multipartite Secret Sharing by Bivariate Interpolation, Journal of Cryptology 22 (2) (2009) 227–258.

[21] Q. Chen, D. Pei, C. Tang, G. Zhao, Efficient integer span program for hierarchical threshold access structure, Information Processing Letters 113 (17) (2013) 621–627.

[22] N. Pakniat, M. Noroozi, Z. Eslami, Secret image sharing scheme with hierarchical threshold access structure, Journal of Visual Communication and Image Representation 25 (5) (2014) 1093 – 1101.

[23] I. Schoenberg, On Hermite-Birkhoff interpolation, Journal of Mathematical Analysis and Applications 16 (1966) 538 – 543.

[24] K. Atkinson, A. Sharma, A partial characterization of poised Hermite–Birkhoff interpolation problems, SIAM Journal on Numerical Analysis 6 (1969) 230–235.

[25] M. Nojoumian, T. C. Lethbridge, A new approach for the trust calculation in social networks, in: E-business and Telecommunication Networks: 3rd International Conf on E-Business, Vol. 9 of CCIS, Springer, 2008, pp. 64–77.

[26] O. H. Ibarra, S. Moran, R. Hui, A generalization of the fast lup matrix decomposition algorithm and applications, Journal of Algorithms 3 (1) (1982) 45–56.

[27] V. V. Williams, Multiplying matrices faster than coppersmith-winograd, in: 44th Symposium on Theory of Computing Conference STOC, ACM, 2012, pp. 887–898.