Wireless Pers Commun (2016) 90:93–107
DOI 10.1007/s11277-016-3332-7

# How to Fairly Share Multiple Secrets Stage by Stage

**Samaneh Mashhadi**[1]

Published online: 28 April 2016


**Abstract** A multi-stage secret sharing scheme (MSSS) allows a dealer to share multiple secrets among a set of participants, in such a way that any authorized subset of participants can reconstruct the secrets stage-by-stage. In this paper, for the first time we propose an efficient MSSS based on the non-homogeneous linear feedback shift register (NHLFSR). According to the properties of NHLFSRs, this scheme has few public information, a new simple distribution, and various techniques for the reconstruction phase.

**Keywords** Cryptography · Threshold scheme · Multi-secret sharing scheme · Multi-stage secret sharing scheme · Non-homogenous linear recursion

## 1 Introduction

A *secret sharing scheme* (SSS) is a protocol for the distribution of a secret $P$ among a set of $n$ participants $\mathcal{M} = \{M_1, \ldots, M_n\}$ according to some access structures $\Gamma \subseteq 2^{\mathcal{M}}$ such that any authorized subset of the participants can reconstruct the secret value by putting their shares together, but any unauthorized subset of them cannot get any information about the secret $P$ [1–5].

### 1.1 Background

*Multi-secret sharing scheme* (MSS) is a generalization of SSS. In a MSS, multiple secrets are distributed among the participants during a secret sharing process. Two categories of MSS according to the secret reconstruction have been proposed, the *multi-stage secret*

✉ Samaneh Mashhadi
smashhadi@iust.ac.ir

[1] Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran 16846 13114, Iran

*sharing scheme* (MSSS) and the *general multi-secret sharing scheme* (GMSS); and depending on any specific situation, each category may be preferable. In a GMSS, all of the secrets are reconstructed simultaneously in one stage [6–10], while, in a MSSS, the secrets have different levels of importance, and any authorized subset of the participants can recover only one secret in each stage [11–15]. In the literature, there are two different types of MSSSs. In the first type (MSSST1), the secret reconstruction can be executed in any order, e.g. the schemes [12–14]. In the second type (MSSST2), the secret reconstruction must be executed in the dealer's predefined order, e.g. [11, 15].

### 1.2 Motivation

Most of the earlier proposed MSSs (GMSSs and MSSSs) are simple modification of the SSS of Shamir [4]. In fact, in either of these MSSs, the dealer employs polynomials in order to distribute the secrets, and the authorized participants should use the Lagrange interpolation formula to recover them. In 2008, for the first time, we employed *linear feedback shift registers* (LFSRs) instead of polynomials in GMSSs [9, 16]. These GMSSs have many advantages due to characteristics of LFSRs.

### 1.3 Contribution

In this paper, we employ the LFSRs in order to suggest a practical MSSST2. Compared to the previous MSSSs, our scheme has fewer public values, and its construction is simpler. Moreover, it allows more than one methods for the reconstruction of secrets. The security of this scheme is based on the security of Shamir's SSS as well as on the properties of LFSR and two-variable one-way function. Besides, the shared secrets can be reused after any unsuccessful recovery phase.

### 1.4 Organization

The reminder of this paper is organized as follows. Section 2 contains some preliminaries. The proposed MSSST2 is presented in Sect. 3, and its security is analyzed in Sect. 4. Finally, we give some comparative results and conclusions in Sects. 5 and 6, respectively.

## 2 Preliminary

In this section we will introduce some fundamental background of our scheme.

### 2.1 Access Structure

**Definition 1** Given a set of participants $\mathcal{M} = \{M_1, M_2, \ldots, M_n\}$, a monotone access structure $\Gamma$ on $\mathcal{M}$ is a set of non-empty subsets of participants which is closed under upward-inclusion

$$(A \in \Gamma, A \subseteq B \subseteq \mathcal{M}) \Rightarrow B \in \Gamma.$$

The sets in $\Gamma$ are called the authorized sets, and the sets not in $\Gamma$ are called the unauthorized sets.

### 2.2 Multi-stage Secret Sharing Schemes

In a MSSST2 the dealer want to share $k$ secrets $P_1, \ldots, P_k$, according to $k$ access structures $\Gamma_1, \ldots, \Gamma_k$, respectively (such that $\Gamma_i \subseteq \Gamma_{i-1}$, for $i = 2, \ldots, k$). The secrets are reconstructed stage-by-stage in special order $P_1, P_2, \ldots, P_k$. In the following, we will propose the definition of a MSSST2.

**Definition 2** The second type of multi-stage secret sharing scheme is a tuple of $\Omega = (\mathsf{Stp}, \mathsf{Dist}, \mathsf{Rec})$ such that:

- The setup algorithm $\mathsf{Stp}$ takes as input the set of participants $\mathcal{M}$ and $k$ different levels of access structures $\Gamma_1, \ldots, \Gamma_k$, such that $\Gamma_i \subseteq \Gamma_{i+1}$, for $i = 1, \ldots, k-1$, and outputs some public and common parameters $\mathsf{pms}$ for the scheme; $\mathsf{pms} \leftarrow \mathsf{Stp}(\mathcal{M}, \{\Gamma_j\}_{1 \le j \le k})$.
- The distribution algorithm $\mathsf{Dist}$ takes as input $\mathsf{pms}$ and the secret $\mathbf{P} = (P_1, \ldots, P_k)$ to be shared, and generate the set of secret shares $\{s_i\}_{M_i \in \mathcal{M}}$ and possibly some pubic output $\mathsf{out}_{\mathsf{pub}}$; $(\{s_i\}_{M_i \in \mathcal{M}}, \mathsf{out}_{\mathsf{pub}}) \leftarrow \mathsf{Dist}(\mathsf{pms}, \mathbf{P})$.
- The reconstruction algorithm $\mathsf{Rec}$ takes as input $\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}$, the index $j = 1$, and the shares $\{s_i\}_{M_i \in A_j}$ of the participants in some subset $A_j \subset \mathcal{M}$, and outputs a possible value $P_1'$ for the first secret in the first stage:

$$P_1' := \mathsf{Rec}(\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}, 1, \{s_i\}_{M_i \in A_j}).$$

  Then the algorithm takes as input $\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}$, an index $j \in \{2, \ldots, k\}$, a possible value $P_{j-1}'$ for the $(j-1)-$th secret, and the shares $\{s_i\}_{M_i \in A_j}$ of the participants in some subset $A_j \subset \mathcal{M}$, and outputs a possible value $P_j'$ for the $j-$th secret in $j-$th stage:

$$P_j' := \mathsf{Rec}(\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}, j, P_{j-1}', \{s_i\}_{M_i \in A_j}).$$

For correctness, we require that for any subset $A \in \Gamma_1$,

$$P_1 := \mathsf{Rec}(\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}, 1, \{s_i\}_{M_i \in A}),$$

and for any index $j \in \{2, \ldots, k\}$ and any subset $A \in \Gamma_j$,

$$P_j = \mathsf{Rec}(\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}, j, P_{j-1}, \{s_i\}_{M_i \in A}).$$

### 2.3 Non-homogenous Linear Feedback Shift Register

In this section mathematical background of new scheme are given. A detailed description of the non-homogeneous linear feedback shift register (NHLFSR) can be found in [16–18].

**Definition 3** A non-homogeneous linear feedback shift register of degree $t-1$ is defined by the equations

$$[\mathsf{NHLFSR}] \qquad \begin{cases} u_0 = c_0, u_1 = c_1, \ldots, u_{t-2} = c_{t-2}, \\ u_{i+t-1} + a_1 u_{i+t-2} + \cdots + a_{t-1} u_i = f(i) \quad (i \ge 0), \end{cases}$$

where $c_0, c_1, \ldots, c_{t-2}$ and $a_1, a_2, \ldots, a_{t-1}$ are constants.

Thus, we have the following Corollary.

**Corollary 1** *Each term $u_i$ of a sequence $(u_i)$ defined by NHLFSR, depends on the previous $t-1$ terms, the coefficient $\{a_i\}_{i=1}^{t-1}$, and function $f(i)$. So, if we know the coefficient*

$\{a_i\}_{i=1}^{t-1}$, $f(i)$ *and* $t-1$ *arbitrary successive terms* $u_m, u_{m+1}, \ldots, u_{m+t-2}$ $(m \geq 0)$ *of the sequence, then we can compute each forward term* $u_j, j \geq m+t-1$, *by repeating the following process*:

$$u_{i+t-1} = f(i) - \sum_{l=2}^{t} a_{l-1} u_{i+t-l} \qquad i \geq m.$$

*Similarly, we can compute each previous term* $u_j$, $0 \leq j < m$, *by repeating the following process*:

$$u_i = a_{t-1}^{-1} \left( f(i) - u_{i+t-1} - \sum_{l=2}^{t-1} a_{l-1} u_{i+t-l} \right) \qquad i \leq m-1.$$

*Example 1* Suppose that the sequence $(u_i)$ is defined by the following NHLFSR

$$\begin{cases} u_0 = c_0, u_1 = c_1, \ldots, u_{t-2} = c_{t-2}, \\ \sum\limits_{j=1}^{t} \binom{t-1}{j-1} (-1)^j u_{i+t-j} = c, \quad i \geq 0, \end{cases}$$

where $c$ is a random integer and $\binom{t}{j} = \frac{t!}{j!(t-j)!}$. Suppose that we know the coefficients $\left\{ \binom{t-1}{j-1} (-1)^j \right\}_{j=1}^{t}$ and $t$ arbitrary successive terms $u_m, u_{m+1}, \ldots, u_{m+t-1}$ of the sequence $(u_i)$, but we don't have $c$. We can determine $c$ from the following equation:

$$\sum_{j=1}^{t} \binom{t-1}{j-1} (-1)^j u_{m+t-j} = c.$$

Then we can determine each forward term, by using the following process:

$$u_{i+t-1} = -c + \sum_{l=2}^{t} \binom{t-1}{l-1} (-1)^l u_{i+t-l} \qquad i > m.$$

Similarly, each previous term, can be easily determined by using the following process:

$$u_i = (-1)^t c + \sum_{j=1}^{t-1} \binom{t-1}{j-1} (-1)^{t+j} u_{i+t-j} \qquad i < m.$$

For example, let

$$\begin{cases} u_0 = 1, u_1 = 2, \\ \sum\limits_{j=1}^{3} \binom{2}{j-1} (-1)^j u_{i+3-j} = -3, \quad i \geq 0. \end{cases}$$

Thus

$$u_{i+2} = 3 - u_i + 2u_{i+1}, \qquad \forall i \geq 0.$$

Therefore the sequence $(u_i)_{i\geq 0} = \{1, 2, 6, 13, 23, 36, 52, \ldots\}$. Suppose that we know the coefficients and 3 arbitrary successive terms $u_4 = 23, u_5 = 36, u_6 = 52$ of the sequence $(u_i)$, but we don't have $c = -3$. We can determine $c$ from the following equation:

$$2u_5 - u_4 - u_6 = c.$$

Then we can determine each forward term, by using the following process:

$$u_{i+2} = 3 - u_i + 2u_{i+1}, \qquad i > 4.$$

Similarly, each previous term, can be easily determined by using the following process:

$$u_i = 3 - u_{i+2} + 2u_{i+1}, \qquad i < 4.$$

Every NHLFSR corresponds with an individual formula which gives its term explicitly. There is no general formula. The following Lemma, proved in [18], provides an explicit formula for calculating the terms of NHLFSR given in Example 1. Since there are various NHLFSR, we are able to design various secret sharing schemes through a similar algorithm.

**Lemma 2** *Suppose that the sequence $(u_i)$ is defined by the NHLFSR given in Example 1. Then we have*

$$u_i = p(i), \quad i \geq 0,$$

*where $p(x)$ is a polynomial of degree $t-1$ , i.e.,*

$$p(x) = B_0 + B_1 x + \cdots + B_{t-1}x^{t-1}.$$

Lemma 2 tells us that the public term of the sequence $(u_i)$, is defined by $p(x)$. Hence, if we know $t$ arbitrary terms of $(u_i)$, then we can construct the polynomial $p(x)$, and consequently, we can compute each term $u_i$ for $i \geq 0$. So, we have the following corollary.

**Corollary 3** *Suppose that the sequence $(u_i)$ is defined by the NHLFSR given in Example 1, and we know $t$ arbitrary terms $u_{m_1}, u_{m_2}, \ldots, u_{m_t}$ of $(u_i)$. Then we can use one of the following methods to compute the coefficients of $p(x)$ and consequently any term $u_i$ for $i \geq 0$.*

1. *Solve the Vandermonde system*

$$\begin{bmatrix} 1 & m_1 & m_1^2 & \cdots & m_1^{t-1} \\ 1 & m_2 & m_2^2 & \cdots & m_2^{t-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & m_t & m_t^2 & \cdots & m_t^{t-1} \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ \vdots \\ B_{t-1} \end{bmatrix} = \begin{bmatrix} u_{m_1} \\ u_{m_2} \\ \vdots \\ u_{m_t} \end{bmatrix}$$

*and compute $B_0, B_1, \ldots, B_{t-1}$ and consequently the public term*

$$u_i = p(i) = B_0 + B_1 i + \cdots + B_{t-1} i^{t-1}.$$

2. *Consider $t$ pairs $\{(m_i, u_{m_i})\}_{i=1}^{t}$ and use Lagrange interpolation as follows:*

$$p(x) = \sum_{i=1}^{t} u_{m_i} \prod_{j=1, j\neq i}^{t} \frac{x - m_j}{m_i - m_j} = B_0 + B_1 x + \cdots + B_{t-1} x^{t-1}.$$

*Then compute*

$$u_i = p(i) \quad i \geq 0.$$

Following the previous example, suppose that we know 3 arbitrary terms $u_1 = 2, u_4 = 23, u_6 = 52$ of $(u_i)$ is defined by

$$\begin{cases} u_0 = 1, u_1 = 2, \\ \sum_{j=1}^{3} \binom{2}{j-1} (-1)^j u_{i+3-j} = -3, \quad i \geq 0. \end{cases}$$

We can use one of the following methods to propose a clear formula for the terms of $(u_i)$.

1. Solve the Vandermonde system

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 4 & 16 \\ 1 & 6 & 36 \end{bmatrix} \begin{bmatrix} B_0 \\ B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} 2 \\ 23 \\ 52 \end{bmatrix}$$

and compute $B_0 = 1, B_1 = \frac{-1}{2}, B_2 = \frac{3}{2}$ and consequently the public term

$$u_i = p(i) = 1 - \frac{1}{2} i + \frac{3}{2} i^2.$$

2. Consider $t$ pairs $\{(1,2), (4,23), (6,52)\}$ and use Lagrange interpolation as follows:

$$p(x) = 2\frac{(x-4)(x-6)}{(1-4)(1-6)} + 23\frac{(x-1)(x-6)}{(4-1)(4-6)} + 52\frac{(x-1)(x-4)}{(6-1)(6-4)} = 1 - \frac{1}{2}x + \frac{3}{2}x^2$$

Thus

$$u_i = p(i) = 1 - \frac{1}{2} i + \frac{3}{2} i^2.$$

## 3 The New Scheme

In this section we propose a novel MSSST2 based on NHLFSR given in Example 1. Since there are various NHLFSR, we are able to design various secret sharing schemes through a similar algorithm. For simplicity, we consider the case where all the access structures are threshold ones. That is, $\Gamma_j = \{A \subseteq P \mid \ |A| \geq t_j\}$.

### 3.1 Stp

Let $\mathcal{M} = \{M_1, M_2, \ldots, M_n\}$ be a set of $n$ participants. A dealer D wants to share $k$ secrets $P_1, \ldots, P_k$ among the participants of $\mathcal{M}$ in such a way that

- Secrets are reconstructed in the dealer's predefined order $P_1, P_2, \ldots, P_k$,
- Any $t_j$ or more participants can recover the secret $P_j$,
- No $t_j - 1$ participants can obtain any information about the secret $P_j$.

Let $1 \le t_1 \le t_2 \le \cdots \le t_k \le n$ (because $\Gamma_i \subseteq \Gamma_{i-1}$, for $i = 2, \ldots, k$). D chooses a prime number $q > P_i$ for $i = 2, \ldots, k$. Also D selects an one-way function $f(r, s) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_q$ and $n$ shares $s_1, \ldots, s_n$, such that $s_i \in \mathbb{Z}$. Then D distributes $s_i$ to participant $M_i$ by a secure channel $(i = 1, 2, \ldots, n)$.

### 3.2 Dist

The dealer performs the following steps:

1. Randomly select two integer $r, c_1$; such that $r \ne P_j, 1 \le j \le k$,
2. Consider NHLFSR which is defined by the equations,

$$[*]\begin{cases} u_{1,0} = P_1, u_{1,1} = f(r, s_1), \ldots, u_{1,t_1-2} = f(r, s_{t_1-2}), \\ \sum_{\lambda=1}^{t_1} \binom{t_1-1}{\lambda-1}(-1)^{\lambda} u_{1,l+t_1-\lambda} = c_1 \bmod q \quad (l \ge 0), \end{cases}$$

3. Compute $r_{1,i} = u_{1,i} - f(r, s_i)$, for $t_1 - 1 \le i \le n$;
4. For $j = 2, 3, \ldots, k$, execute the following steps:

- Consider the following NHLFSR which is defined by the equations,

$$[**]\begin{cases} u_{j,0} = P_j, u_{j,1} = f(P_{j-1}, s_1), \ldots, u_{j,t_j-2} = f(P_{j-1}, s_{t_j-2}), \\ \sum_{\lambda=1}^{t_j} \binom{t_j-1}{\lambda-1}(-1)^{\lambda} u_{j,l+t_j-\lambda} = c_j \bmod q \quad (l \ge 0), \end{cases}$$

- Compute $r_{j,i} = u_{j,i} - f(P_{j-1}, s_i)$, for $t_j - 1 \le i \le n$;

5. Publish all $r, r_{j,i}$ for $1 \le j \le k$, $t_j - 1 \le i \le n$.

### 3.3 Rec

In our scheme, at least $t_j$ participants should provide the secret shadows $f(r, s_i)$ or $f(P_{j-1}, s_i)$ to reconstruct the secret $P_j$ in the $j$th stage of reconstruction.

#### *3.3.1* $\mathsf{Rec}(\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}, 1, \{s_i\}_{M_i \in A_1})$

Here, two different cases for the recovery phase of $P_1$ are discussed according to the indices of the participants, and in each case, various techniques for the recovery phase are proposed.

*Arbitrary participants*: Suppose $t_1$ arbitrary participants $A_1 = \{M_i\}_{i \in I}$ $(I \subseteq \{1, 2, \ldots, n\})$ cooperate to recover the secret $P_1$. They should pool their secret shadows $\{f(r, s_i)\}_{i \in I}$ and compute $t_1$ terms of $[*]$ by their shadows in the following way:

$$u_{1,i} = \begin{cases} f(r, s_i), & \text{if} \quad 1 \le i \le t_1 - 2; \\ f(r, s_i) + r_{1,i}, & \text{if} \quad t_1 - 1 \le i \le n. \end{cases}$$

Now, according to the Corollary 3, they can use one of the following methods to compute $P_1$:

1. In the first method, they must solve the Vandermond system

$$\begin{bmatrix} 1 & i_1 & i_1^2 & \cdots & i_1^{t_1-1} \\ 1 & i_2 & i_2^2 & \cdots & i_2^{t_1-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & i_{t_1} & i_{t_1}^2 & \cdots & i_{t_1}^{t_1-1} \end{bmatrix} \begin{bmatrix} B_{1,0} \\ B_{1,1} \\ \vdots \\ B_{1,t_1-1} \end{bmatrix} = \begin{bmatrix} u_{1,i_1} \\ u_{1,i_2} \\ \vdots \\ u_{1,i_{t_1}} \end{bmatrix},$$

where $I = \{i_1, i_2, \ldots, i_{t_1}\}$, compute $B_{1,0}, B_{1,1}, \ldots, B_{1,t_1-1}$, and consequently compute the public term $u_{1,i}$ of $[*]$ through the following formula:

$$u_{1,i} = p_1(i) = B_{1,0} + B_{1,1} i + \cdots + B_{1,t_1-1} i^{t_1-1} \bmod q, \quad i \ge 0. \tag{1}$$

Thus,

$$\begin{aligned} P_1 = &\quad u_{1,0}, \quad \text{by}[*], \\ &= p_1(0), \quad \text{by Eq. (1)}, \\ &= B_{1,0} \bmod q, \quad \text{by Eq. (1)}. \end{aligned}$$

Therefore, they can compute the secret $P_1$ only by computing $B_{1,0}$.

2. In the second method, they use $t_1$ pairs $\{(i, u_{1,i})\}_{i \in I}$ to reconstruct the secret $P_1$ through the Lagrange interpolation formula:

$$P_1 = p_1(0) = \sum_{i \in I} u_{1,i} \prod_{j \in I, j \ne i} \frac{j}{j - i} \bmod q.$$

*Participants with successive personal indentification numbers*: Suppose $t_1$ participants $A_1 = \{M_i, M_{i+1}, \ldots, M_{i+t_1-1}\}$, $(1 \le i \le n - t_1 + 1)$ cooperate to recover the secret $P_1$. This case is a particular state of the previous case. Beside the two previous methods, we now explain another technique for the recovery phase in this case. At first, they must compute $t_1$ successive terms $u_{1,i}$ of $[*]$ by their shadows in the following way:

$$u_{1,i} = \begin{cases} f(r, s_i), & \text{if} \quad 1 \le i \le t_1 - 2; \\ f(r, s_i) + r_{1,i}, & \text{if} \quad t_1 - 1 \le i \le n. \end{cases}$$

Now, according to Example 1, they can compute $c_1$ from the following equation:

$$\sum_{\lambda=1}^{t_1} \binom{t_1 - 1}{\lambda - 1} (-1)^{\lambda} u_{1,i+t_1-\lambda} = c_1 \bmod q.$$

Then they can compute $u_{1,i-1}, u_{1,i-2}, \ldots, u_{1,0} = P_1$, successively from the following equation:

$$u_{1,\kappa} = (-1)^{t_1} c + \sum_{j=1}^{t_1-1} \binom{t_1 - 1}{j - 1} (-1)^{t_1+j} u_{1,\kappa+t_1-j} \bmod q \qquad \kappa < i.$$

### 3.3.2 $\mathsf{Rec}(\mathsf{pms}, \mathsf{out}_{\mathsf{pub}}, j, P_{j-1}, \{s_i\}_{M_i \in A_j})$

Suppose $t_j$ participants $A_j$ with the knowledge of the secret $P_{j-1}$ want to reconstruct the secret $P_j$ in the $j$th stage ($j \in \{2, \ldots, k\}$). Similarly, according to the properties of NHLFSR, we discuss two different case for the recovery phase of $P_j$.

*Arbitrary participants*: Suppose $t_j$ arbitrary participants $A_j = \{M_i\}_{i \in I}$ ($I \subseteq \{1, 2, \ldots, n\}$) cooperate to recover the secret $P_j$ in the $j$th stage. They should pool their secret shares $f(P_{j-1}, s_i)$ for $i \in I$ and compute $t_j$ terms $u_{j,i}$ of $[**]$ by the following methods:

$$u_{j,i} = \begin{cases} f(P_{j-1}, s_i), & \text{if} \quad 1 \le i \le t_j - 2; \\ f(P_{j-1}, s_i) + r_{j,i}, & \text{if} \quad t_j - 1 \le i \le n. \end{cases}$$

Now, according to Corollary 3 they can use one of the following methods to compute $P_j$:

1. Solve the Vandermond system

$$\begin{bmatrix} 1 & i_1 & i_1^2 & \cdots & i_1^{t_j-1} \\ 1 & i_2 & i_2^2 & \cdots & i_2^{t_j-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & i_{t_j} & i_{t_j}^2 & \cdots & i_{t_j}^{t_j-1} \end{bmatrix} \begin{bmatrix} B_{j,0} \\ B_{j,1} \\ \vdots \\ B_{j,t_j-1} \end{bmatrix} = \begin{bmatrix} u_{j,i_1} \\ u_{j,i_2} \\ \vdots \\ u_{j,t_j} \end{bmatrix},$$

where $I = \{i_1, i_2, \ldots, i_{t_j}\}$, compute $P_j = B_{j,0}$, because the public term $u_{j,i}$ of $[**]$ is

$$u_{j,i} = p_j(i) = B_{j,0} + B_{j,1} i + \cdots + B_{j,t_j-1} i^{t_j-1} \bmod q, \tag{2}$$

and so

$$\begin{aligned} P_j &= u_{j,0}, \quad \text{by } [**], \\ &= p_j(0), \quad \text{by Eq.(2)}, \\ &= B_{j,0} \bmod q, \quad \text{by Eq. (2)}. \end{aligned}$$

Thus, they can compute the secret $P_j$ by computing $B_{j,0}$.

2. Use $t_j$ pairs $\{(i, u_{j,i})\}_{i \in I}$ to reconstruct the secret $P_j$ through the following formula:

$$P_j = p_j(0) = \sum_{i \in I} u_{j,i} \prod_{l \in I, l \ne i} \frac{l}{l - i} \bmod q,$$

*Participants with successive personal indentification numbers:* Suppose $t_j$ participants $A_1 = \{M_i, M_{i+1}, \ldots, M_{i+t_j-1}\}$, $(1 \le i \le n - t_j + 1)$, cooperate to recover the shared secrets. Beside the two previous methods, we now explain another technique for the recovery of $P_j$. They provide the shares $f(P_{j-1}, s_i)$ for $i \in I$ and compute $t_j$ successive terms $u_{j,i}$ of [**] by the following methods:

$$u_{j,i} = \begin{cases} f(P_{j-1}, s_i), & \text{if} \quad 1 \le i \le t_j - 2; \\ f(P_{j-1}, s_i) + r_{j,i}, & \text{if} \quad t_j - 1 \le i \le n. \end{cases}$$

Now, according to Example 1, they can compute $c_j$ from the following equation:

$$\sum_{\lambda=1}^{t_j} \binom{t_j - 1}{\lambda - 1} (-1)^{\lambda} u_{j,i+t_j-\lambda} = c_j \bmod q.$$

Then they can compute $u_{j,i-1}, u_{j,i-2}, \ldots, u_{j,0} = P_j$, successively from the following equation:

$$u_{j,\kappa} = (-1)^{t_j} c_j + \sum_{\lambda=1}^{t_j-1} \binom{t_j - 1}{\lambda - 1} (-1)^{t_j+\lambda} u_{j,\kappa+t_j-\lambda} \bmod q \qquad \kappa < i.$$

### 3.4 Verification Phase

There are many works in the literatures to investigate the problem of cheater detection and identification for SSSs [3, 5–9, 16, 18]. These models can be employed in our proposed MSSST2 directly.

## 4 Security Analysis

In this section we analyze of some possible attacks. The security of this scheme is based on the security of Shamir's SS [4] as well as on the properties of NHLFSR and two-variable one-way function.

### 4.1 Attack

Suppose that $t_j - 1$ or fewer participants want to recover the secret $P_j$.

#### *4.1.1 Analysis*

The recovery phase of each secret $P_j$ is based on one of the following ways:

1. Solving a Vandermond linear system,
2. Using the Lagrange interpolation polynomial,
3. Using NHLFSR of degree $t_j - 1$.

In the first method, suppose $t_j - 1$ or fewer participants pool their secret shares, hence the $t_j$ equations constituting the Vandermond linear system will contain more than $t_j$ unknown symbols. Therefore, they cannot solve Vandermond system, and so it is not possible to obtain the shared secrets and others' secret shares can not be obtained. In the second method, they can obtain $t_j - 1$ or fewer pairs $(i, u_i)$ of the polynomial $p_j(x)$ of degree $t_j - 1$. The number of obtained pairs is less than $t$, and they have no way to specify $p_j(x)$ and can derive nothing about the shared secrets and others' secret shares. In the third method, each term $u_{j,i}$ of NHLFSR depends on the previous $t_j - 1$ terms and constant $c_j$. Thus, If $m$ participants $\{M_i, M_{i+1}, \ldots, M_{i+m-1}\}$, where $1 \le i \le n + 1 - m$ and $1 \le m < t_j$ pool their secret shares, they can not reveal $c_j$ and any previous term $u_j$ for $j < i - 1$ or any forward term $u_j$ for $j > i + m - 2$ by using NHLFSR. Therefore, the shared secrets and others' secret shares can not be obtained in this way.

**Table 1** Comparison of the number of public values

| Scheme | Chang [11], He [14] | Harn [13] | Li [15] | Fatemi [12] | Proposed scheme |
|---|---|---|---|---|---|
| Number of public values | $kn$ | $k(n-t_1)$ | $k(n-t_1+1)$ | $(2k-1)n$ | $\leq k(n-t_1+2)$ |

### 4.2 Attack

Suppose that a participant $M_i$ try to reveal another's share $s_a$ , where $1 \leq a \leq n$, $a \neq i$.

#### *4.2.1 Analysis*

Each participant $M_a$ just pools his shadow $f(r, s_a)$ or $f(P_{l-1}, s_a)$ in the reconstruction phase. According to characteristics of the two variable one-way function, it is impossible to obtain the true share $s_a$ from $f(r, s_a)$ or $f(P_{l-1}, s_a)$.

### 4.3 Attack

$t_j$ participant may try to disintegrate the order by the dealer's determination to reconstruct the secrets.

#### *4.3.1 Analysis*

We see that, in the recovery phase of each secret $P_j$ , each participant $M_i$ should first provide shadow $f(P_{j-1}, s_i)$. Thus, they should reconstruct the secret $P_{j-1}$ firstly. So, secrets should be reconstructed in the dealer's preassigned order.

### 4.4 Attack

A participant $M_i$ may try to reveal another's shadow $f(P_l, s_j)$ that is not published, from the revealed shadows $f(P_{l-1}, s_j)$ or $f(r, s_j)$, where $1 \leq j \leq n$, and $j \neq i$.

#### *4.4.1 Analysis*

According to characteristics of two-variable one-way functions, it become difficult to compute the secret shadow $f(P_l, s_j)$ from the revealed shadows $f(P_{l-1}, s_j)$ or $f(r, s_j)$.

## 5 Discussions

In this section, some important properties of the new scheme is discussed.

### 5.1 Multi-use Scheme

In this scheme the security of the share $s_i$ is based on the properties of the two-variable one-way function $f(r, s)$. To reconstruct each secret $P_j$ , at least $t_j$ participants $\{M_i\}_{i \in I}$ must provide their shadows $f(r, s_i)$ or $f(P_{j-1}, s_i)$ for $i \in I$. Analysis of Attack 4.2 tell us that, the

**Table 2** Computational complexity

| Scheme | Chang [11], He [14] | Harn [13] | Li [15] | Proposed scheme |
|---|---|---|---|---|
| Dist | $2n(t_k-1)T_m+nT_f$ | $2n(n-1)T_m+nT_f$ | $(2n(n-t_k+1)+n^2)T_m+nT_f+nT_i$ | $(n-t_k+1)(t_k-1)T_m+nT_f$ |
| Rec | $(t_k-1)^2T_m+(t_k-1)T_i+t_kT_f$ | $(n-1)^2T_m+(n-1)T_i+t_kT_f$ | $n^2T_m+nT_i+t_kT_f$ | $(t_k-1)^2T_m+(t_k-1)T_i+t_kT_f$ methods 1,2<br>$(t_k-1)^2T_m++t_kT_f$ method 3 |

**Table 3** Performance

| Scheme | Chang [11], Fatemi, [12], He [14] | Harn [13] | Li [15] | Proposed scheme |
|---|---|---|---|---|
| Dist | $(t_k - 1)$ Degree polynomial | $(n - 1)$ Degree polynomial | $n$ Degree polynomial | NHLFSR |
| Rec | Lagrange interpolation $(t_k - 1)$ | Lagrange interpolation $(n - 1)$ | Lagrange interpolation $n$ | NHLFSR or Lagrange interpolation $(t_k - 1)$ |

share $s_i$ of each participant $M_i$ will never be disclosed in the reconstruction phase of secrets $P_1, P_2, \ldots, P_k$ and reuse of it is secure. Hence, this scheme is a multi-use scheme.

### 5.2 Multi-stage Scheme

According to the analysis of Attack 4.1 at least $t_j$ participant must pool in the reconstruction of each secret $P_j$. Thus this scheme is a threshold MSS. Analysis of Attack 4.3 tell us that it is computationally impossible to recover the secret $P_j$, without any knowledge of $P_{j-1}$. So, the secrets need to be constructed in the special order, $P_1, P_2, \ldots, P_k$. Thus this scheme is a MSSST2.

### 5.3 Public Values

From Table 1 it is easy to see that Fatemi's scheme [12] requires the most and Harn's scheme [13] requires the least public information. Li et al's [15] and new proposed scheme, become more attractive, especially when the threshold $t_1$ is very close to the number of participants $n$.

### 5.4 Computational Complexity

In this section, considering computational complexity, we compare proposed MSSST2 with MSSSs proposed in [11–15] and summarize the result in Tables 2 and 3. For convenience, the following notations are used to analyze the computational complexity.

- $T_f$ the time for one one-way function computation.
- $T_m$ the time for one modular multiplication computation.
- $T_i$ the time for one inverse computation.

*Construction phase* All of the previous MSSSs [11–15], are obtained by running $k$ parallel instances of (a simple modification of) Shamir's SSS [4]. In other words, the dealer employs polynomials to distribute secrets. However, we use NHLFSR to have a simple construction phase (Tables 2,3).

*Recovery phase* The recovery phase of the previous MSSSs [11–15], can be considered as a generalization of the recovery phase of Shamir SS. In other words, in all of the previous schemes, the secrets are reconstructed by using the Lagrange interpolation polynomial. While, our scheme has various methods for the recovery phase: Vandermond linear system, Lagrange interpolation, and NHLFSR. In Harn and Li schemes [13, 15], participants must reconstruct $n$ or $(n - 1)$th degree polynomials, whereas in [11, 12, 14] and in the first method of new scheme, the secrets are recovered only by reconstructing

**Table 4** Basic comparisons among recommended schemes

| Property | He [14] | Harn [13] | Chang [11] | Li [15] | Proposed scheme |
|---|---|---|---|---|---|
| Category of MSS | MSSST1 | MSSST1 | MSSST2 | MSSST2 | MSSST2 |
| Many secrets are shared | Yes | Yes | Yes | Yes | Yes |
| Participants can recover only one secret in every stage | Yes | Yes | Yes | Yes | Yes |
| The secret reconstruction must be executed in a predefined order | No | No | Yes | Yes | Yes |
| The shadow is reusable when shared secrets are reconstructed | No | No | Yes | Yes | Yes |
| Only one shadow is kept by each participant | Yes | Yes | Yes | Yes | Yes |
| The size of each shadow is as short as that each shared secret | Yes | Yes | Yes | Yes | Yes |
| Reconstruction of secrets at earlier stage does not weaken | | | | | |
| the secrecy of the remaining secrets | No | No | Yes | Yes | Yes |
| At least $t_j$ participant must cooperate in the reconstruction of each secret | Yes | Yes | Yes | Yes | Yes |
| Have new simple distribution phase | No | No | No | No | Yes |
| Have different methods for reconstruction phase | No | No | No | No | Yes |

$(t_k - 1)$ degree polynomials. Especially, in particular cases, we can use NHLFSR to reconstruct secrets which is easier and faster (Tables 2,3).

## 6 Conclusions

An efficient, computationally secure multi-stage secret sharing scheme based on the mathematical concept non-homogeneous linear feedback shift register is proposed in this paper. It provide great capabilities for many practical applications. This scheme has easy construction phase and different ways for the reconstruction phase. Our analysis shows that it is a computationally secure and efficient scheme. Also this scheme has few public values and less computing time. Each participant shares many secrets with other participants by holding only one shadow. The shadows are as short as the shared secrets. They do not need to be changed when the shared secrets are recovered. Table 4 lists the comparisons among the recommended schemes.

## References

1. Iftene, S. (2007). General secret sharing based on the chinese remaindertheorem with applications in e-voting. *Electronic Notes inTheoretical Computer Science*, *186*, 6784.
2. Hsu, C.-F., & Harn, L. (2014). Multipartite secret sharing based on CRT. *Wireless Personal Communications*, *78*, 271–282.
3. Schoenmakers, B. (2011). Encyclopedia of cryptography and security. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Verifiable secret sharing* (pp. 1357–1358). Heidelberg: Springer.

4. Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*, 612–613.
5. Wu, T.-Y., & Tseng, Y.-M. (2011). A pairing-based publicly verifiable secret sharing scheme. *Journal of Systems Science and Complexity*, *24*, 186–194.
6. Dehkordi, M. H., & Mashhadi, S. (2008). An efficient threshold verifiable multi-secret sharing. *Computer Standards and Interfaces*, *30*, 187–190.
7. Eslami, Z., & Kabiri Rad, S. (2012). A new verifiable multi-secret sharing scheme based on bilinear maps. *Wireless Personal Communications*, *63*, 45946.
8. Lin, C., & Harn, L. (2012). Unconditionally secure verifiable secret sharing scheme. *Advances in Information Sciences and Service Sciences*, *4*, 514–518.
9. Hadian, M., & Mashhadi, S. (2008). New efficient and practical verifiable multi-secret sharing schemes. *Information Sciences*, *178*, 2262–2274.
10. Mashhadi, S. (2015). Computationally-secure multiple secret sharing: Models schemes, and formal security analysis. *The ISC International Journal of Information Security*, *7*, 91–99.
11. Chang, T.-Y., Hwang, M.-S., & Yang, W.-P. (2005). A new multi-stage secret sharing scheme using one-way function. *ACM SIGOPS Operating Systems*, *39*, 48–55.
12. Fatemi, M., Eghlidos, T., & Aref, M. R. (2009). A multi-stage secret sharing scheme using all-or-nothing transform approach. *LNCS*, *5927*, 449–458.
13. Harn, L. (1995). Comment multistage secret sharing based on one-way function. *Electronics Letters*, *31*, 262.
14. He, J., & Dawson, E. (1994). Multistage secret sharing based on one-way function. *Electronics Letters*, *30*, 1591–1592.
15. Li, H.-X., Cheng, C.-T., & Pang, L.-J. (2005). An impoved multi-stage $(t, n)$-threshold secret sharing scheme. *LNCS*, *3739*, 267–274.
16. Hadian, M., & Mashhadi, S. (2008). Verifiable secret sharing schemes based on non-homogeneous linear recursions and elliptic curves. *Computer Communications*, *31*, 1777–1784.
17. Biggs, N. L. (1989). *Discrete mathematics* (Revised ed.). New York: Oxford University Press.
18. Mashhadi, S., & Hadian, M. (2015). Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LFSR public-key cryptosystem. *Information Sciences*, *294*, 31–40.

**Samaneh Mashhadi** received the B.Sc. and M.Sc. degrees with honors in Mathematics from Iran University of Science and Technology (IUST), and Amirkabir University of Technology (AUT) in 2003 and 2005, respectively. She received her Ph.D. with honors in Mathematics (Cryptography) in 2008 from IUST. She is currently an Assistant Professor in Department of Mathematics of IUST. Her research interests include the analysis, design, and application of digital signatures, secret sharing schemes, and security protocols etc.