Wireless Personal Communications (2019) 104:491–503
https://doi.org/10.1007/s11277-018-6032-7

A Proactive Multi Stage Secret Sharing Scheme for Any Given Access Structure

Massoud Hadian Dehkordi[1] · **Samaneh Mashhadi**[1] · **Hossein Oraei**[1]

Published online: 19 October 2018

Abstract
In proactive secret sharing schemes, the secret shares are periodically renewed without modifying the secret such that an adversary is unable to get any information about the secret shares unless he is able to obtain a certain number of secret shares in a short time interval. In this paper, using monotone span programs (MSP) we devise a new linear multi-secret sharing (LMSS) scheme which is also multi-stage. We also give a new general method to construct proactive and multi-use linear multi-secret sharing schemes based on MSP. An important advantage of our method compared to the others is that it does not need private channels between each pair of participants or an encryption scheme between them. Finally, we prove that our new scheme satisfies the definition of a perfect LMSS scheme.

Keywords Monotone span program · Perfect multi-secret sharing scheme · Access structure · Multi-use scheme · Multi-stage scheme

Mathematics Subject Classification 94A60

1 Introduction

In a multi-secret sharing (MSS) scheme, several secrets are distributed between a group of participants by a dealer D such that only authorized sets can reconstruct the secrets by combining their shares (or their pseudo shares), while other subsets cannot know any information about them [4]. For sharing the secrets, there are many techniques such as multilinear maps [17, 18], polynomial interpolation [11, 19], using the Chinese remainder theorem [1, 9], monotone span program (MSP) [2], and so on. The notion of MSP which will be described later, was introduced by Karchmer and Wigderson [8]. In a MSS scheme based

✉ Massoud Hadian Dehkordi
mhadian@iust.ac.ir

Samaneh Mashhadi
smashhadi@iust.ac.ir

Hossein Oraei
hossein_oraei@mathdep.iust.ac.ir

[1] Cryptography and Data Security Laboratory, School of Mathematics, Iran University of Science and Technology, Narmak, Tehran 1684613114, Iran

on MSP, the secrets are taken from a finite field, and each participant's share is obtained by computing a linear combination of some random numbers and the secrets [6, 10]. In the reconstruction phase, all participants of an authorized set compute a linear combination of their shares.

1.1 Background

So, in a Linear multi-secret sharing (LMSS) scheme several secrets are shared among a set of participants in a linear way. This schemes are widely utilized in information distribution area and has been increasingly considered as an important area of research in cryptography for the last 2 decades [6, 7, 10, 12, 23].

1.2 Related Work

In a proactive secret sharing scheme, the secret shares are periodically renewed without modifying the secret such that an adversary which is called mobile adversary is unable to get any information about the secret shares unless he is able to obtain a certain number of secret shares in a short time interval. Proactive secret sharing (PSS) was first introduced by Ostrovsky and Yung in [16]. This concept have been studied intensively in the literature [5, 12–15, 20]. Herzberg et al. [5] proposed a PSS scheme which has mechanisms to detect corrupted shares. In [20], Stinson et al. produced a PSS scheme which is unconditionally secure. They considered an adversary that can corrupt up to a certain number of the participants including the dealer.

In [13], the authors investigated the security of proactive secret sharing schemes. They showed vulnerability of some previous PSS schemes against their attacks. They also pointed out that their presented attacks can be generalized for MSP based PSS schemes [14, 15]. Moreover, they provided necessary and sufficient conditions for making these schemes secure against the generalized attacks. For example, the PSS scheme presented in [12] is proved to be secure against these attacks.

1.3 Motivation

The PSS schemes mentioned above (that is [5, 13–15, 20]), consider either private channels between each pair of participants or an encryption scheme between them. More precisely, in the share renewal phase of these schemes, some communications must be done via private channels or such as the scheme presented in [5], the messages of some communications are encrypted. However, there exist many situations in which this methods are not accessible to the participants or have high expense. In these cases, a PSS scheme without private channels or encrypted messages in its share renewal phase is required.

Also, in [10], Liu et al. proposed a method for providing the share of each participant that be reusable when the secrets are reconstructed. We found that their proposed method has some security weakness. For example, their method does not work for an authorized set consist of only two participants.

Using MSP, there are also linear secret sharing schemes based on graphs which do not work for any given access structure [7, 22].

1.4 Contribution

In this paper, using MSP we propose a new proactive linear multi-secret sharing scheme which does not need private channels between each pair of participants. As far as we know, this scheme is the first MSP based PSS scheme which in its share renewal phase, new share of each participant constructs in a public manner without using encryption schemes. Our scheme also has the following advantages:

- The scheme is multi-stage. That is, the secrets are reconstructed stage by stage in a predetermined order.
- The scheme is multi-use. That is, the share of each participant is reusable when secrets are reconstructed.

We also mention that unlike the graph based scheme [7, 22], our scheme works for any given access structure.

1.5 Organization

The paper is organized as follows. Section 2, describes the required tools. The proposed MSSS scheme is presented in Sect. 3, and in Sect. 4, we describe how this scheme can be made multi-use and proactive. The security proofs and some comparative results are detailed in Sect. 5. Finally in Sect. 6, we conclude the paper.

2 Preliminaries

Here, we summarize some preliminary concepts about secret sharing schemes.

2.1 Secret Sharing Schemes

Definition 1 Suppose that $\mathcal{P} = \{P_1, \ldots, P_m\}$ be a set of participants. Then, a monotone access structure Γ on $\mathcal{P}$ is a set of non-empty subsets of participants which satisfies the monotone ascending property

$$(A \in \Gamma, A \subseteq A' \subseteq \mathcal{P}) \Rightarrow A' \in \Gamma.$$

The sets in Γ and $\mathcal{A} = 2^{\mathcal{P}} \backslash \Gamma$ are called authorized sets and unauthorized sets respectively, where $2^{\mathcal{P}}$ denotes the power set of $\mathcal{P}$. The set $\mathcal{A}$ that we call adversary structure, satisfies the monotone descending property

$$(B \in \mathcal{A}, B' \subseteq B \subseteq \mathcal{P}) \Rightarrow B' \in \mathcal{A}.$$

We denote by $\Gamma_{\min}$ the minimal elements in Γ and by $\mathcal{A}_{\max}$ the maximal elements in $\mathcal{A}$. That is,

$$\Gamma_{\min} = \{A \in \Gamma \mid \forall A' \subsetneqq A \Rightarrow A' \notin \Gamma\},$$

and

$$\mathcal{A}_{\max} = \{B \in \mathcal{A} \mid \forall B \subsetneqq B' \Rightarrow B' \notin \mathcal{A}\}.$$

Definition 2 For any adversary structure $\mathcal{A}$ over $\mathcal{P}$, its dual is defined as

$$\widetilde{\mathcal{A}} = \{B \subseteq \mathcal{P} \mid B^c \notin \mathcal{A}\}.$$

2.1.1 Monotone Span Program and LMSS Schemes

In 1993, Wigderson and Karchmer introduced the concept of MSP which is a model of computation as follows [8]:

Definition 3 A MSP over a set $\mathcal{P}$ is a triple $(\mathbb{F}, M, \Psi)$, in which $\mathbb{F}$ is a finite field, M is a $l \times d$ distribution matrix with entries in $\mathbb{F}$ and $\Psi : \{1, 2, \ldots, d\} \to \mathcal{P}$ is a function.

In the above definition, Ψ is a surjective function that distributes to each participant of $\mathcal{P} = \{P_1, \ldots, P_m\}$ some rows of M.

Definition 4 Suppose that Γ be an access structure for which $\mathcal{A} \subseteq \widetilde{\mathcal{A}}$. A monotone span program $(\mathbb{F}, M, \Psi)$ is called a MSP for Γ with respect to a target vector $\vec{v} \in \mathbb{F}^d \backslash \{(0, \ldots, 0)\}$, if for all $A \subseteq \{P_1, \ldots, P_m\}$ the following conditions is satisfied.

- if $A \in \Gamma$, then $\vec{v} \in span\{M_A\}$.
- if $A \in \mathcal{A}$, then there exists a sweeping vector $\vec{k} = (k_1, k_2, \ldots, k_d)^T \in \mathbb{F}^d$ such that $M_A \vec{k} = \vec{0} \in \mathbb{F}^{n_1}$ with $k_1 = 1$.

where M_A is the matrix M restricted to the rows i with $\Psi(i) \in A$, with the notation $\vec{v} \in span\{M_A\}$ we mean that there is a vector $\overrightarrow{w_A} \in \mathbb{F}^{n_1}$ for which $\vec{v} = \overrightarrow{w_A} M_A$ and n_1 is the number of participants in A.

Similar to the case of one target vector, we say that $(\mathbb{F}, M, \Psi)$ is a MSP for access structures $\Gamma_j, 1 \leq j \leq n$ with respect to some target vectors $\vec{v}_j \in \mathbb{F}^d \backslash \{(0, \ldots, 0)\}$, if it is true that for each $1 \leq j \leq n$, $\vec{v}_j \in span\{M_A\}$ iff $A \in \Gamma_j$, where $\vec{v}_j \in span\{M_A\}$ means that there is $\overrightarrow{w_{jA}}$ for which $\vec{v}_j = \overrightarrow{w_{jA}} M_A$.

It is proved that constructing a MSP $(\mathbb{F}, M, \Psi)$ for access structures Γ_j is equivalent to devising a linear multi-secret sharing (LMSS) scheme for $\Gamma_j, 1 \leq j \leq n$ [21]. Also, $(\mathbb{F}, M, \Psi)$ is a MSP for access structures Γ_j, $1 \leq j \leq n$ iff there exists a (target) vector $\vec{v}_j \in \bigcap_{A \in (\Gamma_j)_{\min}} \sum_{\Psi(i) \in A} V_i \backslash \bigcup_{B \in (\mathcal{A}_j)_{\max}} \sum_{\Psi(i) \in B} V_i$, in which V_i is the space spanned by the row vectors of M distributed to player $\Psi(i)$ and $\vec{v}_j$ can be considered as the above target vectors.

According to the above discussion, we consider the target vector $\vec{v}_j$ to be an d-rowed vector whose jth component is 1 and other components are $0, 1 \leq j \leq n$. Now, we describe how a LMSS scheme which realizes access structure $\Gamma_j, 1 \leq j \leq n$ can be constructed using any MSP $(\mathbb{F}, M, \Psi)$:

- *Distribution step* Suppose the dealer D has secrets $s_1, s_2, \ldots, s_n$. Then, he can construct a distribution vector $\vec{r} = (s_1, s_2, \ldots, s_n, r_{n+1}, \ldots, r_d)^T$ in which $r_{n+1}, \ldots, r_d$ are random elements in $\mathbb{F}$. Next, he computes $\vec{z} = M\vec{r} = (z_1, z_2, \ldots, z_l)^T$ and gives z_i to the participant $P_{\Psi(i)}$.
- *Reconstruction step* In the following, suppose that the notation $\overrightarrow{z_A}$ be the vector $\vec{z}$ restricted to the indices in A. For each authorized set $A \in \Gamma_j$, there is a vector $\overrightarrow{w_{jA}}$ for which $\vec{v}_j = \overrightarrow{w_{jA}} M_A$. So

$$\overrightarrow{w_{jA}} \cdot \overrightarrow{z_A} = \overrightarrow{w_{jA}} \cdot (M_A \vec{r}) = (\overrightarrow{w_{jA}} \cdot M_A)\vec{r} = \vec{v_j} \cdot \vec{r} = s_j \quad (1)$$

that is, the secret s_j can be reconstructed by computing a linear computation of the shares of participants in A.

Definition 5 We say that a secret sharing scheme is perfect if the participants of an unauthorized set pool their shares together, they obtain nothing about the secret.

3 The New LMSS Scheme Based on MSP

In this section, we first propose a new LMSS scheme based on MSP which realizes any given access structure. Then, we give a simple strategy for making the scheme to be a multi-stage LMSS scheme. In the next section, we give several improvements of the scheme by adding additional options to it.

3.1 The LMSS Scheme

As mentioned in the previous section, constructing an LMSS scheme with respect to $\Gamma_{\min}$ is equivalent to building an MSP $\mathcal{M}(\mathbb{F}, M, \Psi)$ by finding linear spaces V_j, $1 \le j \le m$ such that $\bigcap_{A \in \Gamma_{\min}} \sum_{\Psi(j) \in A} V_j \setminus \bigcup_{B \in \mathcal{A}_{\max}} \sum_{\Psi(j) \in B} V_j \neq \emptyset$. Any vector in this nonempty set can be the target vector $\vec{v_i}$, $1 \le i \le n$. Based on this fact, we build a new LMSS scheme as follows.

3.1.1 The Setup Phase

Let $P = \{P_1, \ldots, P_m\}$ be the set of participants and $\Gamma_{\min} = \{A_1, \ldots, A_k\}$ be an access structure over P in which $|A_j| = t_j$, where $1 \le j \le k$ and $|X|$ denotes the number of members of X. Let also the secret s_i to be shared is chosen in S_i, $1 \le i \le n$). We supposed that $S_1 = \ldots = S_n = \mathbb{F}$ be a finite field with the characteristic $char(\mathbb{F}) = 2$ (for example $\mathbb{F} = \mathbb{Z}_2$). For larger secret domain, we can share the secret bit by bit independently. It is obvious that the scheme works still efficiently by doing parallel processing. More generally, we can use a field $\frac{\mathbb{Z}_2}{<f(x)>}$ which has characteristic equal to 2, where $f(x)$ is an irreducible polynomial over $\mathbb{Z}_2$.

We construct an undirected graph $G(V, E)$ with the vertex set V where $|V| = t' = 1 + \sum_{i=1}^{k} t_i - (k-1) + n$ and edge set $E = E_1 \cup E_2 \cup \ldots \cup E_k \cup \{d_1, \ldots, d_n\}$ from a given access structure $\Gamma_{\min} = \{A_1, \ldots, A_k\}$ as follows (see Fig. 1). In the following scheme, all the vectors and their sums are in the vector space $(\mathbb{Z}_2)^{t-1}$ where $t = 1 + \sum_{i=1}^{k} t_i - (k-1) + 1$:

1. For each authorized set $A_j = \{P_{j1}, \ldots, P_{jt_j}\} \in \Gamma_{\min}$, $1 \le j \le k$, draw a path $v_0 - v_{j1} - v_{j2} - \cdots - v_{jt_j-1} - v$ of length t_j from a fixed vertex v_0 to a fixed vertex v. Then, for each secret s_i, draw an edge from v to a final vertex v_i, $1 \le i \le n$.
2. Suppose $f_j : A_j \longrightarrow E_j$, $1 \le j \le k$, is a bijection which associates each participant in A_j with an edge. More precisely we have:

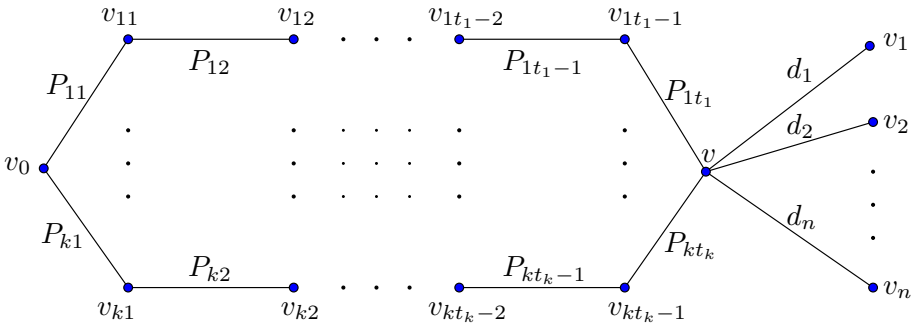

Fig. 1 Schematic representation of the setup phase

$$\begin{aligned} f_j(P_{j1}) &= v_0 v_{j1}, \\ f_j(P_{ji}) &= v_{ji-1} v_{ji}, \text{ where } 2 \le i \le t_j - 1 \text{ and} \\ f_j(P_{jt_j}) &= v_{jt_j-1} v. \end{aligned}$$

Let also d_i be the final edges $vv_i, 1 \le i \le n$. We associate the dealer with this edges.

3. Suppose that $\overrightarrow{e_0} = (0, \ldots, 0) \in (\mathbb{Z}_2)^{t-1}$ and $\overrightarrow{e_h} \in (\mathbb{Z}_2)^{t-1}$. Associate each vertex of the graph with a $(t-1)$-dimensional vector $\overrightarrow{e_h}$ by a map $g : V \longrightarrow (\mathbb{Z}_2)^{t-1}$ such that $\overrightarrow{g(v_0)} = \overrightarrow{e_0}$ and for each $1 \le i \le n$,

$$g(V) \setminus \bigcup_{\substack{j=0 \\ j \neq i}}^{n} \{\overrightarrow{g(v_j)}\}$$

be linearly independent vectors of vector space $(\mathbb{Z}_2)^{t-1}$ (If the number of secrets to be shared is too many, we can set $t = t'$ in order to satisfy the above condition). This condition is needed in the proof of the Proposition 1. Note that in our scheme $\overrightarrow{g(v_i)}$, $1 \le i \le n$, are target vectors.

4. For any $1 \le i \le t_j$, associate each participant $P_{ji} \in A_j$ with the $(t-1)$-dimensional vector $\overrightarrow{u_{ji}}$ of $(\mathbb{Z}_2)^{t-1}$ as follows:

$$\begin{aligned} \overrightarrow{u_{j1}} &= \overrightarrow{g(v_0)} + \overrightarrow{g(v_{j1})}, \\ \overrightarrow{u_{ji}} &= \overrightarrow{g(v_{ji-1})} + \overrightarrow{g(v_{ji})}, \text{ where } 2 \le i \le t_j - 1 \text{ and} \\ \overrightarrow{u_{jt_j}} &= \overrightarrow{g(v_{jt_j-1})} + \overrightarrow{g(v)}. \end{aligned}$$

we associate each participant $\mathcal{P}$ which is not in any A_j, $1 \le j \le k$, with the $(t-1)$ -dimensional vector $\overrightarrow{e_0} = (0, \ldots, 0)$. Let also $\overrightarrow{u_{d_i}}, 1 \le i \le n$, be the $(t-1)$-dimensional vectors of $(\mathbb{Z}_2)^{t-1}$ which are associated with the dealer as follows:

$$\overrightarrow{u_{d_i}} = \overrightarrow{g(v)} + \overrightarrow{g(v_i)}.$$

Example 1 Let $n = 3$, $P = \{P_1, \ldots, P_6\}$ and $\Gamma_{\min} = \{\{P_3, P_6\}, \{P_3, P_4, P_5\}, \{P_1, P_4, P_6\}\}$. For simplicity suppose that we associate each vertex with the vectors $\overrightarrow{e_i}$ of standard basis of

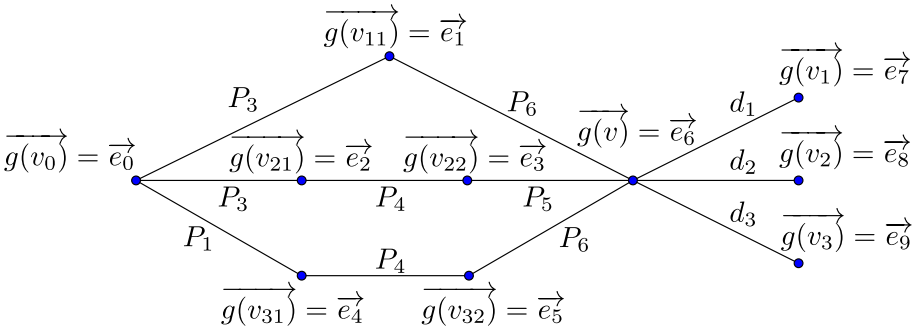

Fig. 2 The illustration of Example 1

$(\mathbb{Z}_2)^7, 1 \le i \le 7, \overrightarrow{e_8} = \overrightarrow{e_7} + \overrightarrow{e_1}$ and $\overrightarrow{e_9} = \overrightarrow{e_7} + \overrightarrow{e_2}$ as shown in Fig. 2. Note that for $i \in \{1, 2, 3\}$, the vectors of $g(V) \setminus \bigcup_{j=0, j\neq i}^{3} \{\overrightarrow{g(v_j)}\}$ are linearly independent. It is easy to see that $\overrightarrow{u_{11}} = \overrightarrow{e_0} + \overrightarrow{e_1}$, $\overrightarrow{u_{12}} = \overrightarrow{e_1} + \overrightarrow{e_6}$, $\overrightarrow{u_{21}} = \overrightarrow{e_0} + \overrightarrow{e_2}$, $\overrightarrow{u_{22}} = \overrightarrow{e_2} + \overrightarrow{e_3}$, $\overrightarrow{u_{23}} = \overrightarrow{e_3} + \overrightarrow{e_6}$, $\overrightarrow{u_{31}} = \overrightarrow{e_0} + \overrightarrow{e_4}$, $\overrightarrow{u_{32}} = \overrightarrow{e_4} + \overrightarrow{e_5}$, $\overrightarrow{u_{33}} = \overrightarrow{e_5} + \overrightarrow{e_6}$, $\overrightarrow{u_{d_1}} = \overrightarrow{e_6} + \overrightarrow{e_7}$, $\overrightarrow{u_{d_2}} = \overrightarrow{e_6} + \overrightarrow{e_8}$, $\overrightarrow{u_{d_3}} = \overrightarrow{e_6} + \overrightarrow{e_9}$. Here we have $\overrightarrow{u_{P_2}} = \overrightarrow{e_0}$ because P_2 is not in any authorized set.

In fact, step 4 are done by the function Ψ of the MSP $\mathcal{M}(\mathbb{Z}_2, M, \Psi)$ in our scheme. Here, there are $l = \sum_{j=1}^{k} t_j$ participants in all authorized set which we show them by $\mathcal{P}_j, 1 \le j \le l$ (if some participants are in more than one authorized set, then they associate with more than one vector). Thus, the matrix M has $l + n$ rows in which the last n of them are $\overrightarrow{u_{d_i}}$, $1 \le i \le n$ and so we have $\Psi(j) = \mathcal{P}_j$, $1 \le j \le l$ and $\Psi(i) = D$, $l + 1 \le i \le l + n$, where D denotes the dealer.

3.1.2 The Distribution Phase

Firstly, the dealer D selects a vector $\vec{r}^T \in (\mathbb{Z}_2)^{t-1}$ uniformly at random such that $< \overrightarrow{g(v_i)}, \vec{r} >= s_i$, $1 \le i \le n$ where T is the transpose and $<\ ,\ >$ shows the inner product. Then D computes $M\vec{r}$ and secretly transmits $\overrightarrow{M_j}\vec{r}$ to player $\mathcal{P}_j$, where $\overrightarrow{M_j}$ denotes the matrix M restricted to the row j with $\Psi(j) = \mathcal{P}_j$. Thus, the share of each player $\mathcal{P}_j$ is $\overrightarrow{M_j}\vec{r}^T, 1 \le j \le l$. Then the dealer publicly broadcasts his shares $\overrightarrow{M_i}\vec{r}^T, l + 1 \le i \le l + n$.

3.1.3 The Reconstruction Phase

As we will show, $\overrightarrow{g(v_i)} \in \bigcap_{A_j \in \Gamma_{\min}} \sum_{\Psi(j') \in A_j} V_{j'} \setminus \bigcup_{B_j \in \mathcal{A}_{\max}} \sum_{\Psi(j') \in B_j} V_{j'}$, $1 \le i \le n$, where the dealer is added to any authorized set A_j. Here we have $V_{j'} = span\{\overrightarrow{M_{j'}}\}$ is the space spanned by the row vectors of M distributed to $\Psi(j')$, $1 \le j' \le l + n$. In other word, only those subsets of participants can reconstruct the secret s_i in which their edges form a path from the vertex v_o to v_i in Fig. 1. Thus, we must add the dealer to each authorized set A_j. More precisely, we also need the share $\overrightarrow{M_{i'}}\vec{r}^T$ for reconstruction of the secret s_i where $1 \le i \le n$ and $i' = i + l$.

We are now in a position to describe the reconstruction phase: For any $A_j \in \Gamma_{\min}$, $1 \le j \le k$, since $\overrightarrow{g(v_i)} \in \sum_{j' \in A_j} V_{j'}$, $1 \le i \le n$, there exist a vector $\vec{w}$ such that $\overrightarrow{g(v_i)} = \vec{w} M_{A_j}$.

Thus $\vec{w}(M_{A_j}\vec{r}^T) = (\vec{w}M_{A_j})\vec{r}^T = \overrightarrow{g(v_i)} \cdot \vec{r}^T = (\overrightarrow{g(v_i)}, \vec{r}) = s_i$. In other words, the participants in authorized set A_j can reconstruct the secret s_i by using a linear combination of their shares.

As the computations of Example 1 of [10], the participants of any authorized set can compute the vector $\vec{w}$ without knowing the row $\overrightarrow{M_j}$ of M associated to participant $\mathcal{P}_j$ of authorized set. We use this fact in the next section to make the scheme multi-use and proactive.

3.2 The Multi-stage Scheme

We make the above scheme multi-stage to ensure n secrets s_i be reconstructed in the special order as $s_1, s_2, \ldots, s_n$. For this, it is enough that the dealer broadcasts his shares as follows:

$$\overrightarrow{M_{l+1}\vec{r}^T} \text{ and}$$
$$\overrightarrow{M_i\vec{r}^T} + s_{i-1}, \text{ where } l+1 < i \leq l+n.$$

The participants of any authorized set can reconstruct s_1, since the dealer publicly broadcasts $\overrightarrow{M_{l+1}\vec{r}^T}$. Then, they compute $\overrightarrow{M_{l+2}\vec{r}^T}$ from $\overrightarrow{M_{l+2}\vec{r}^T} + s_1$ and reconstruct s_2, and so on. Thus, the secrets $s_i, 1 \leq i \leq n$ be reconstructed in the desired order $s_1, s_2, \ldots, s_n$.

4 The Proactive Multi-use Scheme

In LMSS schemes, publishing shares during the process of reconstructing some secrets may leak unintended information of the other secrets unrecovered yet [10]. In this section, we first give a general method to solve this problem for any linear multi-secret sharing scheme based on MSP. Afterwards, we use this method to obtain a new way to make the linear secret sharing scheme proactive.

4.1 The Multi-use Scheme

As mentioned above, it is easy to see that publishing shares of participants of any authorized set in a LMSS scheme based on MSP during the process of reconstructing one secret may leak unintended information of the other secrets unrecovered yet. Here, we show how to solve this problem by using a simple strategy which does not need any private channel between any pair of participants. The other properties of the scheme are the same as in the previous section.

Suppose $\overrightarrow{g(v_i)}$ be target vectors. For each $1 \leq i \leq n$, the dealer randomly selects a vector $\vec{r_i} \in (\mathbb{Z}_2)^{t-1}$ such that $< \overrightarrow{g(v_i)}, \vec{r_i} >= 0$ and for each $1 \leq i, i' \leq n$, $\vec{r_i} \neq \vec{r_{i'}}$. He secretly transmits $\overrightarrow{M_j}$ and $\overrightarrow{M_j\vec{r}^T}$ to player $\mathcal{P}_j, 1 \leq j \leq l$ and publicly broadcasts the vectors $\vec{r_i}, 1 \leq i \leq n$.

Now suppose that the participants $P_{j'}$ of an authorized set A_j want to reconstruct the secret s_i where $1 \leq j' \leq t_j$ and $1 \leq i \leq n$. First, each participant $P_{j'}$ computes $\overrightarrow{M_{j'}\vec{r}_i^T}$. Then, the participants $P_{j'}$ of the authorized set use $\overrightarrow{M_{j'}}(\vec{r}^T + \vec{r}_i^T)$ as their pseudo shares to reconstruct the secret s_i as follows.

$$\vec{w}(M_{A_j}(\vec{r}^T + \vec{r}_i^T)) = (\vec{w}M_{A_j})(\vec{r}^T + \vec{r}_i^T) = \overrightarrow{g(v_i)} \cdot \vec{r}^T + \overrightarrow{g(v_i)} \cdot \vec{r}_i^T = s_i + 0 = s_i.$$

It is easy to see that the other participants cannot get one $P_{j'}$'s pseudo share from the other one, since $\overrightarrow{M_{j'}}$ is unknown for them. As we will show in the next section, this scheme is more efficient than the method described in [10].

4.2 New Proactive Scheme

Here, we describe our proactive secret sharing method which protects the secret by periodically renewing the shares of participants without changing the secret.

4.2.1 Share Renewal

For each $1 \leq i \leq n$, each participant P_j, $1 \leq j \leq l$ randomly selects and broadcasts a vector $\overrightarrow{r_{ij}} \in (\mathbb{Z}_2)^{t-1}$ such that $< \overrightarrow{g(v_i)}, \overrightarrow{r_{ij}} > = 0$. Then, each participant computes $\overrightarrow{r_i} = \overrightarrow{r_{i1}} + \cdots + \overrightarrow{r_{il}}$ which plays the role of random vector $\overrightarrow{r_i}$ selected by dealer in the multi-use scheme. That is, the new share of each participant P_j is $\overrightarrow{M_j}(\overrightarrow{r}^T + \overrightarrow{r_i}^T)$.

4.2.2 Reconstruct the Secret

The reconstruction phase is similar to the of multi-use scheme introduced in previous subsection. Suppose that the participants $P_{j'}$ of an authorized set A_j want to reconstruct the secret s_i. The participants $P_{j'}$ of the authorized set use $\overrightarrow{M_{j'}}(\overrightarrow{r}^T + \overrightarrow{r_i}^T)$ as their new shares to reconstruct the secret s_i as follows.

$$\vec{w}(M_{A_j}(\overrightarrow{r}^T + \overrightarrow{r_i}^T)) = (\vec{w}M_{A_j})(\overrightarrow{r}^T + \overrightarrow{r_i}^T) = \overrightarrow{g(v_i)} \cdot \overrightarrow{r}^T + \overrightarrow{g(v_i)} \cdot \overrightarrow{r_i}^T = s_i + 0 = s_i.$$

5 Security Proofs and Correctness

In this section, we prove that our scheme is a perfect LMSS scheme. We propose the following Lemma for achieving this goal.

Lemma 1 *Consider the scheme presented in Sect. 3. Then, for any* $1 \leq i \leq n$ *it holds that*

$$\overrightarrow{g(v_i)} \in \bigcap_{A_j \in \Gamma_{\min}} \sum_{\Psi(j') \in A_j} V_{j'} \setminus \bigcup_{B_j \in \mathcal{A}_{\max}} \sum_{\Psi(j') \in B_j} V_{j'}.$$

Proof We firstly prove that $\overrightarrow{g(v_i)} \in \bigcap_{A_j \in \Gamma_{\min}} \sum_{\Psi(j') \in A_j} V_{j'}$, where $1 \leq i \leq n$. For any $A_j \in \Gamma_{\min}$ and $1 \leq i \leq n$, according to the construction of the scheme, there must exist a path $v_0 - v_{j1} - v_{j2} - \ldots - v_{jt_j-1} - v - v_i$ from v_0 to v_i. Now not that $\overrightarrow{u_{j1}} + \sum_{i=2}^{t_j-1} \overrightarrow{u_{ji}} + \overrightarrow{u_{jt_j}} + \overrightarrow{u_{d_i}} = (\overrightarrow{g(v_0)} + \overrightarrow{g(v_{j1})}) + \sum_{i=2}^{t_j-1} (\overrightarrow{g(v_{ji-1})} + \overrightarrow{g(v_{ji})}) + (\overrightarrow{g(v_{jt_j-1})} + \overrightarrow{g(v)}) + (\overrightarrow{g(v)} + \overrightarrow{g(v_i)}) = \overrightarrow{g(v_0)} + \overrightarrow{g(v_i)} = \overrightarrow{g(v_i)}$. Since $V_{j'} = span\{\overrightarrow{M_{j'}}\}$, $1 \leq j' \leq l + n$, this equality indicates that for any $A_j \in \Gamma_{\min}$, there is a linear combination of the vectors in $\sum_{\Psi(j') \in A_j} V_{j'}$ which is equal to $\overrightarrow{g(v_i)}$. This means that $\overrightarrow{g(v_i)} \in \sum_{\Psi(j') \in A_j} V_{j'}$. Therefore we have $\overrightarrow{g(v_i)} \in \bigcap_{A_j \in \Gamma_{\min}} \sum_{\Psi(j') \in A_j} V_{j'}, 1 \leq i \leq n$.

Now, for every $1 \leq i \leq n$ we prove that $\overrightarrow{g(v_i)} \notin \bigcup_{B_j \in \mathcal{A}_{\max}} \sum_{\Psi(j') \in B_j} V_{j'}$. For any $B_j \in \mathcal{A}_{\max}$, the construction of the scheme indicates that there is not a path from v_0 to v_i. If we assume that there is a linear combination of the vectors in $\sum_{\Psi(j') \in B_j} V_{j'}$ which is equal to $\overrightarrow{g(v_i)}$, we obtain that $\overrightarrow{g(v_i)} = \overrightarrow{u_{h_1}} + \overrightarrow{u_{h_2}} + \cdots + \overrightarrow{u_{h_q}}$, where $h_j \in B$ and $1 \leq j \leq q$. Now, according to the construction of the scheme, suppose that $\overrightarrow{u_{h_j}} = \overrightarrow{g(v_{j_x})} + \overrightarrow{g(v_{j_y})}$. Then, we have

$$\overrightarrow{g(v_i)} = \overrightarrow{g(v_{1_x})} + \overrightarrow{g(v_{1_y})} + \cdots + \overrightarrow{g(v_{q_x})} + \overrightarrow{g(v_{q_y})}.$$

Note that there have to be an odd number of $\overrightarrow{g(v_i)}$ and an even number of $\overrightarrow{g(v_{1_x})}, \overrightarrow{g(v_{1_y})}, \ldots, \overrightarrow{g(v_{q_x})}, \overrightarrow{g(v_{q_y})}$ on the right side of the above equality. This result follows from the assumptions that $\overrightarrow{g(v_i)}, \overrightarrow{g(v_{1_x})}, \overrightarrow{g(v_{1_y})}, \ldots, \overrightarrow{g(v_{q_x})}, \overrightarrow{g(v_{q_y})}$ are linearly independent and $char(\mathbb{F}) = 2$. Now, according to the construction of the scheme, we conclude that the above equality determines a path from v_0 to v_i. This is a contradiction. Thus, for any $B \in \mathcal{A}_{\max}$, there is not a linear combination of the vectors in $\sum_{\Psi(j') \in B} V_{j'}$ which is equal to $\overrightarrow{g(v_i)}$, where $1 \leq i \leq n$. We obtain that $\overrightarrow{g(v_i)} \notin \sum_{\Psi(j') \in B} V_{j'}$ for each $B \in \mathcal{A}_{\max}$ and therefore $\overrightarrow{g(v_i)} \notin \bigcup_{B_j \in \mathcal{A}_{\max}} \sum_{\Psi(j') \in B_j} V_{j'}$ for every $1 \leq i \leq n$.

Finally, we conclude that for any $1 \leq i \leq n$,

$$\overrightarrow{g(v_i)} \in \bigcap_{A_j \in \Gamma_{\min}} \sum_{\Psi(j') \in A_j} V_{j'} \setminus \bigcup_{B_j \in \mathcal{A}_{\max}} \sum_{\Psi(j') \in B_j} V_{j'}.$$

In the above Lemma, we show that every authorized set $A \in \Gamma$ can recover the secret s_i, $1 \leq i \leq n$ by proving $\overrightarrow{g(v_i)} \in \bigcap_{A_j \in \Gamma_{\min}} \sum_{\Psi(j') \in A_j} V_{j'}$. Now, we have the following Theorem.

Theorem 2 *Our linear multi-secret sharing scheme is perfect.*

Proof We must show that if the participants of an unauthorized set $B \in \mathcal{A}$ pool their shares together, they obtain nothing about the secret s_i, where $1 \leq i \leq n$. In Lemma 1, we prove that $\overrightarrow{g(v_i)} \notin \bigcup_{B_j \in \mathcal{A}_{\max}} \sum_{\Psi(j') \in B_j} V_{j'}$, where $1 \leq i \leq n$. Thus, there is not a linear combination of their shares which is equal to s_i. Therefore, for every $1 \leq i \leq n$, the participants of unauthorized set B has no information on secret s_i.

6 Comparative Results

Here, we give a comparative discussion on the proposed scheme and some of previous schemes. We first want to point out that our multi-use scheme has two advantages than the multi-use scheme [10] which is based on multi-party computation:

1. Compared with the scheme [10], our multi-use scheme does not need private channels between each pair of participants.
2. Unlike our scheme, the multi-use scheme [10] does not work for an authorized set consist of only two participants. More precisely, suppose that in their scheme, this two participants want to recover $s_i, 1 \leq i \leq n$. If they publish their shares for computing the secret, then they can easily gain each other's shares.

Table 1 Basic comparison between Hsu et al. schemes and our scheme

Property	Hsu et al. [6]	Hsu et al. [7]	Liu et al. [10]	S
The scheme is based on MSP	Yes	Yes	Yes	Yes
The scheme uses the graph theory	No	Yes	No	Yes
The scheme works for any given access structure	Yes	No	Yes	Yes
The secrets are reconstructed stage by stage in a predetermined order	No	No	No	Yes
The share of each participant is reusable	No	No	Yes	Yes
The scheme is proactive	No	No	No	Yes

We also compared the proposed proactive scheme with other proactive schemes investigated in the literature [13] such as [14, 15] and found that our scheme is more efficient than their schemes in terms of communication overhead. It is easy to see that our scheme does not need private channels between each pair of participants. In fact, new share of each participant is constructed in a public manner without using encryption schemes. Also, the attacks presented in [13] is not applicable to our scheme while guaranteeing that the M_i, $1 \leq i \leq l$, will never be allowed to appear. To ensure that no adversary gains knowledge about the M_i, $1 \leq i \leq l$ by exhaustive search, we can choose t to be sufficiently large. The results of Sect. 4 can be used for any LMSS scheme based on MSP in which the M_i, $1 \leq i \leq l$, are not public values.

We have also compared some other properties in our new LMSS scheme with other LMSS schemes based on MSP in the literatures [6, 7, 10] (see Table 1). For easiness, the abbreviations S is used for the proposed scheme.

Now, we use the following notations to analyze the number of public values and also complexities of the proposed LMSS scheme:

- T_m: The time required to execute a multiplication operation.
- T_a: The time required to execute an addition operation.

In Tables 2 and 3, we give a comparison of some LMSS schemes in the literatures [6, 7, 10]. In this tables, A, m, n and d are the corresponding authorized set, the number of all participants, the number of secrets and the number of columns of the distribution matrix M, respectively.

Table 2 Comparison of the computational complexities

Step	Hsu et al. [6]	Hsu et al. [7]	Liu et al. [10]	S
Setup	–	dT_a	–	dT_a
Distribution	m^2T_m	mdT_m	mdT_m	$d(m+n)T_m + nT_a$
Reconstruction	$\|A\|T_m$	$\|A\|T_m$	$(m^2+m)T_a$	$\|A\|T_m$

Table 3 Comparison of the number of secret and public values

	Hsu et al. [6]	Hsu et al. [7]	Liu et al. [10]	S
Number of public values	m^2+1	$ml+1$	$ml+1$	$2n$

In summary, we proposed a new perfect LMSS scheme with unconditional security based on MSP which is proactive, multi-use and multi-stage. We also demonstrated its security and correctness. It is interesting to see that our proactive and multi-use schemes is more efficient than the previously investigated schemes in terms of communication overhead which does not need private channels between each pair of participants or an encryption scheme between them. In fact, our constructions are new methods for devising proactive and multi-use secret sharing schemes.

References

1. Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions Information Theory*, *29*(2), 208–210.
2. Cramer, R., Damgård, I., & Maurer, U. (2000). *General secure multi-party computation from any linear secret-sharing scheme*, advances in cryptology-EUROCRYPT, pp. 316–334, 2000.
3. Eslami, Z., & Kabiri Rad, S. (2012). A new verifiable multi-secret sharing scheme based on bilinear maps. *Wireless Personal Communications*, *63*(2), 459–467.
4. Ghasemi, R., Safi, A., & Hadian, M. (2017). *You have full text access to this contentEfficient multisecret sharing scheme using new proposed computational security model*, International Journal Of Communication Systems, https://doi.org/10.1002/dac.3399.
5. Herzberg, A., Jarecki, S., Krawczyk, H., & Yung, M. (1995). Proactive secret sharing or: How to cope with perpetual leakage. In Advances in CryptologyCRYPT0 95 (pp. 339–352). Berlin: Springer.
6. Hsu, C., Cheng, Q., Tang, X., & Zeng, B. (2011). An ideal multi-secret sharing scheme based on MSP. *Information Sciences*, *181*(7), 1403–1409.
7. Hsu, C., Harn, L., & Cui, G. (2014). An ideal multi-secret sharing scheme based on connectivity of graphs. *Wireless Personal Communications*, *77*(1), 383–394.
8. Karchmer, M., & Wigderson, A. (1993). On span programs. In *Structure in complexity theory conference* (pp. 102–111).
9. Liu, Y., Harn, L., & Chang, C.-C. (2015). A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets. *International Journal of Communication Systems*, *28*, 1282–1292.
10. Liu, M., Xiao, L., & Zhang, Z. (2006). Linear multi-secret sharing schemes based on multi-party computation. *Finite Fields and Their Applications*, *12*(4), 704–713.
11. Liu, Y. (2016). Linear (k, n) secret sharing scheme with cheating detection. *Security and Communication Networks*, *9*(13), 2115–2121.
12. Mashhadi, S. (2017). Secure publicly verifiable and proactive secret sharing schemes with general access structure. *Information Sciences*, *378*, 99–108.
13. Nikov, V., Nikova, S., & Preneel, B. (2007). On proactive verifiable secret sharing schemes. *Serdica Journal of Computing*, *1*(3), 337–364.
14. Nikov, V., Nikova, S., Preneel, B., & Vandewalle, J. (2002). Applying general access structure to proactive secret sharing schemes. *IACR Cryptology ePrint Archive*, p. 141.
15. Nikov, V., Nikova, S., Preneel, B., & Vandewalle, J. (2002). On distributed key distribution centers and unconditionally secure proactive verifiable secret sharing schemes based on general access structure. In *Progress in cryptology INDOCRYPT 2002* (pp. 422–435). Berlin: Springer.
16. Ostrovsky, R., & Yung, M. (1991). How to withstand mobile virus attacks. In *Proceedings of the tenth annual ACM symposium on Principles of distributed computing* (pp. 51–59).
17. Peng, Q., & Tian, Y. (2016). Publicly verifiable secret sharing scheme and its application with almost optimal information rate. *Security and Communication Networks*, *9*(18), 6227–6238.
18. Peng, Q., & Tian, Y. (2016). A publicly verifiable secret sharing scheme based on multilinear Diffie–Hellman assumption. *International Journal of Network Security*, *18*(6), 1192–1200.
19. Qin, H., Dai, Y., & Wang, Z. (2009). A secret sharing scheme based on (t, n) threshold and adversary structure. *International Journal of Information Security*, *8*(5), 379–385.
20. Stinson, D. R., & Wei, R. (1999). Unconditionally secure proactive secret sharing scheme with combinatorial structures. In *Selected areas in cryptography*, (pp. 200–214). Berlin: Springer.
21. Xiao, L., & Liu, M. (2005). Linear multi-secret sharing schemes. *Science in China Series F: Information Sciences*, *48*(1), 125–136.

22. Xiao, L., Liu, M., & Zhang, Z. (2005). Statistical multiparty computation based on random walks on graphs. *IACR Cryptology ePrint Archive*, p. 337.
23. Zarepour-Ahmadabadi, J., Shiri-Ahmadabadi, M., Miri, A., & Latif, A. (2018). A new gradual secret sharing scheme with diverse access structure. *Wireless Personal Communications*, *99*(3), 1329–1344.

Massoud Hadian Dehkordi received his Ph.D. degree in Mathematics from Loughborough University, UK, in 1998. He is currently a professor of mathematics at the school of Mathematical Sciences in Iran University of Science and Technology (IUST), Tehran, Iran. His research interests include Number Theory, Cryptography and other related topics.

Samaneh Mashhadi was born in Tafresh, Iran, on March 27, 1982. Shereceived the B.Sc. and M.Sc. degrees with honors in Mathematics fromIran University of Science and Technology (IUST), and Amirkabir University of Technology (AUT) in 2003 and 2005, respectively. She received her Ph.D. withhonors in Mathematics (Cryptography) in 2008 from IUST. She is currently an assistant professor inthe School of Mathematical sciences of IUST. Her research interests include analysis, design, and application of digital signatures, secret sharing schemes, and security protocols.

Hossein Oraei was born in 1990 in Isfahan. He received the B.Sc. and M.Sc. degrees with honors in Mathematics from Qom University and Sharif University of Technology in 2012 and 2014, respectively. He is currently a Ph.D. student in the School of Mathematical sciences at Iran Universityof Science and Technology. His research interests include Symmetric Cryptography and Secret Sharing.