RESEARCH ARTICLE

Ideal Social Secret Sharing Using Birkhoff Interpolation Method

Ziba Eslami¹, Nasrollah Paknia² 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

¹Correspondence
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 \( U = \{P_1, P_2, \ldots, P_n\} \) who are divided into \( m \) hierarchical non-overlapping subsets (i.e., \( U = \bigcup_{i=0}^{m-1} U_i \) and \( U_i \cap U_j = \emptyset \) where \( i \neq j \)) in such a way that the players in \( U_i \) have more authority to recover the secret than those in \( U_j \) 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 \( t_1 > t_2 > \cdots > t_m \). 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 \( A \cap \left( \bigcup_{i=0}^{j} U_{m-i} \right) \geq t_{m-j} \). 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 (specifically 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:

- \( X = \{x_1, \ldots, x_k\} \) is a given set of points in the set of real numbers \( (R) \), where \( x_1 < x_2 < \cdots < x_k \);
- \( E = (e_{i,j})_{1 \leq i \leq k, 0 \leq j \leq l} \) 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
- \( C = \{e_{i,j} : (i, j) \in I(E)\} \) 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

\[
P^{(j)}(x_i) = e_{i,j}, \; (i, j) \in I(E),
\]

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 \( \varphi = \{g_0, g_1, \ldots, g_{N-1}\} \) be a system of linearly independent, \( N-1 \) times continuously differentiable real-valued, functions and \( I'(E) = \{\alpha_i : i = 1, \ldots, N\} \) 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 \( C' = \{c'_i : i = 1, \ldots, N\} \) 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 \( E, X, \varphi \), we are able to solve the Birkhoff interpolation problem as follows:

\[
P(x) = \sum_{j=0}^{N-1} A(E, X, \varphi_j) g_j(x),
\]

where

\[
A(E, X, \varphi) = (a_{ij})_{N \times N},
\]

\[
a_{ij} = g_j^{(\alpha_i(2))}(x_{\alpha_i(1)}) \quad \text{for} \quad i = 1, \ldots, N \quad \text{and} \quad j = 1, \ldots, N, \quad |i| \]

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 cannot 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)):

\[
P(x) = \sum_{j=0}^{N-1} \sum_{i=0}^{N-1} (-1)^{(i+j)} c_{i+1}^{(j+1)} \frac{|A(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x),
\]

which can be rewritten as

\[
P(x) = \sum_{i=0}^{N-1} c_{i+1} \left( \sum_{j=0}^{N-1} (-1)^{(i+j)} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x) \right),
\]

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:

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

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

\[
|A(E, X, \varphi)| = \begin{pmatrix}
1 & 1 & 1 & 1 \\
0 & 2 & 4 & 8 \\
0 & 0 & 0 & 6
\end{pmatrix} = 12,
\]

\[
|A(E, X, \varphi_0)| = \begin{pmatrix}
10 & 1 & 1 & 1 \\
28 & 4 & 8 & 16 \\
6 & 0 & 0 & 6
\end{pmatrix} = 48,
\]

\[
|A(E, X, \varphi_1)| = \begin{pmatrix}
1 & 10 & 1 & 1 \\
0 & 24 & 2 & 8 \\
0 & 0 & 6 & 6
\end{pmatrix} = 24,
\]

\[
|A(E, X, \varphi_2)| = \begin{pmatrix}
1 & 1 & 2 & 4 \\
0 & 28 & 4 & 8 \\
0 & 0 & 6 & 6
\end{pmatrix} = 36,
\]

\[
|A(E, X, \varphi_3)| = \begin{pmatrix}
1 & 1 & 1 & 10 \\
0 & 0 & 2 & 28 \\
0 & 0 & 0 & 6
\end{pmatrix} = 12.
\]

Using equation (2), the result of Birkhoff interpolation would be:

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

2.2. Social Secret Sharing

A social secret sharing scheme is defined by three protocols; “sharing” (Sha), “social tuning” (Sha) 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 \( U \) of \( n \) players \( P_1, P_2, \ldots, P_n \) partitioned into \( m \) levels \( U_1, U_2, \ldots, U_m \). 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 \( q > \max \{2^{-t_1 + 2} \cdot (t_1 - 1)^{(t_1 - 1)/2}, (t_1 - 1)! \cdot n(t_1 - 1)(t_1 - 2)/2, n\} \). 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.

The sharing protocol
To share the secret \( S \in GF(q) \), the dealer proceeds as follows:
1. Generates 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 numbers.
2. For each participant \( P_i \in U \), computes \( s_{hi} = f^{(t_1 - t_1)}(i) \) over \( GF(q) \) as his share from the secret \( S \), where \( f^{(t_1 - t_1)}(\cdot) \) is the \( (t_1 - t_1) \)-th derivative of \( f(\cdot) \) and \( j \) is such that \( P_i \in U_j \).

The reconstruction protocol
Let \( Autsub = \{P_{a_0}, P_{a_1}, \cdots, P_{a_{t_1 - 1}}\} \) 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 \( (t_1 - t_1) \)-th derivative of \( f(\cdot) \), i.e., \( f^{(t_1 - t_1)}(\cdot) \).
2. Let \( S' \) be the last coefficient of \( f^{(t_1 - t_1)}(\cdot) \). Then, retrieves the secret as \( S = \frac{(t_1 - 1)!}{(t_1 - t_1)!} S' \) over \( GF(q) \).

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

3. IDEAL SOCIAL SECRET SHARING

Let \( U = \bigcup_{i=1}^{m} U_i \) 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 \( U_i \). Moreover, assume that there is a threshold \( t_i \) for each level of authority \( U_i \) (\( i = 1, \cdots, m \)). 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 \( 1 \leq j < i \leq m \).

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

\[
q > 2^{m - t_1 + 2} \cdot (t_1 - m - 1)(t_1 - m - 2)/2, (t_1 - 1)! \cdot n(t_1 - 1)(t_1 - m - 1)/2, (t_1 - 1)! \cdot n(t_1 - m - 1)/2, n^{t_1 - m - 2}/2).
\]

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 \( (\xi_1, \xi_2) \). We divide the interval \( (\xi_1, \xi_2) \) into \( m \) subintervals.

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

We associate the subinterval \( I_i \) to the authority level \( U_i \), 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.

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:
The sharing protocol

On input the secret $S \in GF(q)$, 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 $\xi_t = \xi_1 + (\xi_2 - \xi_1)/2$.

2. Let $I_t$ be the subinterval that the initial trust value $\xi_t$ belongs to and let $U_t$ be the corresponding authority level. Places all the participants in $U_t$, i.e., it is assumed that $U = U_t$ at the beginning of the sharing.

3. Generates a polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{12} x^{12} + Sx^{13} - 1$ over $GF(q)$, where $\{a_i\}_{i=0}^{11}$ are random values.

4. Computes the share corresponding to each participant $P_i \in U$ as $sh_i = f(t_i - t_c)(i)$ over $GF(q)$, where $f(t_i - t_c)(\cdot)$ is the $(t_i - t_c)$-th derivative of $f(\cdot)$.

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

---

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

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 $\xi_t$ to each newcomer.

3. Rearrange the set of participants into subsets $U_1, U_2, \ldots, U_m$ 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 $U_k$.

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 $j = 1, \ldots, m$:
   
   i. For each $P_i \in U_j$ ($1 \leq i \leq |U_j|$): assign the least possible non-zero (non-occupied) number from $GF(q)$ as $P_i$’s (new) identity ($ID_{P_i}$).

---

**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) $U_1 = \{P_1, P_5, P_6\}$, $U_2 = \{P_3, P_4, P_8\}$, $U_3 = \{P_2, P_7, P_9, P_{10}\}$. 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: $ID_{P_1} = 10, ID_{P_5} = 1, ID_{P_6} = 8, ID_{P_3} = 4, ID_{P_4} = 6, ID_{P_8} = 2, ID_{P_2} = 3, ID_{P_7} = 9, ID_{P_{10}} = 9$.

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 $P_\beta$ be a party who belongs to $U_\kappa$ in $T_i$ considering his trust value. Therefore, the share that $P_\beta$ receives in $T_i$ is $sh_\beta = f_i(t_i - t_c)(ID_{P_\beta})$, where $ID_{P_\beta}$ is the identity that is assigned to $P_\beta$ in $T_i$.

Furthermore, suppose $P_\beta$’s trust value is equal to $\zeta_{P_\beta} \in I_t$ at the beginning of $T_{i+1}$ and also let his new identity be $ID_{P_\beta}$. As a result, the share that $P_\beta$ receives in $T_{i+1}$ would be equal to $sh_\beta = f_{i+1}(t_{i+1} - t_c)(ID_{P_\beta})$.

---

**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.
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 \( P_\beta \in U \):

1. Each participant \( P_{\alpha_i} \in Autsub:
   (a) Constructs a polynomial \( f_{1\alpha_i}(x) = a_{\alpha_0} + \cdots + a_{(t_1-3)\alpha_i}x^{t_1-3} + a_{(t_1-2)\alpha_i}x^{t_1-2} \) over \( GF(q) \), where \( \{ a_{\alpha_i} \}_{t_i=0}^{t_i-2} \) are random values. Note that the degree of \( f_{1\alpha_i}(\cdot) \) is 1.
   (b) Uses his share from the previous time period and constructs a polynomial \( f_{2\alpha_i}(x) = \sum_{j=0}^{t_k-1} \left[ (-1)^{(i+j)}sh_{\alpha_i}(\left[ \frac{A_{\alpha_i}(E,X,\varphi)}{A_{\alpha_i}(E,X,\varphi)} \right])_{(t_j+1-t_k)x} \right] \) over \( GF(q) \), where \( E \) is the interpolation matrix corresponding to the participants in \( Autsub \) and their former authorities, i.e., \( e_{\alpha_i \alpha_{t_k-t_i+1}} = 1 \iff P_{\alpha_i} \in U_{\alpha_j} \), the other entries of \( E \) are all 0. \( X = \{ ID_{P_{\alpha_0}}, ID_{P_{\alpha_1}}, \cdots, ID_{P_{\alpha_{t_k-1}}} \} \) is the former identity of \( P_1 \) 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 \( P_\beta \in U \):
      i. Computes a subshare of \( P_\beta \)'s new share from the secret \( S \) as \( sh_{P_{\alpha_i} \rightarrow P_\beta} = f_{1\alpha_i}(ID_{P_\beta}) \) over \( GF(q) \) and sends it to him via a secure channel, where \( l \) is such that \( P_\beta \in U_l \) according to \( P_\beta \)'s new authority and \( ID_{P_\beta} \) is \( P_\beta \)'s new identity.

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

The reconstruction protocol

Let \( Autsub = \{ P_{\alpha_0}, P_{\alpha_1}, \cdots, P_{\alpha_{t_k-1}} \} \) 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 \((t_1-t_2)\)-th derivative of \( f(\cdot) \), i.e.,
   \( f^{(t_1-t_2)}(\cdot) \) over \( GF(q) \).
2. Let \( S' \) be the last coefficient of \( f^{(t_1-t_2)}(\cdot) \). Then, retrieves the secret as \( S = \frac{(t_1-t_2)!}{(t_1-t_2)!} S' \) over \( GF(q) \).

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 \( f_h(x) = \sum_{i=0}^{t-1} a_{ij}x^i \) 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:

\[
F(x) = \sum_{i=1}^{t_k-1} b_i x^i + \sum_{j=0}^{t_k-1} (1 - j) x^{j+1} \frac{sh_{\alpha_i}}{|A(E, X, \varphi)|} \left( j + t_1 - t_k \right) \left( x^{j+1 - t_k} \right).
\]

(6)

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

\[
F^{(l+1)}(x) = \sum_{j=0}^{t_k-1} \sum_{i=0}^{t_k-1} (-1)^{(i+j)} \frac{sh_{\alpha_i}}{|A(E, X, \varphi)|} \left( j + t_1 - t_k \right) \left( x^{j+1 - t_k} \right).
\]

(7)

We now show that the final share of each player \(P_h \in U\) in \(T_{h+1}\) is equal to \(sh_{\beta} = f_{h+1}^{(t_1-t_1)}(IDP_{P_h}) = F^{(t_1-t_1)}(IDP_{P_h}) + \sum_{j=0}^{t_k-1} f_{h+1}^{(t_1-t_1)}(IDP_{P_h})\), where \(IDP_{P_h}\) is the identity of \(P_h\) in \(T_{h+1}\) and \(P_h \in U\) according to \(P_h\)’s new trust value:

\[
sh_{\beta} = \sum_{i=0}^{t_k-1} \sum_{j=0}^{t_k-1} f_{h+1}^{(t_1-t_1)}(IDP_{P_h}) = \sum_{j=0}^{t_k-1} f_{h+1}^{(t_1-t_1)}(IDP_{P_h}) = \sum_{i=0}^{t_k-1} f_{h+1}^{(t_1-t_1)}(IDP_{P_h}) = \sum_{j=0}^{t_k-1} \sum_{i=0}^{t_k-1} \frac{|A(E, X, \varphi)|}{j + t_1 - t_k} \left( x^{j+1 - t_k} \right).
\]

(8)

The polynomial \(f_{\alpha_i}(\cdot)\) can be recomputed as follows:

\[
f_{\alpha_i}(x) = f_{2\alpha_i}(x) + \sum_{j=0}^{t_k-1} \frac{|A(E, X, \varphi)|}{j + t_1 - t_k} \left( x^{j+1 - t_k} \right) = \sum_{j=0}^{t_k-1} \left( a_{j\alpha_i} x^j + \sum_{j=0}^{t_k-1} \frac{|A(E, X, \varphi)|}{j + t_1 - t_k} \left( x^{j+1 - t_k} \right) \right).
\]

(9)

where

\[
b_j = (-1)^{i+j-t_1} + \left( x^{j+1 - t_k} \right) \left( x^{j+1 - t_k} \right) = \sum_{j=0}^{t_k-1} \sum_{i=0}^{t_k-1} \left( a_{j\alpha_i} x^j + \sum_{j=0}^{t_k-1} \frac{|A(E, X, \varphi)|}{j + t_1 - t_k} \left( x^{j+1 - t_k} \right) \right).
\]

(10)

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 \(b_{t_1-1}\) from the subshares belonging to the members of \(UnAutsub\). Moreover, \(b_{t_1-1} = \left( \frac{|A(E, X, \varphi)|}{j + t_1 - t_k} \right) \left( x^{j+1 - t_k} \right) \left( x^{j+1 - t_k} \right) = \sum_{j=0}^{t_k-1} \sum_{i=0}^{t_k-1} \left( a_{j\alpha_i} x^j + \sum_{j=0}^{t_k-1} \frac{|A(E, X, \varphi)|}{j + t_1 - t_k} \left( x^{j+1 - t_k} \right) \right)
\]

(11)

Now, we show that the share renewal phase is unconditionally secure. Let \(UnAutsub = \{P_{h_1}, \ldots, P_{h_{t_k-1}}\}\) (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 subshares of \(Autsub\)’s members from the subshares that they receive from \(Autsub\)’s members. In \(T_h\), \(sh_{P_{\alpha_i} \rightarrow P_{\beta_i}} = f_{h+1}^{(t_1-t_1)}(IDP_{P_{\beta_i}})\) is the subshare that each player \(P_{\beta_i} \in UnAutsub\) receives from each player \(P_{\alpha_i} \in Autsub\), where \(P_{\beta_i} \in U\) due to \(P_h\)’s trust value in \(T_h\) and \(IDP_{P_{\beta_i}}\) is the identity of \(P_{\beta_i}\) in \(T_h\).

Z. Eslami et al.

Ideal Social Secret Sharing Using Birkhoff Interpolation Method

DOI: 10.1002/sec
Prepared using secauth.cls
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 $U_k$ or higher levels to become an authorized subset in either of $T_h$ or $T_{h+1}$, i.e., $|UnAutsub \cap U_i| = t_i - 1 \ (i = k, \ldots, m)$ in either of $T_h$ or $T_{h+1}$. Let $U_{m+1}$ 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 $sh_{P_0} = \frac{S'}{t_1!}$ (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:

$$f_j(x) = b_j(t_1 - t_k)x^{t_1 - t_k} + b_j(t_1 - t_{k+1})x^{t_1 - t_{k+1}} + \cdots + b_j(t_1 - t_2)x^{t_1 - t_2} + S'x^{t_1 - 1}$$

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. □

\textit{Theorem 2}

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

\textbf{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. □

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 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 1.

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 make 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 $t_1, t_2, \cdots, m$). 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 $O(t^3 + tn) \in O(tn)$. 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 $O(wn) \in O(t^4n)$.

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 $f_{d, \alpha_1}(\cdot)$ 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

3. Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. 26th Annual IEEE


16. Lin C, Harn L, Ye D. Ideal perfect multilevel threshold secret sharing scheme. Information Assurance


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

<table>
<thead>
<tr>
<th>Protocol (passive)</th>
<th>Share Size</th>
<th>Communication Complexity</th>
<th>Computational Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ideal SSS $</td>
<td>q</td>
<td>$</td>
<td>1 1 1</td>
</tr>
<tr>
<td>Standard SSS $t</td>
<td>q</td>
<td>$</td>
<td>1 3 1</td>
</tr>
</tbody>
</table>