IET Information Security

Research Article

Threshold verifiable multi-secret sharing based on elliptic curves and Chinese remainder theorem

ISSN 1751-8709
Received on 1st May 2018
Revised 7th November 2018
Accepted on 10th January 2019
E-First on 20th February 2019
doi: 10.1049/iet-ifs.2018.5174
www.ietdl.org

Maryam Sheikhi-Garjan[1], *Mojtaba Bahramian*[1] ✉, *Christophe Doche*[2]
[1]*Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, 87317-53153, Iran*
[2]*Departement of Computing, Faculty of Science and Engineering, Macquarie University, North Ryde, NSW 2109, Australia*
✉ *E-mail: bahramianh@kashanu.ac.ir*

Abstract: In this study, the authors propose a new protocol to share secret shadows for verifiable (t, n) secret sharing (VSS) schemes. Unlike traditional VSS schemes, whose communications between the dealer and the participants require a secure channel, the authors' new scheme relies on the elliptic curve cryptosystem and the Chinese remainder theorem operates over a public channel. The security of the secret shadows and the verification algorithm are based on the hardness of the elliptic curve discrete logarithm problem. They also extend the proposed scheme to an efficient verifiable multi-secret sharing (VMSS) scheme, particularly when the number of secrets is more than the threshold. As a result, their scheme is a multi-use and efficient VMSS on the public channel which provides the same level of security as traditional VMSS schemes with much shorter keys.

Nomenclature

T_M	average cost of scalar multiplication on the elliptic curve
T_E	cost of modular exponentiation on the finite field
T_P	cost of a pairing on the elliptic curve
T_{MP}	cost of a multilinear map
T_{DKE}	cost of a double knapsack algorithm
$T_{\mathrm{crt}}(n)$	cost of computing a unique solution for a system of n congruencies
$T_L(t)$	cost of the Lagrange basis of t points
T_H	cost of two-variable one-way hash function
$T_{\mathrm{eq}}(t)$	cost of the calculation of t linear equations

1 Introduction

Secret sharing has been an interesting research area of modern cryptography. It is an imperative tool in a vast range of cryptography applications including safeguarding cryptographic keys, secure multiparty computation, access control, e-voting, *ad-hoc* networks and multi-policy cryptosystems. In 1979, Shamir [1] and Blakley [2] independently introduced the first secret sharing scheme. In those schemes, a *secret s* is split into *n* pieces, called *shadows* or *shares*. This operation is performed by a *dealer* and shared among a group of *n participants*. Only *qualified sets* can pool their shares together and recomputed the secret *s*. The family of all qualified sets of participants is called *the access structure*. If the qualified set is specified by the set of at least *t* participants, which valid using shares can jointly recover the secret, the protocol is called a (t, n) *threshold secret sharing scheme*. In such schemes [1, 2] fewer than *t* shares cannot provide any knowledge about*s* and in this case, an access structure will be referred to as a *threshold access structure*.

In Shamir's scheme, only one secret can be shared during each secret sharing process. Also, the dealer must refresh the secret shadows and redistribute them to the participants to share a new secret, which is a costly process. These weaknesses have been addressed by the introduction of a multi-stage *multi-secret sharing* (*MSS*) scheme by He and Dawson [3] in 1994. In a multi-stage MSS scheme, multiple secrets can be derived in particular/any order in the reconstruction phase [4–9]. The MSS schemes that all secrets could be constructed simultaneously are proposed in [10–15]. To share secrets with various thresholds, an MSS scheme based on CRT and Shamir's scheme is presented in [16].

In order to correctly reconstruct the secret in Shamir's scheme [1], the dealer, who distributes the shadows and the participants, who receive the shadows are all assumed, to be honest. One of the weaknesses of Shamir's scheme is that malicious participants or/and the dealer can submit invalid shares to cheat other participants from recovering the valid secret. A *verifiable secret sharing* (*VSS*) scheme, introduced by Chor *et al.* [17] is designed to prevent this problem. In such a scheme, there is an additional algorithm called *verification*, which allows each participant to verify the consistency and the validity of the shadows received from the dealer or from other participants. Furthermore, *Publicly VSS* (*PVSS*) is introduced by Stadler [18]. PVSS schemes allow anyone, not just participants can check the validity of the shares during the reconstruction phase. An effective threshold PVSS scheme using properties of a multilinear map was presented in [19] whose security relies on the multilinear Diffie–Hellman (MDH) assumption. The verification algorithm of [11, 12, 18, 20, 21] relies on the *discrete logarithm problem* (*DLP*). In addition, as a special case of a secret sharing scheme, a geometry-based $(4, n)$-VSS based on personalised spherical coordinate space is proposed in [22].

In traditional secret sharing schemes, a secure channel between the dealer and the participants is required. It is used by the dealer or participants to distribute the private values (shadows). Certain *verifiable MSS* (*VMSS*) schemes removed the need for a secure channel. In [11], Shao and Cao proposed an efficient VMSS scheme based on [10] by adding the verification property. The distribution of secret shadows in both is done over a secure channel. Zhao *et al.* [20] in 2006 and Dehkordi and Mashhadi [12, 23] in 2008 were solved this problem and proposed public channel between the dealer and participants relies on the intractability of the DLP and of integer factorisation.

So far, many *VMSS* schemes were proposed [10–13, 20, 23] to provide some improvements by reducing public values, computational cost and increasing the security and efficiency. The security of [12, 20, 21, 23, 24] relies either on the hardness of the DLP in a finite field or on the integer factoring problem and the most time-consuming part in these schemes is modular exponentiation.

Recently, *elliptic curve cryptography* (*ECC*) [25–27] has received much attention. ECC provides the same level of security

ElGamal or RSA using much smaller keys. Thus ECC is an interesting choice, especially since it can also reduce the computational cost. Also, *bilinear pairing* (*BP*) on elliptic curves [28] is applied as an important tool in detecting cheaters in the verification phase of secret sharing schemes. The security of BP relies on the computational Diffie–Hellman problem (CDHP). The use of ECC and BP has been found in [13, 14, 16, 29–31].

The VMSS schemes proposed in [13, 14] are based on ECC and BP. Moreover, multiple secrets are reconstructed at one time, there is no secure channel and flexible to change the threshold value. The scheme [14] has performed two improvements on [13] by reducing the number of public values and removing the limitation on the number of secrets.

In [15], the ECC and double knapsack algorithm were employed in the structure of VMSS scheme which has improved the scheme [32] by providing a verification algorithm and public channel.

In [31], a multi-use (t, n) MSS was proposed. In this scheme, the distribution of the secret shadows on the secure channel and reconstruction phase is done using the ECC and Weil pairing on elliptic curves. Furthermore, the secrets can be recovered in any desired order.

In this paper, a new way to share secret shadows based on ECC and Chinese remainder theorem (CRT) are introduced. Our VMSS scheme eliminates the need for a secure channel and multiple secrets can be shared and reconstructed efficiently. The security of the proposed scheme is based on the *elliptic curve DLP* (*ECDLP*).

The remaining of this paper is organised as follows: In Section 2, we present Shamir's scheme, Shao and Cao's scheme, some background on elliptic curves and CRT. Then we propose our scheme in Section 3 and finally, we analyse the performance and security of our scheme in Section 4 before concluding in Section 5.

2 Preliminaries

2.1 Shamir's scheme

Shamir's (t, n) secret sharing scheme [1] consists of two algorithms: *share generation* and *secret reconstruction*. Let us denote by $\mathscr{M}$ the set of n shareholders $\{M_1, \ldots, M_n\}$ and let D a mutually trusted dealer. All computations are performed in the finite field F_p, where p is a large prime number.

i. *Share generation algorithm*: First, D selects a polynomial $P(x)$ of degree $t-1$ such that $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$, where $a_0 = s$ and $\{a_1, a_2, \ldots, a_{t-1}\} \in F_p$ are randomly chosen. The n shares $s_1 = P(1), s_2 = P(2), \ldots, s_n = P(n)$ are computed by D.

   Each share s_i is distributed to the participant M_i by D using a secure channel.

ii. *Secret reconstruction algorithm*: The secret $\boldsymbol{s}$ can be reconstructed by using any $\boldsymbol{t}$ shares and Lagrange interpolation formula. Without any loss of generality, we assume that the $\boldsymbol{t}$ selected shares are $s_1, s_2, \ldots, s_t$. We then have

$$s = P(0) = \sum_{i=1}^{t} s_i \prod_{j=1, j \neq i}^{t} \frac{j}{j-i}. \qquad (1)$$

Although the Shamir's scheme is a simple and efficient method for sharing a secret, one can find the following drawbacks:

- In one process of Shamir's scheme, only one secret can be shared.
- It is a one-time use scheme, all information needs to update for sharing a new secret.
- Need a secure channel between the dealer and participants to distribute the shares.
- To recover the unique secret, the dealer and participants should be honest.

In the next section, we briefly describe Shao and Cao's scheme. In the following scheme, some of the proposed drawbacks are solved. It also gives you some basic information related to a multi-use VMSS scheme.

2.2 Shao and Cao's VMSS

Shao and Cao's scheme is based on [10], adding the verifiable property, which relies on the intractability of the DLP over finite fields. In both [10, 11], a two-variable one-way function is used to protect the secret shadows. We refer to [11] for the properties of this one-way function. Let $P_1, \ldots, P_{k-1}$ be k secrets to be shared and let $f(r, s)$ be a two-variable one-way function, where r is a random integer and s is a secret shadow. D performs the following steps:

i. Choose a prime p and a generator g of order q such that $q | p-1$ and the DLP in the group generated by g is hard.

ii. Choose randomly n distinct secret shadows $s_1, s_2, \ldots, s_n$ and distribute s_i to M_i using a secure channel.

iii. Select an integer r and compute $f(r, s_1), f(r, s_2), \ldots, f(r, s_n)$.

- If $k \leq t$

  ○ Select random numbers $P_k, P_{k+1}, \ldots, P_{t-1}$ in order to construct the polynomial $h(x)$ mod q of degree $t-1$ such that:

$$h(x) = \sum_{i=0}^{t-1} P_i x^i \bmod q.$$

  ○ Compute

$$\{y_i = h(f(r, s_i)) \bmod q\}_{i=1}^{n}$$

$$\{G_i = g^{P_i} \bmod p\}_{i=0}^{t-1}.$$

  ○ Publish $\{r, y_1, y_2, \ldots, y_n, G_0, G_1, \ldots, G_{t-1}\}$.

- If $k > t$

  ○ Construct $h(x) = P_0 + P_1x + \cdots + P_{k-1}x^{k-1} \bmod q$.

  ○ Compute $\{y_i = h(f(r, s_i)) \bmod q\}_{i=1}^{n}$, $\{h(i) \bmod q\}_{i=1}^{k-t}$ and $\{G_i = g^{P_i} \bmod p\}_{i=0}^{k-1}$.

  ○ Publish $(r, h(1), \ldots, h(k-t), y_1, \ldots, y_n, G_0, \ldots, G_{k-1})$.

Each participant M_i can verify whether its share is valid or not by computing the following:

$$g^{y_i} = \prod_{j=0}^{\max(k,t)-1} G_j^{f(r, s_i)^j} \bmod p.$$

When at least t shares $f(r, s_i)$ are pooled together, participants M_i can check whether others' secret shadows are valid or not by checking the following equalities:

$$g^{y_j} = \prod_{i=0}^{\max(k,t)-1} (G_i)^{f(r, s_j)^i} \bmod p, \quad \text{for } j = 1, 2, \ldots, t, j \neq i.$$

Then the polynomial $h(x)$ can be uniquely computed by Lagrange interpolation polynomial as follows:

i. If $k \leq t$

$$\sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{x - f(r, s_j)}{f(r, s_i) - f(r, s_j)} \bmod q$$
$$= P_0 + \cdots + P_{k-1}x^{k-1} + P_kx^k + \cdots + P_{t-1}x^{t-1} \bmod q.$$

1. If $k > t$

$$\begin{aligned}&\sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - f(r,s_j)}{f(r,s_i)-f(r,s_j)} \prod_{l=1, l\neq f(r,s_i)}^{t} \frac{x-l}{f(r,s_i)-l}\\ &\quad+ \sum_{i=1}^{k-t} h(i) \prod_{j=1,j\neq i}^{k-t} \frac{x-j}{i-j} \prod_{l=1,l\neq f(r,s_l)}^{t} \frac{x-f(r,s_l)}{i-f(r,s_l)} \bmod q\\ &\quad= P_0 + P_1 x + \cdots + P_{k-1}x^{k-1} \bmod q\,.\end{aligned}$$

Moreover, the participants can check the validity of the secrets that were sent to them by checking that

$$G_i = g^{P_i} \bmod p, \quad \text{for } i = 0, 1, \ldots, k-1.$$

2.3 Chinese remainder theorem

Let $(x_1, n_1), (x_2, n_2), \ldots, (x_t, n_t)$ be integers where n_i's denote positive pairwise coprime integers greater than 1, $t \geq 2$ and $0 \leq x_i < n_i$, respectively, a system of congruencies

$$\begin{aligned} x &\equiv x_1 \mod n_1\\ &\vdots\\ x &\equiv x_t \mod n_t\end{aligned} \qquad (2)$$

has a unique solution x modulo $N = \prod_{i=1}^{t} n_i$.

Let $N_i = N/n_i$ and $N_i'N_i \equiv 1 \bmod n_i$, one gets the solution eventually $x = \sum_{i=1}^{t} x_i N_i N_i'$.

2.4 Elliptic curves

Here, we briefly give the definitions and some properties of elliptic curves. For more information see [33]. Let F_q be a field of a characteristic p, with p different from 2 and 3. An *elliptic curve* E defined over F_q is given by the equation $y^2 = x^3 + ax + b$, where $a, b \in F_q$ and $4a^3 + 27b^2 \neq 0 \bmod q$. The set of all solutions $(x, y) \in F_q$ together with the *point at infinity*, denoted by $\mathcal{O}$ form a finite Abelian group denoted by $E(F_q)$. Geometrically adding two points is given by the tangent and chord method. More precisely, for two arbitrary points $P = (x_p, y_p)$ and $Q = (x_q, y_q) \in E(F_q)$ the addition $R = P + Q$ can be defined as

$$R = \begin{cases} \mathcal{O} & \text{if } x_p = x_q, y_p = -y_q\\ Q & \text{if } P = \mathcal{O}\\ P & \text{if } Q = \mathcal{O}\\ (x_r, y_r) & \text{otherwise}\end{cases}$$

where

$$x_r = \lambda^2 - x_p - x_q, \quad y_r = \lambda(x_p - x_r) - y_p$$

and

$$\lambda = \begin{cases} \dfrac{y_q - y_p}{x_q - x_p} & \text{if } P \neq Q\\[2ex] \dfrac{3x^2 + a}{2y_p} & \text{if } P = Q, y_p \neq 0.\end{cases}$$

The *opposite* of the point P is denoted by $-P$ and satisfies $P - P = \mathcal{O}$.

Relying on this addition, we can introduce a new operation called *scalar multiplication*, which given a non-negative integer $d \in Z$ and a point $P \in E(F_q)$ consists in adding P or $-P$ to itself $d - 1$ or $-d - 1$ times, depending if d is positive or negative. The result, denoted by dP is again a point on the curve E.

2.5 Elliptic curve cryptography

The well-known public key cryptosystem RSA and ElGamal were based on modular arithmetic. The security of RSA relies on the difficulty to factor integers, while ElGamal hinges on the hardness of DLP in a finite field. In 1985, Koblitz [25] and Miller [27] proposed a new paradigm called *elliptic curve cryptography* (*ECC*), which could provide an effective cryptographic system. ECC provides an alternative system for digital signatures and encryption for secure key distribution [34]. Recently, ECC has drawn lots of attention because of its advantages like short key length, fast computation speed, and smaller storage capacity.

The security of an elliptic curve cryptosystem is based on the hardness of the *ECDLP*. Given $P \in E(F_q)$ a point of order n and let $Q \in \langle P \rangle$, solving the ECDLP consists in finding an integer d, $0 \leq d \leq n - 1$, such that $Q = dP$.

The primary advantage of ECC is that solving the ECDLP in $E(F_q)$ is harder than solving the DLP in F_q^*. The best-known algorithms to solve ECDLP are exponential time, whereas factoring integers or solving the DLP can be done in sub-exponential time. As a corollary, for the same level of security, the size of keys in ECC is smaller than its rival cryptosystems RSA and ElGamal. For instance, 224-bit keys for ECC provide the same level of security than 2048-bit keys for RSA or ElGamal. By increasing the key size, the security gap increases dramatically between the systems. For example, keys of size 256-bit and 512-bit for ECC, respectively, provide the same level of security as 3000-bit and 15,000-bit keys for RSA or ElGamal [25, 27].

3 Proposed scheme

In this section, we describe our verifiable threshold secret sharing scheme rely on the properties of ECC and CRT. This scheme consists of four algorithms **Initialisation, Distribution, Verification** and **Reconstruction**. As before, let D denotes a trusted dealer and $\mathcal{M} = \{M_1, M_2, \ldots, M_n\}$ denote the set of participants.

- The secret can be reconstructed by every qualified subset of at least t participants of $\mathcal{M}$.
- It enables each participant to verify the validity of his share.
- It also allows each participant who is involved in secret reconstruction to check the validity of other participants' share.
- The master shadows/shares are multi-use. As they are protected during the secret sharing process and reusable for refreshing the public values of the new secret.
- The scheme can be extended to a multi-use (t, n) VMSS.
- The security of the proposed scheme is based on *ECDLP*. Therefore, it is a computationally secure scheme.

3.1 Our VSS scheme

Initialisation phase: In the initialisation phase, the trusted dealer D chooses the master secret shares and transmits them to the M_i on a public channel. This phase will be executed only once for a multi-use secret sharing scheme. Let E be an elliptic curve defined over a finite field F_p, where $p \neq 2, 3$ is a prime number and $T \in E(F_p)$ be a base point of prime order ℓ. The public information i $\{F_p, E, T\}$. D chooses a prime number $p_0 < \ell$ and n distinct positive integers $p_1, \ldots, p_n$ along with the following properties:

- $p_0 < p_i$ for $1 \leq i \leq n$.
- $p_1, \ldots, p_n$ are n pairwise coprime or prime numbers.

The following steps are done between D and M_i's to transfer the master secret shadows $p_1, \ldots, p_n$ to the participants:

i. D chooses an integer d, $1 < |d| < \ell$ as his/her private key and publishes $G = dT$ as his/her public key.
ii. Each participant $M_i, 1 \leq i \leq n$ randomly selects an integer n_i, $1 < |n_i| < \ell$ as his/her private key, computes $T_i = n_i T$ and broadcasts T_i. To make sure that T_i's are distinct D will ask new one until $T_i \neq T_j$ for $i \neq j$ and publish (T_i, ID_i) as a public key M_i. (ID_i is the corresponding identity of M_i).

iii. $G_i = dn_iT = (x_i, y_i)$ is a common key between D and M_i. Both D and M_i using his/her private key and public information T_i and G can compute G_i.

iv. D computes $c_i = p_ix_i$, where $G_i = dT_i = (x_i, y_i)$ and finally broadcasts c_i for $1 \le i \le n$.

v. Each participant M_i, $1 \le i \le n$ retrieves G_i using his/her private key n_i and G then computes $p_i = c_ix_i^{-1}$.

At the end of this phase both D and M_i get the master share p_i.

Distribution phase: Assume that $s < \ell$ denote the secret which the D wishes to share in a (t, n) secret sharing process. The D runs the following algorithm:

i. Construct the polynomial $F(x)$ of degree $t-1$, where $a_1, a_2, \ldots, a_{t-1} \bmod \ell$ are randomly chosen integers as coefficients of $F(x)$.

$$F(x) = s + a_1x + \cdots + a_{t-1}x^{t-1} \bmod \ell\,.$$

ii. Select n random integers $p_0 \le y_i < p_i$ for $1 \le i \le n$, such that $x_i = y_i \bmod p_0$ and x_i's be n distinct integers.

iii. Compute $F(x_i) \bmod \ell$ for $1 \le i \le n$ and $A_0 = sT, A_1 = a_1T, \ldots, A_{t-1} = a_{t-1}T$.

iv. Compute a unique integer $X \bmod \prod_{i=1}^{n} p_i$ such that $X \equiv y_i \bmod p_i$ using the values $\{y_1, y_2, \ldots, y_n\}$, $\{p_1, \ldots, p_n\}$ and *CRT*.

v. Publish $\{X, F(x_1), \ldots, F(x_n), A_0, \ldots, A_{t-1}\}$ as public information.

Verification phase: Any participant can verify the validity of other participant's shares by using the following verification algorithm, which uses the additive structure of elliptic curves.

i. Each participant M_i can check the following equations to verify whether the public value published by the dealer is consistent with its shadow:

$$F(x_i)T = \sum_{j=0}^{t-1} x_i^jA_j, \quad \text{for}\, i = 1, \ldots, n\,. \tag{3}$$

ii. Without any loss of generality, suppose that participants $\{M_i\}_{i=1}^{t}$ are willing to recover multiple secrets from at least t shares x_i pooled together. Each participant M_i can check the validity of others' secret shadows by checking the following equations:

$$F(x_j)T = \sum_{i=0}^{t-1} x_j^iA_i, \quad \text{for } j = 1, \ldots, t, j \ne i\,. \tag{4}$$

Reconstruction phase:

i. The $s = F(0)$ can be uniquely determined by Lagrange interpolation method, as follows:

$$s = \sum_{i=1}^{t} F(x_i) \prod_{j=1, j \ne i}^{t} \frac{x_j}{x_j - x_i} \bmod \ell\,.$$

ii. If the secrets are $k \le t$, using the Lagrange interpolation method, the polynomial $F(x)$ can be determined as follows:

$$F(x) = \sum_{i=1}^{t} F(x_i) \prod_{j=1, j \ne i}^{t} \frac{x - x_j}{x_i - x_j} \bmod \ell\,.$$

3.2 Our VMSS scheme

Assume that $\{s_0, s_1, \ldots, s_{k-1} < \ell\}$ denote k secrets to be shared in one secret sharing process. If $k \le t$ like the schemes [10–12], the secrets can be considered as the coefficients of the $F(x)$ in the proposed VSS scheme. Here we introduce an efficient scheme to share k secrets simultaneously when $k > t$. The dealer does the following:

i. Run the initialisation phase of the previous VSS scheme.

ii. Set the polynomial $S(x)$ of degree $k-1$, where $s_0, s_1, \ldots, s_{k-1}$ are coefficients

$$S(x) = s_0 + s_1x + \cdots + s_{k-1}x^{k-1} \bmod \ell\,.$$

iii. Choose randomly an integer $0 < r < \ell$ and compute

$$S'(x) = r\prod_{j=0}^{k-1}(x - j) = s'_0 + s'_1x + \cdots + s'_{k-1}x^{k-1}\,.$$

iv. Compute the polynomial $H(x) = S(x) - S'(x)$.

v. Run the *distribution phase* of the proposed *VSS scheme*.

vi. Publish $\{X, H(x), F(x_1), \ldots, F(x_n), A_0, \ldots, A_{t-1}\}$.

vii Run *the verification phase* of the proposed *VSS scheme*.

.

Recovery phase:

i. As before, $r = F(0)$ can be uniquely determined by Lagrange interpolation method, as follows:

$$r = \sum_{i=1}^{t} F(x_i) \prod_{j=1, j \ne i}^{t} \frac{x_j}{x_j - x_i}\,.$$

ii. Compute the polynomial $S'(x)$,

$$r\prod_{i=0}^{k-1}(x - i) = s'_0 + s'_1x + \cdots + s'_{k-1}x^{k-1}\,.$$

iii. The polynomial $S'(x)$ along with public values $H(x)$ result in $S(x)$ as follows:

$$S(x) = H(x) + S'(x)$$

3.3 Updating phase

To share the new secrets, some public values need to refresh. As in our scheme, the master secret shadows are multi-use, there is no need to run initialisation again, the D just updates the public values in the distribution part. In particular, computing a new X is very efficient. As we pointed before, $X = \sum_{i=1}^{n} y_iP_iP'_i \bmod (\prod_{i=1}^{n} p_i)$ where $P_i = \prod_{j=1, j \ne i}^{n} p_j$ and $P_iP'_i \equiv 1 \bmod p_i$. Once the values $P_iP'_i$ for $i = 1, \ldots, n$ are computed by D, can be saved and reused again to refresh X. In each updating phase, D only selects y_i's and compute a new X using $P_iP'_i$'s.

4 Security and performance

In this section, we examine the security of the proposed scheme regarding the following aspects:

4.1 Security

Theorem 1: Any group of t or more participants can compute k secrets $s_0, s_1, \ldots, s_{k-1}$ and any group of $t-1$ or fewer, cannot reconstruct any secrets.

Proof: Without loss of generality, assume that $k < t$ and M_1, M_2, ..., M_t pool together their valid secret shares x_1, x_2, ..., x_t. Let $F(x) = s_0 + s_1x + \cdots + s_{t-1}x^{t-1}$ be a polynomial of a degree $t-1$ in which coefficients are secret. In this case, using the public values $F(x_1), \ldots, F(x_t)$, we have a system of t linear equations $s_0 + s_1x_i + \cdots + s_{t-1}x_i^{t-1} = F(x_i)$ and t unknown values $s_0, s_1, \ldots, s_{t-1}$. By our assumption on the choice of x_i's, $x_i \ne x_j$ for $i \ne j$, the system has a unique solution. One can also interpolate through t points with an at-most $t-1$ degree polynomial $G(x)$ using the Lagrange interpolating method. The uniqueness of the interpolating polynomial shows that $G(x) = F(x)$. It is clear that for any $t-1$ points $(x_i, F(x_i))$, we have a system of $t-1$ linear equations and t unknown values. Moreover, the degree of interpolating polynomial is at most $t-2$. □

Theorem 2: In the proposed scheme, the master secret shadows $p_1, \ldots, p_n$ cannot be computed from public parameters G, T_i and c_i.

Proof: If an attacker (or $M_j, j \neq i$) wants to derive p_i from the public parameters $G = dT, T_i = n_iT, c_i = p_i x_{dn_iT}$ would need to solve the CDHP to compute $dn_iT = (x_{dn_iT}, y_{dn_iT})$ from $T_i = n_iT, G = dT$ or the ECDLP, which is computationally hard. Therefore, only M_i using her/his private key n_i can compute $n_iG = n_idT$ and obtain the corresponding master secret shadow p_i. □

Theorem 3: In the proposed VSS scheme, it is computationally hard to compute the secrets $s_0, s_1, \ldots, s_{k-1}$ from public values $A_0, \ldots, A_{k-1}$.

Proof: $A_i \in \langle T \rangle$ and $A_i = s_iT$'s are public information and used in the verification phase. If an attacker wants to obtain s_i directly from the public value $A_i = s_iT$ would effectively be able to solve the ECDLP. The same is true for the VMSS scheme. □

Theorem 4: The scheme is secure against the participants-cheating scenario, i.e. the secret shares provided by the participants in the reconstruction phase can be verified and the cheaters can be detected. Furthermore, the scheme can check the validity of the secrets after reconstruction phase, so invalid secrets can be identified.

Proof: Suppose that M_i provides an invalid share x_i' instead of x_i to the combiner or participant who is responsible for reconstructing the secrets. As we know, $F(x_i), i = 1, \ldots, n$ and $A_k, k = 0, 1, \ldots, t-1$ are public values. Combiner computes $R = \sum_{k=0}^{t-1} x_i'^k A_k$ and checks whether $R = F(x_i)T$ or not. If $R \neq F(x_i)T$ combiner identifies M_i as a cheater. If combiner is not trusted and wants to cheat other participants by publishing invalid secrets at the end of reconstructing phase, in this case upon receiving s_i's each participant can verify the validity of the secrets using the public information A_i's if $s_iT = A_i$ holds. □

Theorem 5: In our scheme, the master secret shadows $p_1, p_2, \ldots, p_n$ are multi-use.

Proof: Once the secrets are shared, only x_i's will be revealed and y_i, p_i's are kept secret, as we mentioned above, it is computationally hard obtaining p_i's from c_i's. Regarding $p_i | X - y_i$ and $x_i = y_i \bmod p_0$, the possibility of computing p_i from x_i is equal to find all possible values $p_0 \leq y_i \leq X$ in which $x_i = y_i \bmod p_0$ and search all values that divide $X - y_i$ which has exponential time complexity. □

4.2 Performance

In this section, we analyse the efficiency of our new verifiable MSS scheme. The performance analysis and comparison with similar schemes can be viewed from the following aspects in Table 1:

i. The need for a secure channel.
ii. The verifiability of secret shadows.
iii. Multi-use.
iv. The degree of the polynomial in the distribution phase.
v. The security of the scheme.
vi. The number of public values needs to be updated.
vii The computing in the verification phase.
.

We also compared the computation complexity of our scheme with the schemes [12, 13, 15, 16, 19, 30, 31] to share k ($k \geq 1$) secrets in the distribution, recovery and verification phases. We only consider major time-consuming operations in performance analysis of our scheme and other schemes. So, we do not count the number of finite field multiplications and additions are done in the process of sharing a secret or secrets.

In our scheme, the initialisation phase is responsible for generating public channel between the dealer and participants to share reusable master secret shares. The security of the proposed public channel is based on ECDLP. In this phase, two elliptic curve scalar multiplications (T_M) are done by the dealer and each participant M_i to compute G, T_i and common key G_i. So, to share multi-use master shares among n participants $(3n+1)T_M$ are done by the dealer and participants. For the multi-use purpose, this algorithm runs only once so, we do not include the computational cost of this phase in Table 2.

The major operations in the distribution phase are T_{crt} and tT_M for computing of X and $A_0, A_1, \ldots, A_{t-1}$, respectively. In the verification phase, to check the validity of a secret shadow x_i using (3), tT_M are needed. Therefore, to verify t secret shadows, t^2T_M are done by the combiner.

In the recovery phase, combiner computes t Lagrange basis $T_L(t)$ to reconstruct the secret or secrets. More detailed information is given in Table 2.

Table 1 Comparison with other schemes

Features	Our scheme	[12]	[13]	[15]	[16]	[19]	[30]	[31]
(1)	no	no	no	no	yes	no	no	yes
(2)	yes	yes	yes	yes	no	yes	yes	no
(3)	yes	yes	yes	yes	no	yes	yes	yes
(4)	*t*−1	*k*−1	*t*−1	*k*	*t*	*t*−1	*t*−1	*t*−1
(5)	ECDLP	DLP-RSA	ECDLP-DLP	ECDLP-DKP	FCRT	MDHP	ECDLP	ECDLP-DLP
(6)	$n+k+t+1$ $(k > t)$ $n+t+1$ $(k \leq t)$	$2n+k-t+1$ $(k > t)$ $2n+1$ $(k \leq t)$	$n+1$, $k=t$	$k+3$	$k+n$	$3n+t$, $k=1$	$nt+n^2$, $k=1$	$2k$
(7)	SM	ME	BP	DKE-SM	unverifiable	MP	BP	unverifiable

Table 2 Performance

Phases	Our scheme	[12]	[13]	[15]	[16]	[19]	[31]
distribution	tT_M	$n(T_E+T_H)$	$(n+1)T_M$	$(2n+1)T_M+T_{\text{DKE}}$	$T_{\text{ctr}}(k)$	$(3n+t)T_M+n(T_{\text{MP}}+T_E)$	$k(T_M+T_P)$
verification	t^2T_M	$t(T_E+T_H)$	$2tT_P$	$2nT_M+nT_{\text{DKE}}$	unverifiable	$2tT_{\text{MP}}$	unverifiable
recovery	$T_L(t)$	$T_L(k)$	$T_{eq}(t)$	$T_L(k)$	$T_L(t)$	$2tT_E+T_L(t)$	ktT_P+ktT_E

4.3 Comparison with previous works

In this section, we compared the efficiency of our new verifiable MSS scheme with other schemes regarding performance and security. In Table 2, we only compare the proposed scheme with the schemes [12, 13, 15, 16, 19, 31] which all have trusted party.

In the schemes [16, 31], there exists a secure channel between the dealer and participants, while our scheme and [12, 13, 15, 19] provide the computationally secure public channel. The security of our public channel and [13, 15, 19] is based on ECDLP to transfer the multi-use master secret shadows between the dealer and participants. The public channel of the scheme [12] is based on the intractability of the factorisation and the discrete logarithm modulo a large composite number. In [15], there is another public channel. The security of the public channel between the dealer and trusted combiner is based on finding double knapsack constants which are only known by the dealer and trusted combiner. In addition, the communication between the participants and trusted combiner is done on a public channel by employing the double knapsack algorithm. In the same security level, our proposed public channel provides a higher security level with the small bitlength size of required parameters.

In recent years, Weil pairing on elliptic curves has been used in the construction of MSS and VMSS schemes [13, 14, 30, 31]. Weil pairing has been used as a tool to transfer the ECDLP on $E(F_q)$ to DLP in the finite field F_{q^k}. A necessary requirement for security of pairing-based schemes is that DLP cannot be feasibly computed in the finite field F_{q^k}. For instance, in an 80-bit security level, the bitlength of q^k should be at least 1024 which is equivalent to bitlength of an RSA modulus in the same level. While the minimum bitlength of ℓ (prime order of base point $T \in E(F_q)$) so that ECDLP to be hard enough, is 160. As security requirements increase, the gap between the size of q^k and ℓ increases. In a 256-bit security level, the minimum bitlength of q^k is 15,360 opposed to 512 for ℓ. The properties of ECC (i.e. non-pairing based) in the setup and verification phases of our scheme can provide small parameters which save much power, bandwidth, storage and speed up computations.

If $k > t$, our VMSS scheme is more efficient in the reconstruction phase compare with [11, 12, 15, 31]. As main computation related to interpolation, verification, and public values are done over a $(t-1)$ th degree polynomial. In the scheme proposed, in [11, 12, 15] a $(k-1)$ th degree polynomial is reconstructed to share k secrets when $k > t$. In this case, one has to do k main operations instead of t. In [31] the degree of polynomial is $t-1$ but to reconstruct k secrets kt pairings, kt exponentiations (apart from multiplications) are needed. Hence, as k grows the computational cost consequently will increase in such schemes.

In [16], a threshold MSS scheme using CRT is proposed. Because of the mathematical structure of CRT, the dealer can set a polynomial to share k secrets among participants so that each secret can be reconstructed with a specific threshold. While in [16], the dealer submits all one-time use master shadows and the CRT modulo and its prime factorisation on a secure channel to the participants, in our proposed scheme by generating reusable master secret shadows, public channel and verification algorithm gains more efficiency. Furthermore, to share new secrets some information needs to be refreshed, in Shao and Cao's scheme and [12], the master secret shadows (s_i's) are protected by a two-variable one-way function $f(r, s_i)$ during the secrets reconstruction. So the dealer has to calculate $f(r, s_1), \ldots, f(r, s_n)$ for n secret shadows $s_1, \ldots, s_n$. Moreover, each of t participants M_i is involved in secrets recovery phase has to compute $f(r, s_i)$. To share new secrets these computations will be repeated with new r. To share new k secrets in [31], k scalar multiplications on the group of elliptic curve points are needed, while in our scheme, the updating phase is very efficient. We use the properties of CRT to reduce the computations in this part. As we mentioned in Section 3.3, the dealer computes X using $P_iP_i^{'}$ and y_i for $i = 1, \ldots, n$. So, the dealer can save $P_iP_i^{'}$'s and reuse them in the computation of a new X using new y_i's.

In [15, 30], verifiable threshold secret sharing schemes were proposed based on BP and MDH assumption, respectively. While Meng and Li [30] have solved key management problem for threshold signature in mobile *ad-hoc* network by removing the need for a trusted party, the computational cost of the scheme in distribution, verification and recovery phase compare to our scheme is really high. As in [30], each participant constructs a polynomial of degree $t-1$ which all t coefficients of the polynomial are points on elliptic curves, and each participant provides $n-1$ shares to other participants. In addition, the scheme has $nt + n^2$ public values and two verification algorithms based on the BP, which are used in the distribution and recovery phases. In [15], a publicly verifiable secret sharing is proposed to share a secret which is assumed to be a multilinear pairing. This scheme requires to refresh $3n + t$ public information to share a new secret in comparison with $n + t + 1$ in our VSS to share t secrets.

5 Conclusion

This paper proposes a multi-use (t, n) VSS and VMSS with the interesting property that no secure channel between the dealer and the participants is needed to exchange master multi-use secret shadows. The proposed scheme efficiently renews the public information and uses ECC, CRT and features. The secret shadows distribution and verification phases that are computationally secure under the hardness of the ECDLP.

6 Acknowledgments

The authors thank the referees for their careful reading and valuable comments. This research was partially supported by the University of Kashan under grant no. 682460/004.

7 References

[1] Shamir, A.: ‘How to share a secret’, *Commun. ACM*, 1979, **22**, (11), pp. 612–613

[2] Blakley, G.R.: ‘Safeguarding cryptographic keys’. Proc. 1979 AFIPS National Computer Conf., New York, New York, 1979, vol. 48, pp. 313–317

[3] He, J., Dawson, E.: ‘Multistage secret sharing based on one-way function’, *Electron. Lett.*, 1994, **30**, (19), pp. 1591–1592

[4] He, J., Dawson, E.: ‘Multisecret-sharing scheme based on one-way function’, *Electron. Lett.*, 1995, **31**, (2), pp. 93–95

[5] Harn, L.: ‘Comment: multistage secret sharing based on one-way function’, *Electron. Lett.*, 1995, **31**, (4), pp. 262–262

[6] Harn, L.: ‘Efficient sharing (broadcasting) of multiple secrets’, *IEEE Proc. Comput. Digit. Techn.*, 1995, **142**, (3), pp. 237–240

[7] Chang, T.Y., Hwang, M.S., Yang, W.P.: ‘A new multi-stage secret sharing scheme using one-way function’, *ACM SIGOPS Oper. Syst.*, 2005, **39**, (1), pp. 48–55

[8] Li, H.X., Cheng, C.T., Pang, L.J.: ‘An improved multi-stage (t,n)-threshold secret sharing scheme’. Advances in Web-Age Information Management, Hangzhou, China, 2005 (LNCS, **3739**), pp. 267–274

[9] Fatemi, M., Eghlidos, T., Aref, M.: ‘A multi-stage secret sharing scheme using all-or-nothing transform’, 2009

[10] Yang, C.C., Chang, T.Y., Hwang, M.S.: ‘A (t, n) multi-secret sharing scheme’, *Appl. Math. Comput.*, 2004, **151**, (2), pp. 483–490

[11] Shao, J., Cao, Z.: ‘A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme’, *Appl. Math. Comput.*, 2005, **168**, (1), pp. 135–140

[12] Dehkordi, M.H., Mashhadi, S.: ‘An efficient threshold verifiable multi-secret sharing’, *Comput. Stand. Interfaces*, 2008, **30**, (3), pp. 187–190

[13] Wang, S.J., Tsai, Y.R., Shen, C.C.: ‘Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ECC’, *Wirel. Pers. Commun.*, 2011, **56**, (1), pp. 173–182

[14] Eslami, Z., Rad, S.K.: ‘A new verifiable multi-secret sharing scheme based on bilinear maps’, *Wirel. Pers. Commun.*, 2012, **63**, (2), pp. 459–467

[15] Patel, N., Vyavahare, P.D., Panchal, M.: ‘A novel verifiable multi-secret sharing scheme based on elliptic curve cryptography’. The Tenth Int. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE 2016), Nice, France, 2016, pp. 230–234

[16] Chan, C.-W., Chang, C.-C.: ‘A scheme for threshold multi-secret sharing’, *Appl. Math. Comput.*, 2005, **166**, (1), pp. 1–14

[17] Chor, B., Goldwasser, S., Micali, S., *et al.*: ‘Verifiable secret sharing and achieving simultaneity in the presence of faults’. Proc. of the 26th IEEE Annual Symp. on Foundations of Computer Science, Washington DC, 1985, pp. 383–395

[18] Stadler, M.: ‘Publicly verifiable secret sharing’. Proc. of the 15th Annual Int. Conf. on Theory and Application of Cryptographic Techniques, Saragossa, Spain, 1996 (LNCS, **1070**), pp. 190–199

[19] Peng, Q., Tian, Y.: ‘A publicly verifiable secret sharing scheme based on multilinear Diffie-Hellman assumption’, *Int. J. Netw. Secur.*, 2016, **18**, (6), pp. 1192–1200

[20] Zhao, J., Zhang, J., Zhao, R.: 'A practical verifiable multi-secret sharing scheme', *Comput. Stand. Interfaces*, 2007, **29**, (1), pp. 138–141

[21] Wang, F., Zhou, Y.-S., Li, D.-F.: 'Dynamic threshold changeable multi-policy secret sharing scheme', *Secur. Commun. Netw.*, 2015, **8**, (18), pp. 3653–3658

[22] Tan, Z., Yang, G., Cheng, W.*, et al.*: 'Distributed secret sharing scheme based on personalized spherical coordinates space', *Comput. Sci. Inf. Syst.*, 2013, **10**, (3), pp. 1269–1291

[23] Dehkordi, M.H., Mashhadi, S.: 'New efficient and practical verifiable multi-secret sharing schemes', *Inf. Sci.*, 2008, **178**, (9), pp. 2262–2274

[24] Chen, L., Gollmann, D., Mitchell, C.J.*, et al.*: 'Secret sharing with reusable polynomials'. Proc. of the Second Australian Conf. on Information Security and Privacy-ACISP'97, Sydney, NSW, Australia, 1997 (LNCS), pp. 183–193

[25] Koblitz, N.: 'Elliptic curve cryptosystems', *Math. Comput.*, 1987, **48**, (177), pp. 203–209

[26] Koblitz, N., Menezes, A., Vanstone, S.: 'The state of elliptic curve cryptography', *Des. Codes Cryptogr.*, 2000, **19**, (2), pp. 173–193

[27] Miller, V.S.: 'Use of elliptic curves in cryptography'. Advances in Cryptology CRYPTO85 Proc., SantaBarbara, CA, USA, 1986, pp. 417–426

[28] Menezes, A.J., Okamoto, T., Vanstone, S.A.: 'Reducing elliptic curve logarithms to logarithms in a finite field', *IEEE Trans. Inf. Theory*, 1993, **39**, (5), pp. 1639–1646

[29] Hua, S., Aimin, W.: 'A multi-secret sharing scheme with general access structures based on elliptic curve'. 3rd Int. Conf. on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 2010, pp. 629–632, (2), 173–193 (2000)

[30] Meng, X., Li, Y.: 'A novel verifiable threshold signature scheme based on bilinear pairing in mobile *ad hoc* network'. Proc. of the IEEE Int. Conf. on Information and Automation (ICIA'12), Shenyang, China, 2012, pp. 361–366

[31] Fatemi, M., Ghasemi, R., Eghlidos, T.*, et al.*: 'Efficient multistage secret sharing scheme using bilinear map', *IET Inf. Sec.*, 2014, **8**, (4), pp. 224–229

[32] Lin, H.Y., Yeh, Y.S.: 'Dynamic multi-secret sharing scheme', *Int. J. Contemp. Math. Sci.*, 2008, **3**, pp. 37–42

[33] Washington, L.C.: '*Elliptic curves: number theory and cryptography*' (CRC Press, London, New York, 2008)

[34] Diffie, W., Hellman, M.E.: 'New directions in cryptography', *IEEE Trans. Inf. Theory*, 1976, **22**, (6), pp. 644–654