

RESEARCH ARTICLE

Ideal Social Secret Sharing Using Birkhoff Interpolation Method

Ziba Eslami^{*1}, Nasrollah Pakniat² and Mehrdad Nojoumian³

¹Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran.

²Iranian Research Institute of Information Science and Technology (IRANDOC), Tehran, Iran.

³Department of Computer & Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, USA.

ABSTRACT

The concept of *social secret sharing* was introduced in 2010 by Nojoumian et al. In Nojoumian et al.'s scheme (called SSS), the number of shares allocated to each party depends on the player's 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. 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. Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS

Secret Sharing; Social Secret Sharing; Hierarchical Threshold Access Structure; Trust Modeling; Birkhoff Interpolation

*Correspondence

Ziba Eslami, Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran.

Received ...

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 [1, 2]. 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) [3], 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 [4, 5, 6]. In *proactive secret sharing* (PSS) [7], 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) [8] can be used. In a *weighted secret sharing* (WSS) scheme [9], 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) [10, 11], the number of shares allocated to each party depends on the player's 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 [12, 13, 14]

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 [2]. 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).

In hierarchical threshold secret sharing schemes [15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25], the secret is shared among a set of participants $\mathcal{U} = \{P_1, P_2, \dots, P_n\}$ who are divided into m hierarchical non-overlapping subsets (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 such a way that the players in \mathcal{U}_i have more authority to recover the secret than those in \mathcal{U}_j for $1 \leq j < i \leq m$. *Disjunctive hierarchical threshold secret sharing* [15, 16, 17, 18] is one of the important types of hierarchical threshold secret sharing in which the access structure is determined by a strictly decreasing sequence of threshold parameters $t_1 > t_2 > \dots > t_m$. In a disjunctive hierarchical threshold secret sharing scheme, a subset of participants A is authorized if there exists some $0 \leq j \leq m-1$ such that $|A \cap (\bigcup_{i=0}^j \mathcal{U}_{m-i})| \geq t_{m-j}$. Compared to the other types of hierarchical threshold secret sharings, in disjunctive hierarchical threshold secret sharing, players in the higher levels have more power for the secret recovery. We refer the interested reviewers to [18, 19, 21, 22, 23, 24, 25] to see other types of hierarchical threshold secret sharing schemes.

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. It should be noted that it is not straightforward to construct a social secret sharing

scheme from a hierarchical threshold secret sharing scheme. This is mainly due to the fact that in social secret sharing schemes, participants (on their own) should be able to produce shares for newcomers or new shares for those whose authority levels have been changed. However, existing literature on hierarchical threshold secret sharing schemes (specially Tassa's scheme [18]) is not able to address these issues and therefore, we had to solve these problems to achieve our ideal social secret sharing scheme.

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:

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

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

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 problems, that are unconditionally well posed, the Birkhoff interpolation problem may not admit a unique solution. The sufficient conditions for Birkhoff interpolation problem to be well posed over finite fields are given in [18].

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

Let $\varphi = \{g_0, g_1, \dots, g_{N-1}\}$ be a system of linearly independent, $N - 1$ times continuously differentiable real-valued, functions and $I'(E) = \{\alpha_i : i = 1, \dots, N\}$ 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 $C' = \{c'_i : i = 1, \dots, N\}$ 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:

$$P(x) = \sum_{j=0}^{N-1} \frac{|A(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x), \quad (2)$$

where

$$A(E, X, \varphi) = (a_{ij})_{N \times N}, \quad (3)$$

$a_{ij} = g_{j-1}^{(\alpha_i(2))}(x_{\alpha_i(1)})$ for $i = 1, \dots, N$ and $j = 1, \dots, N$, $|\cdot|$ is the determinant operation and $A(E, X, \varphi_j)$ can be computed by replacing $(j + 1)$ -th column of matrix (3) with C' .

Equation (2) is widely used to construct hierarchical threshold secret sharing schemes using Birkhoff interpolation [18, 20, 21, 24]. However, relying upon this equation in which the entire column C' should be available, it might seem that we can not employ Birkhoff interpolation to construct dynamic or social secret sharing schemes (where each shareholder has access to only one entry of C'). In the following, we show how this equation can be modified to solve the problem.

By reformulating equation (2) (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 (equation (1)):

$$P(x) = \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} (-1)^{(i+j)} c'_{i+1} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x), \quad (4)$$

which can be rewritten as

$$P(x) = \sum_{i=0}^{N-1} c'_{i+1} \left(\sum_{j=0}^{N-1} (-1)^{(i+j)} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x) \right), \quad (5)$$

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:

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

As a result, we have $N = 4$ 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 values and Equations (2) and (3), 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 equation (2), 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 [26]. 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 [10, 11].

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, \dots, P_n partitioned into m levels $\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_m$. Also, assume that the sequence of threshold requirements $t_1 > t_2 > \dots > t_m$ 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.

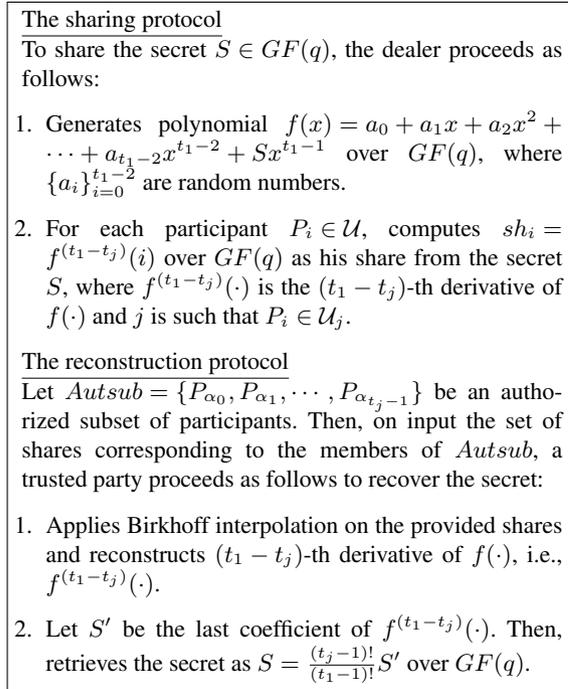


Figure 1. Tassa's Disjunctive Hierarchical Threshold Secret Sharing Scheme.

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 ($i = 1, \dots, m$). 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 $1 \leq j < i \leq m$.

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 power 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 [18]. 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 [26], which is also used in [10, 11, 12]. 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

$$\begin{aligned} I_1 &= \left(\xi_1, \xi_1 + \frac{(\xi_2 - \xi_1)}{m} \right), \\ I_2 &= \left[\xi_1 + \frac{(\xi_2 - \xi_1)}{m}, \xi_1 + \frac{2(\xi_2 - \xi_1)}{m} \right), \\ &\vdots \\ I_m &= \left[\xi_2 - \frac{(\xi_2 - \xi_1)}{m}, \xi_2 \right). \end{aligned}$$

We associate the subinterval I_i to the authority level \mathcal{U}_i , for $i = 1, \dots, m$. 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.

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 is what make the proposed scheme different from Tassa's scheme and adds new functionalities to the scheme. 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:

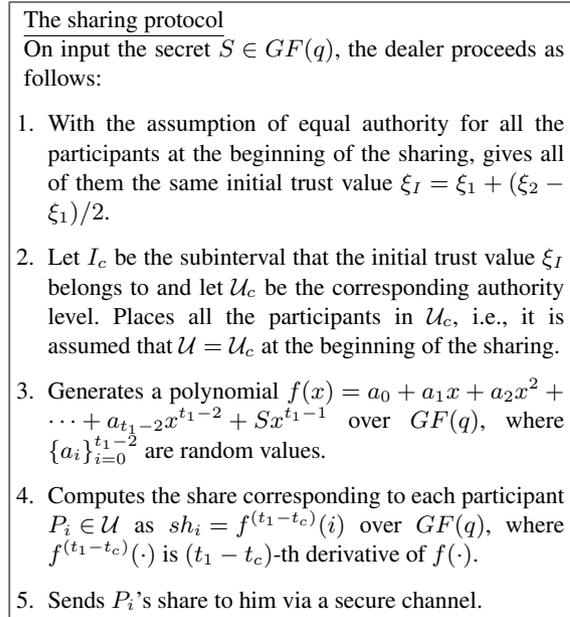


Figure 2. Sharing Protocol of the Ideal Social Secret Sharing Scheme.

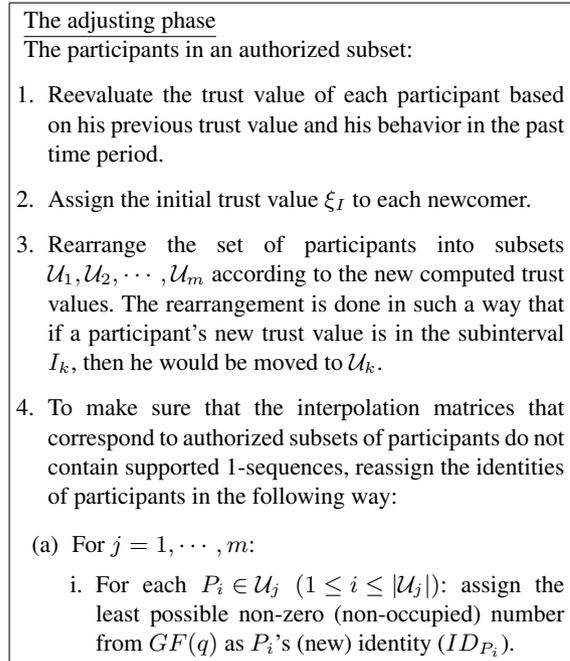


Figure 3. Adjusting Phase of the Ideal Social Secret Sharing Scheme.

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. In the proposed scheme, this is assured through step 4 of Figure 3 and therefore, in this example, the identity allocation could be $ID_{P_1} = 1, ID_{P_5} = 2, ID_{P_6} = 3, ID_{P_3} = 4, ID_{P_4} = 5, ID_{P_8} = 6, ID_{P_2} = 7, ID_{P_7} = 8, ID_{P_9} = 9, ID_{P_{10}} = 10$; however, ignoring this step may result in the following identity allocation which might lead to an unsolvable instance of the Birkhoff interpolation problem: $ID_{P_1} = 10, ID_{P_5} = 1, ID_{P_6} = 8, ID_{P_3} = 7, ID_{P_4} = 6, ID_{P_8} = 5, ID_{P_2} = 4, ID_{P_7} = 3, ID_{P_9} = 2, ID_{P_{10}} = 9$.

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.

It should be noted that in Tassa's secret sharing scheme, participants are not able to generate shares for newcomers or for those whose authority level have been changed. The issue is overcome in the proposed scheme through equation (5).

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 $sh_\beta = f_{i+1}^{(t_1-t_l)}(ID'_{P_\beta})$.

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.

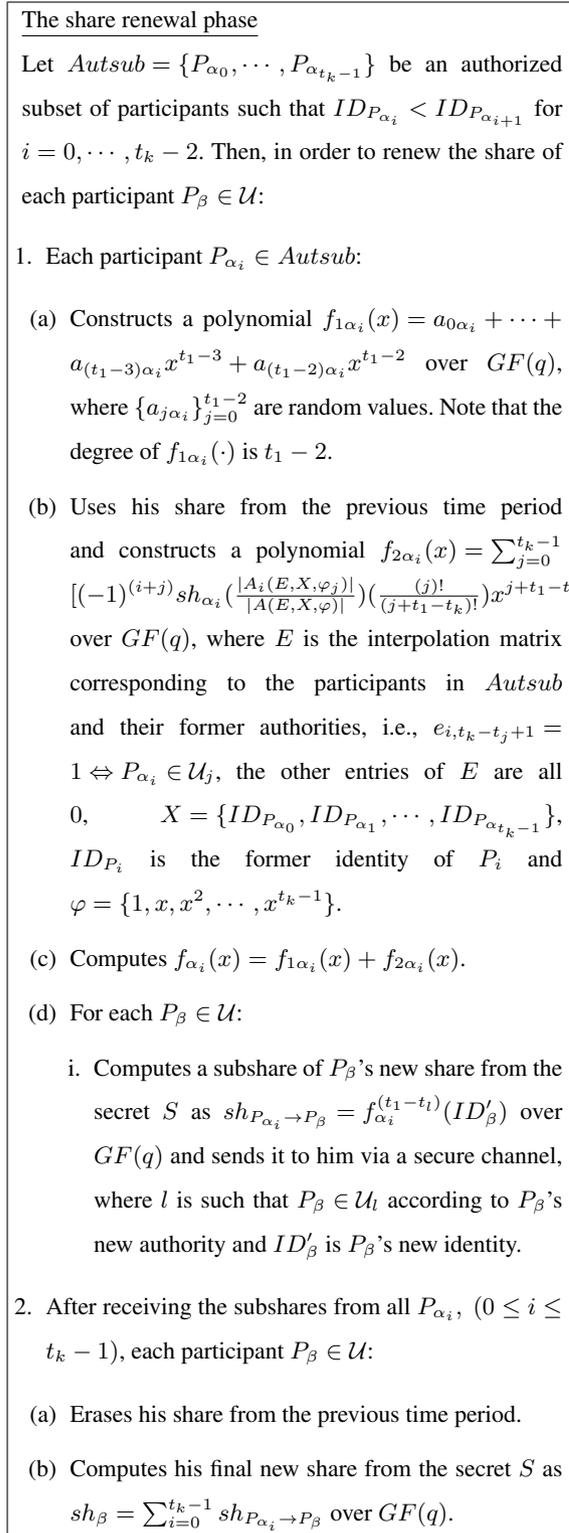


Figure 4. Share Renewal Phase of the Ideal Social Secret Sharing Scheme.

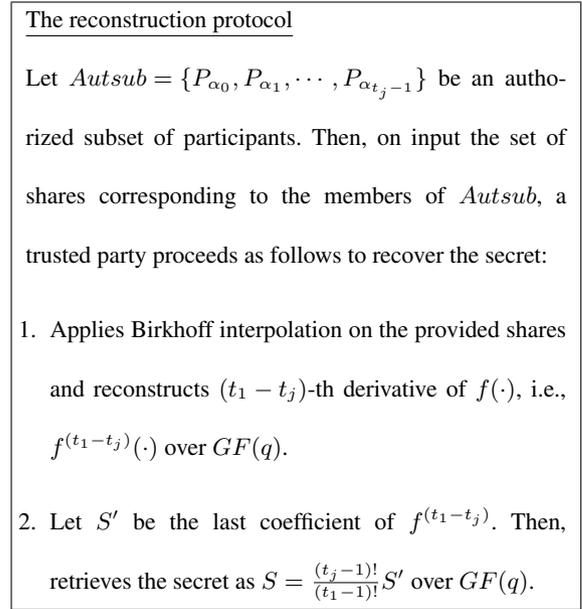


Figure 5. Reconstruction Protocol of the Ideal Social Secret Sharing Scheme.

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 1

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 $A_{\text{tsub}} = \{P_{\alpha_0}, \dots, P_{\alpha_{t_k-1}}\}$ can be used to retrieve the

following polynomial:

$$F(x) = \sum_{i=t_1-t_k}^{t_1-1} b_i x^i = \sum_{j=0}^{t_k-1} \sum_{i=0}^{t_k-1} (-1)^{(i+j)} sh_{\alpha_i} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} \frac{(j)!}{(j+t_1-t_k)!} (x^{j+t_1-t_k}). \quad (6)$$

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:

$$F^{(t_1-t_l)}(x) = \sum_{j=\max\{0, (t_k-t_l)\}}^{t_k-1} \sum_{i=0}^{t_k-1} (-1)^{(i+j)} sh_{\alpha_i} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} \frac{(j)!}{(j+t_1-t_k)!} \frac{(j-t_k+t_l)!}{(j-t_k+t_l)!} (x^{j-t_k+t_l}). \quad (7)$$

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:

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

Now, we show that the share renewal phase is unconditionally secure. Let $UnAutsub = \{P_{\beta_1}, \dots, P_{\beta_{t_k-1}}\}$ ($1 \leq k \leq m$) 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 , $sh_{P_{\alpha_i} \rightarrow P_{\beta_r}} = f_{\alpha_i}^{(t_1-t_l)}(ID'_{P_{\beta_r}})$ 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:

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

where

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

for $j = (t_1 - t_k), \dots, (t_1 - 1)$. Denoting $a_{j\alpha_i}$ by c_j for $j = 0, \dots, (t_1 - t_k - 1)$ and $a_{j\alpha_i} + sh_{\alpha_i} b_j$ by c_j for $j = (t_1 - t_k), \dots, (t_1 - 2)$, 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, $b_{t_1-1} = [(-1)^{i+t_k-1} \left(\frac{|A_i(E, X, \varphi_{t_k-1})|}{|A(E, X, \varphi)|} \right) \left(\frac{(t_k-1)!}{(t_1-1)!} \right)]$ 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 $h = 1, 2, \dots$. 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 $UnAutsb$ 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., $|UnAutsb \cap \mathcal{U}_i| = t_i - 1$ ($i = k, \dots, m$) 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 $ImaginAutsb = UnAutsb \cup \{P_0\}$ 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 $ImaginAutsb$ would be well-posed in all periods. As a result, the shares of $ImaginAutsb$'s members can be used to recover polynomials:

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

at T_j for $j = h$ or $h + 1$. The well-posedness of the corresponding Birkhoff interpolation problems implies that the shares of the $ImaginAutsb$'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. \square

Theorem 2

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 1. 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 1, 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. \square

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 performed 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 than 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 I.

4.2.1. Share Size

In Nojoumian et al.'s scheme, assigning different levels of authority is achieved using Shamir's weighted threshold secret sharing scheme [2]. In Shamir's scheme, the size of the assigned share to each shareholder 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 a consequence, the same statement is true about Nojoumian et al.'s scheme. Therefore, the share size of Nojoumian et al.'s scheme is approximated to $t|q|$, where t is the threshold of the scheme. Compared to Nojoumian et al.'s scheme, in our proposed scheme, different levels of authority is achieved using Tassa's hierarchical threshold secret sharing scheme (the second scheme of [18]). The ideality of Tassa's scheme makes the proposed scheme an Ideal social secret sharing scheme, i.e., the size of each participant's share in the proposed scheme is a fixed value equal to $|q|$.

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 [10, 11]). 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, \dots , 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 $O(wtn) \in O(t^2n)$.

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 equation (2). 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 [27]. The best known solution for matrix multiplication requires $O(t^{2.373})$ operations [28], 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 $O(t^2n)$ 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.

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.

The proposed scheme is only secure in the passive adversarial model. Using a similar method to the one used in [24], it is straightforward to obtain a computationally secure version of the proposed scheme in the active adversarial model. However, modifying the proposed scheme in such a way that the result would be unconditionally secure in the active adversarial model seems to be a challenging problem which we leave it as a future work.

REFERENCES

1. Blakley GR. Safeguarding cryptographic keys. *Proceedings of the National Computer Conference*, vol. 48, 1979; 313–317.
2. Shamir A. How to share a secret. *Communications of the ACM* 1979; 22(11):612–613.
3. Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. *26th Annual IEEE*

- Symposium on Foundations of Computer Science FOCS*, 1985; 383–395.
4. Feldman P. A Practical Scheme for Non-interactive Verifiable Secret Sharing. *Proceedings of the 28th Annual Symposium on Foundations of Computer Science, SFCS '87*, 1987; 427–438.
 5. Pedersen TP. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '91*, 1992; 129–140.
 6. Stinson DR, Wei R. Unconditionally secure proactive secret sharing scheme with combinatorial structures. *Selected Areas in Cryptography, Lecture Notes in Computer Science*, vol. 1758. Springer, 2000; 200–214.
 7. Herzberg A, Jarecki S, Krawczyk H, Yung M. Proactive secret sharing or: How to cope with perpetual leakage. *Advances in Cryptology CRYPTO 95, Lecture Notes in Computer Science*, vol. 963, Springer, 1995; 339–352.
 8. Nojoumian M, Stinson DR. On dealer-free dynamic threshold schemes. *Advances in Mathematics of Communications (AMC)* 2013; 7(1):39–56.
 9. Benaloh JC, Leichter J. Generalized secret sharing and monotone functions. *8th Annual International Cryptology Conference CRYPTO, LNCS*, vol. 403, Springer, 1988; 27–35.
 10. Nojoumian M, Stinson DR. Brief announcement: Secret sharing based on the social behaviors of players. *29th ACM Symposium on Principles of Distributed Computing (PODC)*, 2010; 239–240.
 11. Nojoumian M, Stinson DR, Grainger M. Unconditionally secure social secret sharing scheme. *IET Information Security (IFS), Special Issue on Multi-Agent and Distributed Information Security* 2010; 4(4):202–211.
 12. Nojoumian M, Stinson DR. Social secret sharing in cloud computing using a new trust function. *10th IEEE Annual International Conference on Privacy, Security and Trust (PST)*, 2012; 161–167.
 13. Nojoumian M, Stinson DR. Socio-rational secret sharing as a new direction in rational cryptography. *3rd International Conference on Decision and Game Theory for Security (GameSec), LNCS*, vol. 7638, Springer, 2012; 18–37.
 14. Wang Y, Liu Z, Wang H, Xu Q. Social rational secure multi-party computation. *Concurrency and Computation: Practice and Experience* 2014; 26(5):1067–1083.
 15. Brickell EF. Some ideal secret sharing schemes. *Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology, EUROCRYPT '89*, 1990; 468–475.
 16. Lin C, Harn L, Ye D. Ideal perfect multilevel threshold secret sharing scheme. *Information Assurance*

- and Security, 2009. IAS '09. Fifth International Conference on*, vol. 2, 2009; 118–121.
17. Simmons GJ. How to (really) share a secret. *Proceedings on Advances in cryptology, CRYPTO '88*, 1990; 390–448.
 18. Tassa T. Hierarchical Threshold Secret Sharing. *Journal of Cryptology* 2007; **20**(2):237–264.
 19. Tassa T, Dyn N. Multipartite Secret Sharing by Bivariate Interpolation. *Journal of Cryptology* 2009; **22**(2):227–258.
 20. Guo C, Chang CC, Qin C. A hierarchical threshold secret image sharing. *Pattern Recognition Letters* 2012; **33**(1):83–91.
 21. Pakniat N, Noroozi M, Eslami Z. Secret image sharing scheme with hierarchical threshold access structure. *Journal of Visual Communication and Image Representation* 2014; **25**(5):1093 – 1101.
 22. Basu A, Sengupta I, Sing JK. Secured hierarchical secret sharing using ecc based signcryption. *Security and Communication Networks* 2012; **5**(7):752–763.
 23. Padró C, Sáez G. Secret sharing schemes with bipartite access structure. *Information Theory, IEEE Transactions on* 2006; **46**(7):2596–2604.
 24. Pakniat N, Noroozi M, Eslami Z. Distributed key generation protocol with hierarchical threshold access structure. *IET Information Security* 2015; **9**:248–255.
 25. Eslami Z, Pakniat N, Noroozi M. Hierarchical threshold multi-secret sharing scheme based on birkhoff interpolation and cellular automata. *Computer Architecture and Digital Systems (CADS), 2015 18th CSI International Symposium on*, 2015; 1–6.
 26. Nojoumian M, Lethbridge TC. A new approach for the trust calculation in social networks. *E-business and Telecommunication Networks: 3rd International Conf on E-Business, CCIS*, vol. 9, Springer, 2008; 64–77.
 27. Ibarra OH, Moran S, Hui R. A generalization of the fast lup matrix decomposition algorithm and applications. *Journal of Algorithms* 1982; **3**(1):45–56.
 28. Williams VV. Multiplying matrices faster than coppersmith-winograd. *44th Symposium on Theory of Computing Conference STOC, ACM*, 2012; 887–898.

Table 1. Comparison of Our Ideal SSS with Standard SSS.

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