The ISC Int'l Journal of Information Security

ISeCure

January 2023, Volume 15, Number 1 (pp. 127–137)

http://www.isecure-journal.org

A New Social Multi-Secret Sharing Scheme using Birkhoff Interpolation and Chinese Remainder Theorem

Mohammad Ebrahim Ebrahimi Kiasari [1], Nasrollah Pakniat [2], Abdolrasoul Mirghadri [3,1,*], and Mojtaba Nazari [1]

[1] *Faculty of Basic Science, Islamic Azad University-Khorramabad Branch, Khorramabad, Iran.*
[2] *Information Science Research Department, Iranian Research Institute for Information Science and Technology, Tehran, Iran.*
[3] *Faculty and Research Center of Communication and Information Technology, Imam Hossein University, Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: –
Revised: –
Accepted: –
Published Online: –

Keywords:
Multi-Secret Sharing, Multi-Stage Secret Sharing, Social Secret Sharing, Hierarchical Threshold Access Structure

Type: –

doi: --

dor: --

ABSTRACT

Secret sharing (SS) schemes allow the sharing of a secret among a set of trustees in such a way that only some qualified subsets of them can recover the secret. Ordinary SS schemes assume that the trust to each trustee is fixed over time. However, this is not the case in many real scenarios. Social secret sharing (SSS) is a recently introduced type of SS that addresses this issue. It allows the sharing of a secret among a set of trustees such that the amount of trust to each participant could be changed over time. There exist only a few SSS schemes in the literature; most of them can share only one secret during each execution. Hence, these schemes lack the required efficiency in situations where multiple secrets need to be shared. According to the literature, there exists only one social multi-secret sharing ($SMSS$) scheme in which, all the secrets are reconstructed at one stage. However, in many applications, the secrets should be recovered in multiple stages and even according to some pre-specified order. To address these problems, this paper proposes a new $SMSS$ scheme by using the Birkhoff interpolation method and the Chinese remainder theorem. In the proposed scheme, the shareholders can recover the secrets in different stages and according to the specified order by the dealer. The security analysis of the proposed scheme shows that it meets all the needed security requirements. In addition, the performance analysis of the proposed scheme indicates its overall superiority over the related schemes.

1 Introduction

In 1979, Shamir [1] and Blakley [2], independently, introduced the concept of secret sharing (SS). In SS schemes, a dealer shares a secret among a set of trustees in such a way that some predetermined subsets of them (called authorized subsets) can reconstruct the secret by using their shares. The access structure of an SS scheme is defined to be the set of all its authorized subsets. (t, n) Threshold secret sharing (TSS) is the most widely used type of SS. In this type of SS, the authorized subsets are those containing at least t trustees. Ordinary TSS schemes can share only one secret during each execution [1–5]. However, many secret sharing applications, such as

* Corresponding author.
Email addresses: ebrahimikiasari@yahoo.com, pakniat@irandoc.ac.ir, amrghdri@ihu.ac.ir, mo_nazari@hotmail.com
ISSN: 2008-2045

sharing encryption keys and data files, require protecting more than one secret. To use the ordinary SS schemes in these applications, each of these methods must be executed many times. This is not an efficient approach.

To overcome this issue, Harn introduced the concept of multi-secret sharing (MSS) in 1995 [6]. After that, many MSS schemes have been introduced to the literature in which the researchers tried to improve the efficiency or security or add new functionalities, or support more general access structures [7–15].

Existing MSS schemes can be divided into two categories: multi-stage schemes and single-stage ones. In multi-stage MSS schemes, the secrets can be reconstructed in different stages without compromising the security of non-reconstructed secrets [16–23]. Compared to multi-stage MSS schemes, single-stage ones are more efficient, but in these schemes, all the secrets are reconstructed simultaneously.

In the above-mentioned schemes, the participants' shares are some fixed values over time. However, this is inappropriate for the secrets with a long lifetime. That is because, for such secrets, a mobile adversary can corrupt an arbitrary number of trustees over time and recover the secret by obtaining the shares corresponding to an authorized subset. Proactive secret sharing (PSS) is another variant of secret sharing that is proposed to solve this problem [24]. In PSS schemes, participants' shares are renewed at specified time intervals (without the participation of the dealer) and therefore, the shares from different time intervals are inconsistent with each other and cannot be used to reconstruct the secret.

In the reviewed schemes, the shares corresponding to all trustees have equal importance, i.e., replacing the share corresponding to any trustee with the share corresponding to any other one does not affect the secret(s) reconstruction process. Multipartite SS is another variant of secret sharing in which, trustees could have shares with different importance according to the existing trust in them [25–29].

One desirable property that is missing in the above schemes is the ability to change the shares' importance over time according to the varying trust of the trustees. To address this issue, in 2010, Nojoumian *et al.* [30] introduced the concept of social secret sharing (SSS). In an SSS scheme, the importance of trustees' shares from the secret depends on their reputations and behaviors over time. In this type of SS, trustees' shares are updated periodically over time to adjust their shares according to their reputations and behaviors.

In their seminal work, Nojoumian *et al.* [30] at first proposed an SSS scheme secure in the passive adversary model (in the passive adversarial model, the adversary is only allowed to eavesdrop on the exchanged messages). Then, they used the verifiable SS scheme of [31] and proposed an SSS scheme secure in the active adversarial model (compared to the passive adversarial model, in the active one, the adversary is also able to modify, delete and send messages). In [32], the authors introduced the concept of socio-rational secret sharing. In [33], SSS schemes are used to create a self-organizing environment in cloud computing. In [34], Eslami *et al.* used Tassa's hierarchical TSS ($HTSS$) scheme [26] and proposed an ideal SSS scheme secure in the passive adversarial model. In this scheme, 1) the shares are generated using appropriate derivatives of some polynomial; 2) by using the properties of the Birkhoff interpolation method, the trustees can renew their shares without the participation of the dealer; 3) authorized subsets can recover the secrets by using the Birkhoff interpolation method.

In [35], Pakniat and Eslami used symmetric encryption schemes and proposed a social MSS ($SMSS$) scheme. This scheme, which is the only existing $SMSS$ scheme, is not multi-stage (i.e., all the secrets are reconstructed at once in this scheme). Therefore, this scheme cannot be used in situations in which the reconstruction of the secrets should be done in different stages and even more, according to a specified order. To address these problems, a new $SMSS$ scheme is proposed in this paper. The proposed scheme uses the Chinese remainder theorem to extend the SSS scheme of [34] to an $SMSS$ that provides the mentioned features. After providing the details of our scheme, it is proved that the proposed scheme provides the required security properties. Finally, the proposed scheme is compared with the related ones in terms of the provided features, the share size, and computational and communication costs. Considering the provided features of the proposed scheme, the comparison results indicate the overall superiority of the proposed scheme.

The rest of this paper is organized as follows: In Section 2, the required preliminaries, including the Chinese remainder theorem, the Birkhoff interpolation method, and the definition of social multi-secret sharing schemes are provided. Afterward, in Section 3, the details of the proposed $SMSS$ scheme are presented and in Section 4 and Section 5, its security and efficiency are analyzed. Finally, in Section 6, the conclusions are provided.

2 Preliminaries

In this section, the required preliminaries, including the Chinese remainder theorem, the Birkhoff inter-

polation method, Tassa's $HTSS$ scheme, and the definition of social multi-secret sharing schemes are provided.

2.1 The Chinese Remainder Theorem

Let $q_1, \ldots, q_n$ be pairwise co-prime integers and $r_1, \ldots, r_n$ be arbitrary integers such that $r_i \in Z_{q_i}$. Then, the system of equations $y \equiv r_i \pmod{q_i}, 1 \leq i \leq n$ has a unique solution for $y \bmod q$, where $q = \prod_{i=1}^{n} q_i$ [36]. The value of y can be computed as $y = \sum_{i=1}^{n} r_i t_i M_i \pmod{q}$ where, $M_i = \frac{q}{q_i}$ and $t_i = M_i^{-1} \pmod{q_i}$.

It should be noted here that although CRT has been widely used in SS schemes [37, 38], we use it for binding the shares, and not for sharing (recovery) process.

2.2 The Birkhoff Interpolation

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

- $X = \{x_1, \ldots, x_k\}$ be a set of points in the set of real numbers such that $x_1 < x_2 < \cdots < x_k$.
- $E = (e_{i,j})_{1 \leq i \leq k, 0 \leq j \leq h}$ be a matrix with binary entries (hereafter, we assume that the last column of E is non-zero), $I(E) = \{(i,j) : e_{i,j} = 1\}$ and $N = |I(E)|$.
- $C = \{c_{i,j} : (i,j) \in I(E)\}$ be a set of N real numbers.

Then, the problem of the Birkhoff interpolation that corresponds to the triplet $\langle X, E, C \rangle$ is to find a polynomial $P(x) \in R_{N-1}[x]$ such that the following N equalities are satisfied:

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

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 the degree at most $N-1$. The matrix E is called the interpolation matrix.

The Birkhoff interpolation problem may not always result in a unique solution. The required conditions for the uniqueness of the solution of the Birkhoff interpolation (over finite groups) are described in [26].

In the following, the Birkhoff interpolation procedure is described.

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 $I'(E) = \{\alpha_i : i = 0, \ldots, N-1\}$ be a vector that is obtained by lexicographically ordering of entries of $I(E)$ (in $I'(E)$ the pair (i,j) proceeds (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 $C' = \{c'_i : i = 0, \ldots, N-1\}$ 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 of E, X, and φ, we can solve the Birkhoff interpolation problem as follows:

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

where,

$$A(E,X,\varphi) = \tag{3}$$
$$\begin{bmatrix} g_0^{(\alpha_0(2))}(x_{\alpha_0(1)}) & g_1^{(\alpha_0(2))}(x_{\alpha_0(1)}) & \cdots & g_{N-1}^{(\alpha_0(2))}(x_{\alpha_0(1)}) \\ g_0^{(\alpha_1(2))}(x_{\alpha_1(1)}) & g_1^{(\alpha_1(2))}(x_{\alpha_1(1)}) & \cdots & g_{N-1}^{(\alpha_1(2))}(x_{\alpha_1(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(\alpha_{N-1}(2))}(x_{\alpha_{N-1}(1)}) & g_1^{(\alpha_{N-1}(2))}(x_{\alpha_{N-1}(1)}) & \cdots & g_{N-1}^{(\alpha_{N-1}(2))}(x_{\alpha_{N-1}(1)}) \end{bmatrix}$$

$|\cdot|$ is the determinant operation and $A(E,X,\varphi_j)$ can be computed by replacing $(j+1)$-th column of matrix of Equation 3 with C'.

By reformulating Equation 2, we have the following equation for the Birkhoff interpolating procedure:

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

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.

2.3 Tassa's HTSS Scheme

Same as the SSS scheme of [34], the proposed $SMSS$ scheme in the next section is based on Tassa's disjunctive $HTSS$ scheme [26]. Therefore, a brief review of Tassa's scheme is provided in this section. Let $U = \{P_1, P_2, \ldots, P_n\}$ be a group of trustees partitioned into m levels $U_1, U_2, \ldots, U_m$. Assume that there is a hierarchy among these levels so that the amount of trust to trustees in U_i is more than that of those in U_j for $i > j$. Suppose there exists a sequence of threshold numbers $t_1, t_2, \ldots, t_m$ that determines the access structure of the scheme. Let q be a properly chosen prime number. Using these notations, the details of Tassa's $HTSS$ scheme are presented in Figure 1.

2.4 Social Multi-Secret Sharing

In $SMSS$ schemes, trust to different trustees is not the same and it can vary over time, based on each trustee's behavior. To simulate this property, in $SMSS$ schemes, more important shares will be assigned to more trusted participants. Moreover, based on the trustees' behavior over time, the importance of their shares can also be increased or decreased. An $SMSS$ scheme can be described by using three protocols: The Sharing (Sha), the Social Tuning (Tun), and the Reconstruction (Rec). Through Sha, the dealer shares a set of secrets among trustees.

The sharing protocol

To share the secret $s \in Z_q$, the dealer :

(1) Choose random values $a_0, \ldots, a_{t_1-2}$ and generates the 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 $GF(q)$.

(2) Compute the share corresponding to each trustee $P_i \in \mathcal{U}$ as $f^{(t_1-t_j)}(i)$ where, j is such that$P_i \in \mathcal{U}_j$ and $f^{(t_1-t_j)}(\cdot)$ is the $(t_1 - t_j)$-th derivative of $f(\cdot)$.

The reconstruction protocol

Let $\{P_{\alpha_0}, P_{\alpha_1}, \ldots, P_{\alpha_{t_j-1}}\}$ be an authorized subset of trustees. Then, using the shares corresponding to the members of this subset, anyone can recover the secret as follows:

(1) Reconstruct $(t_1 - t_j)$-th derivative of $f(\cdot)$, i.e., $f^{(t_1-t_j)}(\cdot)$ by using the Birkhoff interpolation method.

(2) Retrieve the secret as $s = \frac{(t_j-1)!}{(t_1-1)!} s'$ over $GF(q)$ where s' is the last coefficient of $f^{(t_1-t_j)}(\cdot)$.

Figure 1. Tassa's disjunctive HTSS scheme

Then, the dealer leaves the scheme and does not participate in the rest of it. Through *Tun*, which is performed periodically after *Sha*, the trustees can tune the trust to each of them and obtain new shares according to their new trust values. Newcomers are also able to join the scheme through this protocol. Finally, when an authorized subset of trustees decides to reconstruct the last retrievable secret, they use *Rec* and in addition to the recovered secret, they compute their shares from the next retrievable secret.

3 The Proposed Scheme

In this section, a new social multi-secret sharing scheme is proposed. The proposed scheme uses the Chinese remainder theorem to extend the scheme of [34] to an *SMSS*.

Let n be the maximum number of the trustees over time and $S = \{s_1, \ldots, s_r\}$ denotes the set of secrets. Three types of entities are involved in the proposed scheme: 1) the dealer D, 2) the group of shareholders P, and 3) a trusted third party TTP. D generates the shares corresponding to the shareholders and TTP through *Sha* and then leaves the scheme. The trustees can tune their shares according to their behavior using *Tun*. This can neither be done without requiring the participation of D nor TTP. Newcomers can also join the scheme through this protocol. With the help of TTP, authorized subsets can reconstruct the last retrievable secret and also compute their shares from the next secret through *Rec*.

To assign different trust values to trustees, we assume that there exist m trust levels $U_1, \ldots, U_m$. Using this notation, for a trustee to be in the i-th trust level means that it is a member of U_i. Assume that there exists a hierarchy among the trust levels in such a way that there exists more trust in the trustees in the higher levels compared to those in the lower ones. Furthermore, assume a threshold value t_i for each trust level U_i $(i = 1, \ldots, m)$, which indicates the number of the required trustees from this or higher levels to reconstruct a secret. Note that this sequence of the threshold values specifies the access structure of the scheme. To simulate the existing hierarchy among trust levels, we should have $t_i < t_j$ for $1 \leq j < i \leq m$. In addition, to prevent the possibility of the reconstruction of the secrets by only one trustee, we should have $t_m > 1$.

A trust function (such as the one suggested in [39]) is also required for calculating the amount of trust to each trustee at the beginning of each time interval. Let (ξ_1, ξ_2) be the output range of the employed trust function. We divide this range into m equal length subintervals $I_1, \ldots, I_m$ and assign each of these subintervals to a trust level; i.e., if the trust value of a trustee is in the subinterval I_i $(i = 1, \ldots, m)$, then this trustee will be moved to U_i.

Using the above notations, the details of the protocols of the proposed scheme are described in the following sections.

3.1 The Sharing Protocol (Sha)

Through this protocol, the dealer shares the set of secrets among the group of trustees $U = \{P_1, \ldots, P_n\}$. The details of this protocol of our scheme are provided in Figure 2.

3.2 The Social Tuning Protocol (Tun)

This protocol of our scheme is almost the same as that of [34]. It consists of two phases: 1) the adjusting, and 2) the share renewal. The details of these phases of our scheme are provided in Figure 3 and Figure 4.

3.3 The Reconstruction Protocol (Rec)

If some authorized subset of trustees decides to recover a secret, they execute the *Rec* protocol and in addition to recovering the last retrievable secret, compute their shares from the next secret. The details of this protocol are presented in Figure 5.

4 Security Analysis

In this section, we prove that our *SMSS* scheme provides the needed security requirements. It should be noted here that the security of the proposed scheme is

The sharing protocol

On input of the set of the secrets $S = \{s_1, s_2, \ldots, s_r\}$, the dealer:

(1) Chooses n prime numbers $q_1, q_2, \ldots, q_n$ and computes $q = \prod_{i=1}^{n} q_i$. The prime numbers $q_1, q_2, \ldots, q_n$ should be chosen in such a way that the following conditions be satisfied regarding q:
   (a) Computing any prime factor of q be computationally infeasible,
   (b) $q > s_i$ for $i = 1, \ldots, r$, and $q > n$,
   (c) $q > 2^{t_m - t_1 + 2} \cdot (t_1 - t_m - 1)^{(t_1 - t_m - 1)/2} \cdot (t_1 - t_m - 1)! \cdot n^{(t_1 - t_m - 1)(t_1 - t_m - 2)/2}$
   The last condition is employed so that the underlying Birkhoff interpolations that need to be solved in the next protocols of the proposed scheme be well-posed.

(2) Assumes equal trust to all the trustees and puts all of them at the trust level $\mathcal{U}_c$, where $\mathcal{U}_c$ is the trust level corresponding to the subinterval that the initial trust value $\xi_I = \xi_1 + (\xi_2 - \xi_1)/2$ belongs to it.

(3) Sets the value i equal to r.

(4) Selects values $a_{0,i}, a_{1,i}, \ldots, a_{t_1-2,i}$ from Z_q randomly, sets $a_{t_1-1,i} = s_i$ and generates the polynomial:

$$f_i(x) = a_{0,i} + a_{1,i}x + a_{2,i}x^2 + \cdots + a_{t_1-1,i}x^{t_1-1}$$

(5) For $j = 1, \ldots, n$: calculates P_j's share from the secret s_i as $SH_j^i = f_i^{(t_1-t_c)}(x_j)$ over $GF(q)$, where $f_i^{(t_1-t_c)}(\cdot)$ denotes $(t_1 - t_c)$-th derivative of f_i.

(6) Uses the Chinese remainder theorem to compute C_i modulo $q = \prod_{j=1}^{n} q_j$ such that for $j = 1, \ldots, n$: $C_i = SH_j^i \pmod{q_j}$ and if $i > 1$, it computes $v_i = C_i \oplus s_{i-1}$.

(7) Sets i equal to $i - 1$, and returns to Step 4 if $i \geq 1$.

(8) Sends $v_2, v_3, \ldots, v_r$ to TTP and $(SH_1^1, q_1), (SH_2^1, q_2), \ldots, (SH_n^1, q_n)$ to $P_1, P_2, \ldots, P_n$, respectively, via a secure channel.

Figure 2. The sharing protocol of the proposed SMSS scheme

based on the security of Tassa's scheme [26], Zarepoor *et al.*'s scheme [40], and Eslami *et al.*'s scheme [34].

Lemma 1. *In the proposed scheme, unauthorized subsets cannot reconstruct a (non-retrieved) secret by using their shares and the retrieved secrets.*

Proof. To prove this lemma, first, note that the underlying polynomial shared in each time interval is independent of the previously retrieved secrets. Therefore, the knowledge of the previously retrieved secrets provides no advantage to the trustees in an unauthorized subset. Therefore, the only thing that we should prove here is that unauthorized subsets are unable to reconstruct the secret when only one secret is shared by using our scheme (i.e., same as [40]). Assume that t_i participants, for simplicity say $\mathcal{B} = \{P_1, P_2, \ldots, P_{t_k}\}$ co-operate to recover s_i. Each participant can calculate his/her share as $SH_j^i = C_i \pmod{q_j}$ for $j = 1, 2, \ldots, t_k$. Thus $SH_j^i = f_i(x_j)$, where $f_i(x) \in Z_q[x]$ is the secret polynomial corresponding to secret s_i. As $f_i(x)$ is a $t_1 - 1$ degree polynomial, it can be written as Equation 5, where coefficients $A_{0,i}, A_{1,i}, \ldots, A_{t_1-1,i}$ are unknown elements of Z_q.

$$f_i(x) = A_{0,i} + A_{1,i}x + \cdots + A_{t_1-1,i}x^{t_1-1} \quad (5)$$

where:

$$A_{y,i} = \begin{cases} a_{y,i}, & 0 \leq y < t_1 - t_k \\ a_{y,i} + (-1)^{i+l} sh_i^j \left(\frac{|A_i(E,X,\varphi_l)|}{|A(E,X,\varphi)|} \right) \cdot \left(\frac{l!}{(l+t_1-t_k)!} \right), & t_1 - t_k \leq y < t_1 - 1, \\ & 0 \leq l < t_k - 2 \\ (-1)^{i+t_k-1} sh_i^j \left(\frac{\left| A_i\left(E,X,\varphi_{t_k-1}\right) \right|}{|A(E,X,\varphi)|} \right) \cdot \left(\frac{(t_k-1)!}{(t_1-1)!} \right), & y = t_1 - 1 \end{cases} \quad (6)$$

Therefore, each participant in $\mathcal{B}$ can obtain a linear equation with t_i unknowns $A_{0,i}, A_{1,i}, \ldots, A_{t_i-1,i}$; i.e.,

In this phase, the trustees in an authorized subset:

(1) Reevaluate the trust value of each shareholder based on his previous trust value and his behavior in the past period.

(2) Assign the initial trust value ξ_I to each newcomer.

(3) Rearrange the set of participants into subsets $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_m$ according to the newly computed trust values. The rearrangement is done in such a way that if a trustee's new trust value is in the subinterval I_x, then this trustee would be moved to the trust level $\mathcal{U}_x$.

(4) To make sure of the well-posedness of the Birkhoff interpolation problems corresponding to authorized subsets in the future period, update trustees' identities as follows:
   (a) For $j = 1, \ldots, m$:
      (i) For each $P_i \in \mathcal{U}_j$ $(1 \leq i \leq |\mathcal{U}_j|)$: assign the least possible non-zero unallocated number from $GF(q)$ as the new identity of P_i (i.e.,ID_{P_i}).

Figure 3. The adjusting phase of the proposed SMSS scheme

Let $Autsub = \{P_{\alpha_0}, \ldots, P_{\alpha_{t_k-1}}\}$ be an authorized subset of trustees and s_j be the last retrievable secret according to the specified order. Then, to renew each shareholder's share:

(1) Each trustee $P_{\alpha_i} \in Autsub$:

(a) Constructs a polynomial $f_{1\alpha_i}(x) = a_{0\alpha_i} + a_{1\alpha_i}x + a_{2\alpha_i}x^2 + \cdots + a_{(t_1-2)\alpha_i}x^{t_1-2}$ and

$$f_{2\alpha_i}(x) = \sum_{l=0}^{t_k-1} \Big[(-1)^{i+l} sh^j_{\alpha_i} \cdot \Big(\frac{|A_i(E, X, \varphi_l)|}{|A(E, X, \varphi)|} \Big) \cdot \Big(\frac{l!}{(l+t_1-t_k)!} \Big) x^{l+t_1-t_k} \Big]$$

and computes $f_{\alpha_i}(x) = f_{1\alpha_i}(x) + f_{2\alpha_i}(x)$, over $GF(q)$, where $\{a_{x\alpha_i}\}_{x=0}^{t_1-2}$ are random values, E is the interpolation matrix that corresponds to $Autsub$ and their trust levels from the previous time interval.

(b) For each $P_\beta \in \mathcal{U}$:
Computes a part of P_β's new share from the secret s_j as $sh^j_{P_{\alpha_i} \to P_\beta} = f^{(t_1-t_h)}_{\alpha_i}(ID'_\beta)$ over $GF(q)$ and sends it to P_β via a secure channel. Here, h is the index of the trust level to which P_β belongs (based on the calculated trust value in the tuning phase) and ID'_β is the new identity of P_β.

(2) After receiving the subshares from all P_{α_i}, $(0 \le i \le t_k - 1)$, each shareholder $P_\beta \in \mathcal{U}$:
Deletes his share from the previous period and computes his new share from the secret s_j as $(SH^j_\beta = \sum_{i=0}^{t_k-1} sh^j_{P_{\alpha_i} \to P_\beta}, q_\beta)$.

Figure 4. The share renewal phase of the proposed SMSS scheme

they can form the following system of linear equations:

$$\begin{aligned} A_{0,i} + A_{1,i}x_1 + \cdots + A_{t_i-1,i}x_1^{t_i-1} &= SH^i_1 \\ A_{0,i} + A_{1,i}x_2 + \cdots + A_{t_i-1,i}x_2^{t_i-1} &= SH^i_2 \\ \vdots \\ A_{0,i} + A_{1,i}x_{t_i-1} + \cdots + A_{t_i-1,i}x_{t_i-1}^{t_i-1} &= SH^i_{t_i-1} \end{aligned} \quad (7)$$

In the matrix form we have:

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t_i-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t_i-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{t_i} & x_{t_i}^2 & \cdots & x_{t_i}^{t_i-1} \end{pmatrix} \begin{pmatrix} A_{0,i} \\ A_{1,i} \\ \vdots \\ A_{t_i-1,i} \end{pmatrix} = \begin{pmatrix} SH^i_1 \\ SH^i_2 \\ \vdots \\ SH^i_{t_i} \end{pmatrix} \quad (8)$$

Let $Autsub = \{P_{\alpha_0}, P_{\alpha_1}, \ldots, P_{\alpha_{t_k-1}}\}$ be an authorized subset of trustees, and $s_j (j \in \{1, \ldots, r\})$ be the last retrievable secret according to the specified order. To reconstruct s_j,

(1) Each $P_\beta \in Autsub$:

(a) Sends SH^j_β *to* TTP via a secure channel.

(2) *TTP*:

(a) Applies the Birkhoff interpolation on the received shares and reconstructs $(t_1 - t_k)$-th derivative of some polynomial $f_j(\cdot), (i.e., f_j^{(t_1-t_k)}(\cdot))$ over $GF(q)$.

(b) Retrieves the secret s_j by calculating $s_j = \frac{(t_k-1)!}{(t_1-1)!}s'_j$ over $GF(q)$ where s'_j, is the last coefficient of the reconstructed polynomial.

(c) Sends s_j to the trustees in $Autsub$ via a secure channel.

(d) If $j = r$, then the execution of the scheme is terminated. Otherwise, computes $C_{j+1} = v_{j+1} \oplus s_j$, and sends it to all trustees via a secure channel.

(3) Each $P_\beta \in U$:

(a) Computes his share from the new secret s_{j+1} as follows:
$(SH^{j+1}_\beta = C_{j+1} \pmod{q_\beta}, q_\beta)$

(4) Trustees in an authorized subset (according to the initial trust values) tune all trustees' shares by using the share renewal phase of the *Tun* protocol.

Figure 5. The reconstruction protocol of the proposed SMSS scheme

The coefficient matrix, M, is a Vandermonde matrix. There is a well-known formula for the determinant of a $t_i \times t_i$ Vandermonde matrix:

$$det\ M = \prod_{1 \le i \le j < t_i} (x_i - x_j) \pmod{q} \quad (9)$$

As it is assumed that the x_is are distinct, $det\ M \neq 0$, which implies that the system has a unique solution over Z_q and any t_i participants can reconstruct polynomial $f_i(x)$ and obtain s_i. According to the above discussions, suppose $t_i - 1$ or fewer participants pool their secret shares, hence the t_i equations constituting the Vandermonde linear system will contain more than t_i unknown symbols. Therefore, they cannot solve the Vandermonde system, and so it is not possible to obtain the shared secrets and others' secret shares cannot be obtained. This completes the proof. □

Lemma 2. *The share renewal phase of the proposed SMSS scheme is secure.*

Proof. Let *Autsub* be the authorized subset of trustees that run the share renewal phase. To prove this lemma, first, we show that for $s_j (j \in \{1, \ldots, r\})$, unauthorized subsets of players in this phase cannot obtain any information about the old shares of *Autsub*'s members, and then, we prove that unauthorized subsets of players obtain no information about the secret by having access to their shares belonging to different periods.

Let $UnAutsub = \left\{P_{\beta_1}, \ldots, P_{\beta_{t_k-1}}\right\} (1 \leq k \leq m)$ be an unauthorized subset of players in period T_h. In T_h, $sh^j_{P_{\alpha_i} \to P_{\beta_r}} = f^{(t_1-t_l)}_{\alpha_i}\left(ID'_{\beta_r}\right)$, is the subshare that each player $P_{\beta_r} \in UnAutsub$ receives from each player $P_{\alpha_i} \in Autsub$, where $P_{\beta_r} \in U_l$ 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:

$$
\begin{aligned}
f_{\alpha_i}(x) &= f_{1\alpha_i}(x) + f_{2\alpha_i}(x) \\
&= \sum_{v=0}^{t_1-2} a_{v\alpha_i} x^v + \sum_{v=0}^{t_k-1} \Bigg[(-1)^{i+v} sh^j_{\alpha_i} \\
&\quad \cdot \Big(\frac{|A_i(E,X,\varphi_v)|}{|A(E,X,\varphi)|}\Big) \cdot \Big(\frac{v!}{(v+t_1-t_k)!}\Big) x^{v+t_1-t_k}\Bigg] \\
&= \sum_{v=0}^{t_1-t_k-1} a_{v\alpha_i} x^v + \sum_{v=t_1-t_k}^{t_1-2} \Bigg[a_{v\alpha_i} + (-1)^{i+v-t_1+t_k} \\
&\quad sh^j_{\alpha_i} \Big(\frac{|A_i(E,X,\boldsymbol{\varphi}_{v-t_1+t_k})|}{|A(E,X,\varphi)|}\Big) \cdot \\
&\quad \Big(\frac{(v-t_1+t_k)!}{v!}\Big) x^v\Bigg] + \Bigg[(-1)^{i+t_k-1} sh^j_{\alpha_i} \\
&\quad \Big(\frac{|A_i(E,X,\boldsymbol{\varphi}_{t_k-1})|}{|A(E,X,\varphi)|}\Big) \cdot \Big(\frac{(t_k-1)!}{(t_1-1)!}\Big)\Bigg] x^{t_1-1} \\
&= \sum_{v=0}^{t_1-t_k-1} a_{v\alpha_i} x^v + \sum_{v=t_1-t_k}^{t_1-2} \Big[\Big(a_{v\alpha_i} + sh^j_{\alpha_i} b_v\Big) x^v\Big] \\
&\quad + sh^j_{\alpha_i} b_{t_1-1} x^{t_1-1}
\end{aligned}
$$

Where

$$b_v = (-1)^{i+v-t_1+t_k}\Big(\frac{|A_i(E,X,\varphi_{v-t_1+t_k})|}{|A(E,X,\varphi)|}\Big) \cdot \Big(\frac{(v-t_1+t_k)!}{v!}\Big)$$

for $v = (t_1 - t_k), \ldots, (t_1 - 1)$. Denoting $a_{v\alpha_i}$ by c_v for $v = 0, \ldots, (t_1 - t_k - 1)$ and $(a_{v\alpha_i} + sh^j_{\alpha_i} b_v)$ by c_v for $v = (t_1 - t_k), \ldots, (t_1 - 2)$, we have:

$$f_{\alpha_i}(x) = \sum_{v=0}^{t_1-2} c_v x^v + sh^j_{\alpha_i} b_{t_1-1} x^{t_1-1}.$$

Therefore, the procedure that each player follows in the share renewal phase is the same as the sharing of the secret $s_j = sh^j_{\alpha_i} b_{t_1-1}$ using Tassa's secret sharing scheme. The unconditional security of Tassa's scheme makes it impossible to obtain any information on $sh^j_{\alpha_i} b_{t_1-1}$ from the sub-shares belonging to the members of *UnAutsub*. Moreover, $b_{t_1-1} = (-1)^{i+t_k-1}\Big(\frac{|A_i(E,X,\varphi_{t_k-1})|}{|A(E,X,\varphi)|}\Big) \cdot \Big(\frac{(t_k-1)!}{(t_1-1)!}\Big)$ can be computed publicly. Hence, obtaining any information on $sh^j_{\alpha_i}$ from the sub-shares computed by P_{α_i} is equal to obtaining the same information on $sh^j_{\alpha_i} b_{t_1-1}$. As mentioned, the procedure that is done by each member of the authorized subset participating in this phase is equivalent to the situation in which, Tassa's *SS* scheme is used to share the secret $s_j = sh^j_{\alpha_i} b_{t_1-1}$. Therefore, it can be concluded that the partial shares computed by the members of the authorized subset in this phase of our scheme reveal no information about their old shares. The previous lemma also shows that using shares from different periods yields no advantage to the unauthorized subsets. Therefore, it can be concluded that this phase of the proposed scheme is secure. □

Lemma 3. *The proposed SMSS scheme is secure in the passive adversary model.*

Proof. To prove this lemma, we analyze the security of each protocol of the proposed scheme. The security of the Tun relies on the security of the share renewal phase, which proved to be secure in Lemma 2. Therefore, *Tun* is secure.

The set of shares generated at the end of *Sha* for sharing the secrets $s_1, s_2, \ldots, s_r$ is equal to the shares generated by Tassa's *SS* scheme when it is used to share the secret s_1. Using this fact and the unconditional security of Tassa's scheme in the passive adversarial model, we conclude that *Sha* is also secure in the passive adversarial model.

As explained earlier, *Rec* consists of several steps: first, the last recoverable secret (according to the specified order) is reconstructed. Then, the trustees' shares from the next secret are calculated using the auxiliary value corresponding to the next secret, which is at the disposal of *TTP*. Finally, *Tun* is executed to tune trustees' shares according to the current trust to each of them. The first step is exactly the reconstruction protocol of Tassa's scheme when the secret is s_i, where i is the index of the last recoverable secret. Therefore, based on the unconditional security of Tassa's scheme, this step of Rec is secure. The security of the second step is a direct result of the security of calculating trustees' shares in the reconstruction protocol of Zarepoor *et al.*'s scheme [40]. The security of the final step is also proved in Lemma 2. Therefore, it can be concluded that *Rec* is also secure. Based on the security of all protocols of the proposed scheme, it can be concluded that the proposed *SMSS* scheme is secure. □

Lemma 4. *In the proposed scheme, even authorized subsets of trustees cannot reconstruct all the secrets at once.*

Proof. Let *Autsub* be an arbitrary authorized subset of participants at the current period and $s_i, 1 \leq i < r$, be the last retrievable secret. Then, the members of *Autsub* can use their shares and recover s_i. However, to compute their shares from s_{i+1}, they need to know v_{i+1}. Since $v_{i+1} = C_{i+1} \oplus s_i, i > 0$, hence without knowing v_{i+1}, participants are unable to determine C_{i+1} and therefore, they cannot compute their shares from the next secret. Therefore, we can conclude that without the participation of TTP, even authorized subsets of trustees cannot reconstruct any secret besides the last retrievable one. □

Lemma 5. *The secrets can only be reconstructed according to the specified order.*

Proof. Suppose that $i-1$ secrets from the set of secrets are reconstructed according to the specified order (this means that $s_1, s_2, \ldots, s_{i-1}$ are reconstructed). To reconstruct another secret $s_j, i < j \leq r$, the trustees should first obtain their shares from that secret which can only be done through C_j. However, without knowing s_{j-1}, they are unable to obtain C_j and consequently, their shares from s_j. Therefore, without first reconstructing s_{j-1}, it is even impossible even for authorized subsets to obtain their shares from s_j. □

5 Performance Analysis

In this section, the performance of the proposed scheme is analyzed and it is compared with other related schemes. The comparison is done in terms of the computational and communication costs, the share size, and properties provided by the schemes.

5.1 Computational Complexity

To determine the computational complexity, we calculate the number of multiplication operations performed in each protocol of the proposed scheme. According to the details of the proposed scheme, the computational complexity of Tun and *Rec* depends on the size of the authorized subset that performs them. However, the size of the authorized subsets could be equal to $t_1, t_2, \ldots,$ or t_m and therefore, they are not of the same size. To simplify calculations and make comparisons possible, here we consider the worst-case regarding our scheme in which the size of the authorized subset is equal to t_1. We also assume that $t_1 = t$ where t is the threshold parameter used in other schemes.

In *Sha*, first, the dealer needs to compute the derivatives of r polynomials of degree $t-1$ and then he should compute the value of some polynomials of degree at most $t-1$ at n points. The former can be done in $O(rt^2)$ and the latter can be done in $O(rnt)$. Hence, the overall computational complexity of *Sha* is of order $O(t^2 + rnt) \in O(rnt)$.

The share renewal phase is the time-consuming phase of Tun. In this phase, each participating trustee should perform a part of the Birkhoff interpolation procedure by using his old share (Step 1-(a) of shares renewal phase (Figure 4)). Then, he should compute the value of this polynomial (of degree $t-1$) or one of its derivatives at n points (Step 1-(b) of the shares renewal phase (Figure 4)). In the first step, each participating trustee should compute the determinant of $t+1$ matrices of the size $t \times t$. Using the best-known algorithm for determinant computation, this step can be done in order of $O(t^{3.373})$ [41]. It is also obvious that the computational complexity of the second step is of order $O(tn + t^2)$. Therefore, the overall computational complexity of the Tun protocol of our scheme is of order $O(t^{3.373} + tn)$.

Finally, in *Rec*, TTP applies the Birkhoff interpolation method on the shares corresponding to an authorized subset. As we stated earlier, this takes $O(t^{3.373})$ operations. The next step in which, the trustees calculate their shares from the next secret, does not require any multiplication. At the end of this protocol, the participating trustees should execute Tun, which as stated before it can be done in order $O(t^{3.373} + tn)$. Therefore, the overall computational complexity of this protocol is of order $O(t^{3.373} + tn)$.

5.2 Communication Complexity

To analyze the communication complexity of the proposed scheme, we calculate the number of communication rounds required in each of its protocols. In this regard, we only consider the messages sent through secure channels and ignore other messages. In *Sha*, the dealer sends the trustees' share to them and some values to TTP. Therefore, this protocol requires only one communication round. Tun also requires only one communication round (Step 1-(b) of the renewal phase). In *Rec*, at first, the members of an authorized subset send their shares to TTP. Then, TTP reconstructs the secret and sends the secret and another value (an auxiliary value to enable trustees to compute their shares from the next secret) to the trustees. At last, the members of an authorized subset execute Tun so that trustees' shares are tuned according to the current trust to each of them. Therefore, *Rec* requires three communication rounds.

5.3 Share Size

The share size of an SS scheme is the size of the private shares assigned to each of its trustees. In the

Table 1. Comparison of the proposed scheme with the related ones in terms of the communicational and the computational costs

Scheme	*Communication complexity*			*Computational complexity*		
	Sha	*Tun*	*Rec*	*Sha*	*Tun*	*Rec*
[30]	1	3	3	$O(t^2n)$	$O(t^2n)$	$O(t\log t)$
[34]	1	1	1	$O(tn)$	$O(t^{3.373}+tn)$	$O(t^{3.373})$
[35]	1	1	1	$O(t^2)+O(r+nt^2)$	$O(nt^3)$	$O(r+t^2)$
Ours	1	1	3	$O(t^2+trn)\in O(trn)$	$O(t^{3.373}+tn)$	$O(t^{3.373}+tn)$

proposed scheme, trustees' shares consist of two parts: 1) the value of some polynomial at some given point module q and 2) the corresponding module to the Chinese remainder theorem assigned to them. Both of these values are of order q, therefore, the share size of each trustee in the proposed scheme is equal to $2 \mid q \mid$ bits, where $\mid q \mid = \lceil \log_2^q \rceil$.

5.4 Comparisons

In this section, the proposed scheme is compared with the related ones in terms of the computational and communication costs, the share size, and properties provided by the schemes. The results are presented in Table 1 and Table 2. Compared to the schemes of Nojoumian *et al.* [30] and Eslami *et al.* [34], despite the greater communication and computational complexities (Table 1), the proposed scheme can share multiple secrets at one execution. Note that since the schemes of [30] and [34] are not able to share multiple secrets, it is not possible to compare these schemes with the proposed one in terms of 1) being multi-stage or single-stage and 2) being able to reconstruct the secret according to some specified order.

Compared to Pakniat and Eslami's scheme [35], as it can be seen from Table 1, the proposed scheme is more efficient in terms of the share size and the computational costs of *Tun*. However, the scheme of [35] is more efficient in terms of the computational complexity of *Sha* and *Rec*, and communication costs of *Rec*. However, considering, the desirable properties provided by the proposed scheme (i.e., being multi-stage and providing the ability to dictate the order in which the secrets should be retrieved), the overall superiority of the proposed scheme over the only other existing *SMSS* one can be concluded.

6 Conclusion

In this paper, a new social multi-secret sharing (*SMSS*) scheme is proposed and its security is proved. The proposed scheme uses the Chinese remainder theorem to extend the social secret sharing (*SSS*) scheme of [34] to an *SMSS* one. The proposed scheme is the only existing *SMSS* scheme that provides the following desirable features: 1) being multi-stage and 2) being able to dictate the order in which the secrets should be retrieved. Considering these desirable features, the small share size, and the comparable computational and communication complexities of the proposed scheme, the overall superiority of the proposed scheme over the related ones could be concluded. Despite the provided desirable features, the proposed scheme requires a trusted third party to help participants to recover their secrets. This is a drawback that limits the scenarios in which the proposed scheme can be used. Currently, we have no idea about the possibility or impossibility of addressing this limitation and leave it as an open problem for future works.

Table 2. Comparison of the proposed scheme with the related ones in terms of the share size and provided features by each of them (1) Gradual reconstruction of the secrets, (2) Reconstruction according to the specified order, (3) Multi-secret sharing

Scheme	*GRMS* [1]	*Re.a.* [2]	*MSS* [3]	*The share size*
[30]	–	–	*No*	$t \mid q \mid$
[34]	–	–	*No*	$\mid q \mid$
[35]	*No*	*Yes*	*Yes*	$t \mid q \mid$
Ours	*Yes*	*Yes*	*Yes*	$2 \mid q \mid$

References

[1] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[2] George Robert Blakley. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on*, pages 313–313. IEEE Computer Society, 1979.

[3] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, pages 383–395. IEEE, 1985.

[4] Lidong Zhou, Fred B Schneider, and Robbert Van Renesse. Apss: Proactive secret sharing in asynchronous systems. *ACM transactions on information and system security (TISSEC)*, 8(3):259–286, 2005.

[5] David Schultz, Barbara Liskov, and Moses Liskov. Mpss: mobile proactive secret sharing. *ACM Transactions on Information and System Security (TISSEC)*, 13(4):1–32, 2010.

[6] Lein Harn. Efficient sharing (broadcasting) of multiple secrets. *IEE Proceedings-Computers and Digital Techniques*, 142(3):237–240, 1995.

[7] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang. A (t, n) multi-secret sharing

scheme. *Applied Mathematics and Computation*, 151(2):483–490, 2004.

[8] Liao-Jun Pang and Yu-Min Wang. A new (t, n) multi-secret sharing scheme based on shamir's secret sharing. *Applied Mathematics and Computation*, 167(2):840–848, 2005.

[9] Jianjie Zhao, Jianzhong Zhang, and Rong Zhao. A practical verifiable multi-secret sharing scheme. *Computer Standards & Interfaces*, 29(1):138–141, 2007.

[10] Massoud Hadian Dehkordi and Samaneh Mashhadi. An efficient threshold verifiable multi-secret sharing. *Computer Standards & Interfaces*, 30(3):187–190, 2008.

[11] Ziba Eslami and Saideh Kabiri Rad. A new verifiable multi-secret sharing scheme based on bilinear maps. *Wireless Personal Communications*, 63(2):459–467, 2012.

[12] Massoud Hadian Dehkordi and Samaneh Mashhadi. New efficient and practical verifiable multi-secret sharing schemes. *Information Sciences*, 178(9):2262–2274, 2008.

[13] Ali Nakhaei Amroudi, Ali Zaghain, and Mahdi Sajadieh. A verifiable (k, n, m)-threshold multi-secret sharing scheme based on ntru cryptosystem. *Wireless Personal Communications*, 96(1):1393–1405, 2017.

[14] Nasrollah Pakniat, Mahnaz Noroozi, and Ziba Eslami. Reducing multi-secret sharing problem to sharing a single secret based on cellular automata. *The CSI Journal on Computer Science and Engineering*, 14(1), 2017.

[15] Massoud Hadian Dehkordi and Hossein Oraei. How to construct a verifiable multi-secret sharing scheme based on graded encoding schemes. *IET Information Security*, 13(4):343–351, 2019.

[16] Huanping Liu, Yixian Yang, and Fangchun Yang. Multistage secret sharing based on one-way function. *Electronics Letters*, 21(4):561–564, 1999.

[17] Hossein Pilaram and Taraneh Eghlidos. An efficient lattice based multi-stage secret sharing scheme. *IEEE Transactions on Dependable and Secure Computing*, 14(1):2–8, 2015.

[18] Mitra Fatemi, Reza Ghasemi, Taraneh Eghlidos, and Mohammad Reza Aref. Efficient multistage secret sharing scheme using bilinear map. *IET Information Security*, 8(4):224–229, 2014.

[19] Samaneh Mashhadi. New multi-stage secret sharing in the standard model. *Information Processing Letters*, 127:43–48, 2017.

[20] Samaneh Mashhadi, Massoud Hadian Dehkordi, and Niloofar Kiamari. Provably secure verifiable multi-stage secret sharing scheme based on monotone span program. *IET Information Security*, 11(6):326–331, 2017.

[21] Massoud Hadian Dehkordi, Samaneh Mashhadi, and Hossein Oraei. A proactive multi stage secret sharing scheme for any given access structure. *Wireless Personal Communications*, 104(1):491–503, 2019.

[22] Jamal Zarepour-Ahmadabadi, MohammadEbrahim Shiri-Ahmadabadi, and Alimohammad Latif. A cellular automata-based multi-stage secret image sharing scheme. *Multimedia Tools and Applications*, 77(18):24073–24096, 2018.

[23] Samaneh Mashhadi. Computationally secure multiple secret sharing: Models, schemes, and formal security analysis. *The ISC International Journal of Information Security*, 7(2):91–99, 2015.

[24] Amir Herzberg, Stanisław Jarecki, Hugo Krawczyk, and Moti Yung. Proactive secret sharing or: How to cope with perpetual leakage. In *annual international cryptology conference*, pages 339–352. Springer, 1995.

[25] Carles Padró and Germán Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 46(7):2596–2604, 2000.

[26] Tamir Tassa. Hierarchical threshold secret sharing. *Journal of cryptology*, 20(2):237–264, 2007.

[27] Tamir Tassa and Nira Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology*, 22(2):227–258, 2009.

[28] Ziba Eslami, Nasrollah Pakniat, and Mahnaz Noroozi. Hierarchical threshold multi-secret sharing scheme based on birkhoff interpolation and cellular automata. In *2015 18th CSI International Symposium on Computer Architecture and Digital Systems (CADS)*, pages 1–6. IEEE, 2015.

[29] Nasrollah Pakniat, Mahnaz Noroozi, and Ziba Eslami. Distributed key generation protocol with hierarchical threshold access structure. *IET Information Security*, 9(4):248–255, 2015.

[30] Mehrdad Nojoumian, Douglas R Stinson, and Morgan Grainger. Unconditionally secure social secret sharing scheme. *IET information security*, 4(4):202–211, 2010.

[31] Douglas R Stinson and Ruizhong Wei. Unconditionally secure proactive secret sharing scheme with combinatorial structures. In *International Workshop on Selected Areas in Cryptography*, pages 200–214. Springer, 1999.

[32] Mehrdad Nojoumian and Douglas R Stinson. Socio-rational secret sharing as a new direction in rational cryptography. In *International Conference on Decision and Game Theory for Security*, pages 18–37. Springer, 2012.

[33] Mehrdad Nojoumian and Douglas R Stinson. Social secret sharing in cloud computing using a new trust function. In *2012 Tenth Annual International Conference on Privacy, Security*

and Trust, pages 161–167. IEEE, 2012.

[34] Ziba Eslami, Nasrollah Pakniat, and Mehrdad Nojoumian. Ideal social secret sharing using birkhoff interpolation method. *Security and Communication Networks*, 9(18):4973–4982, 2016.

[35] Nasrollah Pakniat and Ziba Eslami. Verifiable social multi-secret sharing secure in active adversarial model. *Journal of Computing and Security*, 4(1):3–12, 2017.

[36] Henri Cohen. *A course in computational algebraic number theory*, volume 8. Springer-Verlag Berlin, 1993.

[37] Lein Harn, Miao Fuyou, and Chin-Chen Chang. Verifiable secret sharing based on the chinese remainder theorem. *Security and Communication Networks*, 7(6):950–957, 2014.

[38] Wei Hua and Xiaofeng Liao. A secret image sharing scheme based on piecewise linear chaotic map and chinese remainder theorem. *Multimedia Tools and Applications*, 76(5):7087–7103, 2017.

[39] Mehrdad Nojoumian and Timothy C Lethbridge. A new approach for the trust calculation in social networks. In *International Conference on E-Business and Telecommunication Networks*, pages 64–77. Springer, 2006.

[40] Jamal Zarepour-Ahmadabadi, MohammadEbrahim Shiri-Ahmadabadi, Ali Miri, and AliMohammad Latif. A new gradual secret sharing scheme with diverse access structure. *Wireless Personal Communications*, 99(3):1329–1344, 2018.

[41] Virginia Vassilevska Williams. Multiplying matrices faster than coppersmith-winograd. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 887–898, 2012.

Mohammad Ebrahim Ebrahimi Kiasari is a Ph.D. student in Applied Mathematics at the Islamic Azad University of Khorramabad Branch. He received his master's degree in Applied Mathematics in 2010 from the Islamic Azad University of Ghaemshahr Branch. In addition to teaching university math courses, he has authored articles in the field of numerical analysis and cryptography.

Nasrollah Pakniat received his Ph.D. in 2015 from Shahid Beheshti University. He received his M.Sc. degree in Computer Science from Shahid Beheshti University in 2011. He holds a B.Sc. degree in Computer Science from the Shahid Bahonar University of Kerman in 2008. He continued his scientific experience in 2016 as a faculty member of the Iranian Research Institute for Information Science and Technology (IranDoc). He is an assistant professor in the Information Science Research Department of IranDoc. His research interests include cryptography, network security, and text mining.

Abdolrasoul Mirghadri received the B.Sc., M.Sc. and Ph.D. degrees in Mathematical Statistics, from the faculty of Science, Shiraz University in 1986, 1989 and 2001, respectively. He is an associate professor at the faculty and research center of communication and information technology, Imam Hossein University, Tehran, Iran since 1989. His research interest includes Cryptography, Statistics and Stochastic Processes. He is a member of the ISC scientific society.

Mojtaba Nazari received his Ph.D. degree in Applied Mathematics from UTM University of Malaysia in 2015. He received his master's and bachelor's degrees in Applied Mathematics in 1997 and 1999 from Shahid Chamran University of Ahvaz and Ferdowsi university of Mashhad. He is an associate professor at the faculty of Basic Science, Islamic Azad University of Khorramabad Branch, Iran since 2000. His research interest includes Numerical Analysis, Differential Equation and Fluid Mechanics.