A NEW VERIFIABLE MULTI-SECRET SHARING SCHEME BASED ON ELLIPTIC CURVES AND PAIRINGS

Mojtaba Bahramian
Department of Pure Mathematics
Faculty of Mathematical Sciences
University of Kashan
P. O. Box 87317-53153
Kashan, I. R. Iran
bahramianh@kashanu.ac.ir

Khadijeh Eslami
Department of Pure Mathematics
Faculty of Mathematical Sciences
University of Kashan
P. O. Box 87317-53153
Kashan, I. R. Iran
kh.eslami@grad.kashanu.ac.ir

Abstract. In 2008, Liu, Huang, Luo and Dai, proposed a (t, n) multi-point sharing scheme by using self-pairings on the elliptic curves. The Liu's scheme is not verifiable, needs a secure channel and also there exists some restrictions in the number of secrets to be shared. In this paper we propose a new verifiable multi-secret sharing scheme which is based on that of Liu. In our scheme, there is no need to a secure channel and also there is no limit on the number of secrets. Furthermore, to identify the cheaters, the combiner can verify the secrets which have been sent by other participants during the reconstruction phase.

Keywords: secret sharing, cryptography, elliptic curves, bilinear maps.

1. Introduction

Secret sharing schemes are important tools used in many cryptographic protocols and security techniques. A secret sharing scheme consists of a dealer, who knows a secret, a set P any of whose elements is called a participant, and a family $\mathcal{A}$ of subsets of P, called an access structure. In such a scheme, the dealer distributes shares among the participants in such a way that any $A \in \mathcal{A}$ is able to recover the prescribed secret by pooling its members shares together, whereas any subset of P not lying in $\mathcal{A}$ knows nothing about the secret. If P is of cardinality n, and $\mathcal{A}$ consists of all subsets of P with at least t elements, then the scheme is referred to as a $(t, n)-$threshold secret sharing scheme. Secret sharing schemes can be used in many different domains such as secure data storage, secure multi-party computational, group key management and secure information communication. Secret sharing schemes for general access structures were proposed by Ito, Saito, and Nishizeki [17] in 1993, and more efficient schemes were introduced in, e.g., [1, 2, 5].

The first (t, n)-threshold secret sharing schemes were independently introduced by Shamir [24] and Blakley [3]. Shamir's scheme is based on the Lagrange interpolating polynomial, while Blakley's scheme is based on linear projective geometry.

A Multi-secret sharing (MSS) scheme, is a scheme in which several secrets are shared among participants and when any predetermined subset of them pool their information, they will be able to reconstruct all the secrets. The first MSS scheme was introduced by He and Dawson [15] in 1994, and was improved in e. g., [7, 6, 12, 13, 14, 16, 21]. MSS scheme can be used in many different domains, for example, launching intercontinental ballistic missiles, authenticating electronic transactions and opening a bank vault.

In 1994, Jackson et al. [18] classified the MSS scheme into the following two categories: the one-time-use schemes and the multi-use schemes. In a one-time-use scheme, the dealer updates the information distributed amongst the participants after reconstructing the secrets, while in a multi-use scheme, every participant only needs to keep one shadow and use it iteratively. Because distributing shadows to the participants is costly and difficult, the implementation of multi-use schemes is much better.

It should be noticed that the early secret sharing schemes were initiated on the assumption that both the dealer and participants are honest. However, it is very often in practice that a dishonest dealer distributes a fake shadow or a malicious participant provides the other ones with some fake shares. Hence, to remedy this pathology, the researchers were stimulated to work out the schemes which have the capability of being verified. Indeed, a so-called verifiable secret sharing (VSS) scheme is one in which all the participants are able to verify each other and, of course, the dealer.

The first VSS scheme was introduced in 1985 by chore et. al. [10]. Thenceforward, Harn [14] proposed a verifiable multi-secret sharing (VMSS) scheme in 1995. That immediately turned out to be of high computational costs. In fact, Harn's verification process needs any participant to solve a variety of equations. Chen's scheme [8], introduced in 1997, was one of the next attempts to improve Harn's scheme that, despite being of a partial success, was still a scheme with rather high computational costs. Finally, Shao and Cao [25] introduced a new efficient VMSS scheme based on YCH [29] and the hardness of discrete logarithm problem.

In 2008 Chen et al. [9] proposed a threshold secret sharing scheme based on bilinear maps. Chen's scheme was a single secret sharing scheme based on the idea of constructing a Vandermonde matrix to change the threshold. Chen's scheme was improved to a multi-secret sharing by Wang et al. [27]. They proposed a verifiable (t, n)-threshold multi-secret sharing scheme based on bilinear maps; it was subject to the restriction that the number of secrets should not exceed the threshold. Afterwards, Eslami et al. [11] modified Wang's scheme and proposed a new one which dispelled the aforementioned restriction.

In 2008 Liu et. al. [22] presented a $(t, n)-$threshold multi-secret sharing scheme by using self-pairing on an elliptic curve. It is worth pointing out that the privilege of the usage of elliptic curves stands on the fact that solving discrete logarithm problem over elliptic curves is usually difficult and far-reaching. In Liu's scheme the number of secrets, m, must be less than or equal to the threshold t. Moreover, his scheme is not a verifiable one and, at the same time, needs a secure channel.

In this paper we propose a verifiable (t, n)-threshold multi-secret sharing scheme based on elliptic curves and bilinear maps. The approach we take here is to try to exhibit a modified version of Liu's scheme which, at the same time, eliminates the need to restricting the number of secrets and does not require any secure channel. Moreover, our scheme benefits from the fact that the combiner (who can be one the participants) is also able to verify the shares pooled in the reconstruction phase.

The rest of this paper is organized as follows: In Section 2, we summarize the elementary notions of elliptic curves and bilinear maps. Review of Liu's scheme will be given in Section 3. Finally, Sections 4 and 5 are devoted to the presentation of our scheme besides analysing it and comparing to some of the schemes known in the literature.

2. Preliminaries

In this section, we will briefly provide the necessary background on elliptic curves and bilinear maps. The reader could consult a standard text book on the subject, e. g. [26, 28].

2.1 Elliptic curve cryptography

The elliptic curve cryptography (ECC) was suggested separately by Neal Koblitz [19] and Victor S. Miller [23] in 1985. It should be pointed out that merely the finite fields $\mathbb{F}_q$ where q is either a prime or $q = 2^n$ for some integer n, were firstly involved. Recently, elliptic curve cryptography has attained much attention as it has many advantages like a short key length and fast computation speed. In this subsection, we will give the definitions and some elementary properties of the elliptic curves. An elliptic curve E over the finite field $\mathbb{F}_q$ is defined by Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ and its discriminant, $\Delta = -4a_2^3a_6+a_2^2a_4^2+18a_2a_4a_6-4a_4^3 - 27a_6^2$, is supposed to be nonzero. If q is not dividable by 2 or 3, then by an appropriate change of variables, Eq. (2.1) can be reformulated as the short

Weierstrass form

$$y^2 = x^3 + Ax + B, \tag{2.2}$$

for $A, B \in \mathbb{F}_q$.

The points on an elliptic curve together with an extra point $\mathcal{O}$, which is called the point at infinity, form a finite abelian group with an addition law. Indeed, if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points on E, then set $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

and

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q, \\ \dfrac{3x_1^2 + A}{2y_1}, & P = Q. \end{cases}$$

Discrete logarithm problem on elliptic curves

Throughout, we let q be some power of a prime and let the elliptic curve E be defined by Eq. (2.2). Also, let $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 | y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$. Assume next that $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$, the subgroup generated by P. The discrete logarithm problem on E is to find the integer k satisfying $Q = kP$. In general, there is no polynomial time algorithm on $\log q$ to solve the discrete logarithm problem on $E(\mathbb{F}_q)$. This is why the cryptographic schemes which are based on elliptic curves have become valuable and interesting.

2.2 Bilinear maps

The definition of a bilinear map lies on the following two well-known problems in cryptography; namely CDHP and DDHP. To state these problems, let G be a cyclic additive group of order a prime number r with P as a generator. The so-called computational Diffie-Hellman problem (CDHP) involves computing abP for a given triple (P, aP, bP) with $a, b \in \mathbb{Z}_r^*$. Also the Decision Diffie-Hellman problem (DDHP) concerns the decision on whether $c = ab$ holds for a given quadruple (P, aP, bP, cP) with $a, b, c \in \mathbb{Z}_r^*$.

We say that a group G is a Gap Diffie-Hellman (GDH) group provided DDHP in G is easy to solve while simultaneously, CDHP in G is hard to treat; see [4] for more information.

Let G_1 be a cyclic additive group of order a prime r, and let G_2 be a cyclic multiplicative group of the same order. We assume that the DDHP in G_1 is easy while it is hard in G_2. Suppose moreover that CDHP in G_1 and DLP G_2 are hard to solve. A bilinear map is a map (or a pairing) $e : G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in \mathbb{Z}_r^*$.
2. Non-Degeneracy: there exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

3. Computability: e is efficiently computable, i.e., there exists a polynomial time algorithm to compute $e(P, Q) \in G_2$, for all $P, Q \in G_1$.

Pairing-based cryptography stands over the idea of using the construction and properties of bilinear maps between two suitable groups. The strategy is to exploit such maps to reduce a problem in one of the groups to a problem in the second one in such a way that, compared to the original one, the resulting problem is usually much more convenient to treat.

It should be emphasized that the existence of G_1 and G_2 with these properties follows from Weil pairing [28, 11.2] and Tate pairing [28, 11.3]. Indeed, one can take for G_1 an elliptic curve and for G_2 the underlying field of G_1.

Let K be a field, $\overline{K}$ its algebraic closure and let $E = E(\overline{K})$ be an elliptic curve over $\overline{K}$. For $l \neq 0$, let $E[l]$ denote the subgroup of $l-$torsion points, which contains all the points P with $lP = \mathcal{O}$. If $char(K) = 0$ or $char(K) = p$ where l is not dividable by p, then $E[l]$ can be represented as a direct sum of two cyclic groups namely, $E[l] \cong Z_l \oplus Z_l$. If this is the case, let $\{G, H\}$ be a generating set for $E[l]$. Then any point in $E[l]$ can be represented as a linear combination of G and H. Consider two points P and Q in $E[l]$, so that we have $P = a_1 G + b_1 H$ and $Q = a_2 G + b_2 H$, for integers $a_1, a_2, b_1, b_2 \in [0, l-1]$. We can now define the following pairing map for any two arbitrary integers $\alpha, \beta \in [0, l-1]$:

$$\begin{gathered} e_{\alpha,\beta} : E[l] \times E[l] \to E[l] \\ e_{\alpha,\beta}(P, Q) = (a_1 b_2 - a_2 b_1)(\alpha G + \beta H) \end{gathered} \tag{2.3}$$

The trivial case when $\alpha = \beta = 0$ has been excluded. The pairing $e_{\alpha,\beta}$ is called self-pairing because it maps $E[l] \times E[l]$ to $E[l]$.

We notice that this is the particular pairing by means of which we will define our proposed scheme in Section 4.

Theorem 2.1 ([20],Prop.3.1)**.** *The pairing $e_{\alpha,\beta}$ has the following properties:*

1. *Identity: for all $P \in E[l]$, $e_{\alpha,\beta}(P, P) = \mathcal{O}$.*
2. *Bilinearity: for all $P, Q, R \in E[l]$, $e_{\alpha,\beta}(P+Q, R) = e_{\alpha,\beta}(P, R) + e_{\alpha,\beta}(Q, R)$ and $e_{\alpha,\beta}(P, Q+R) = e_{\alpha,\beta}(P, Q) + e_{\alpha,\beta}(P, R)$.*
3. *Anti-symmetry: for all $P \in E[l]$, $e_{\alpha,\beta}(P, Q) = -e_{\alpha,\beta}(Q, P)$.*
4. *Non-degeneracy: for all $P \in E[l]$, $e_{\alpha,\beta}(P, \mathcal{O}) = \mathcal{O}$. Moreover, if $e_{\alpha,\beta}(P, Q) = \mathcal{O}$ for all $P \in E[l]$, then $Q = \mathcal{O}$.*

3. A Review of Liu's scheme

In this section, we briefly introduce the scheme posed by Liu et. al. in [22] which is actually a scheme for sharing points on an elliptic curve. This scheme consists of the following phases: initialization, shadow distribution, point sharing and point reconstruction. Below, we provide overview of any of these phases.

Let D be a trusted dealer, and let $U_1, U_2, \dots, U_n$ be honest participants. The dealer wants to distribute secrets $M_1, M_2, \dots, M_m$ between the participants such that any group consisting of at least t participants can reconstruct all the secrets, but no group of less than t participants can do.

3.1 Initialization

In Liu's scheme, the dealer publishes public information on a public bulletin which can be accessed by every participant. The dealer uses the following steps to set up the parameters of the sharing scheme.

1. The dealer chooses an elliptic curve E over the finite field $\mathbb{F}_q$ where $q = p^r$, p being a large enough prime for which the DLP and ECDLP are simultaneously hard in $\mathbb{F}_q^*$ and $E(\mathbb{F}_q)$ respectively. The dealer then chooses a large prime l such that $E[l] \subseteq E(\mathbb{F}_{q^k})$ for some integer k.
2. The dealer D chooses a generating set $\{G, H\}$ of $E[l]$ and two integers $\alpha, \beta \in [1, l-1]$, which determine the pairing $e_{\alpha,\beta}$ as defined before.
3. Finally, the dealer publishes $\{E, q, l, k, \alpha G + \beta H\}$ in the public bulletin.

3.2 Shadow distribution

In this phase, the dealer D uses the following steps to distribute the shadows to the participants. As stated before, this should be done in such a way that any group consisting of at least t participants can reconstruct the shared points, but no group with less than t participants can.

1. D considers the matrix A of size $n \times t$ as

$$A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2^2 & \dots & 2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & n & n^2 & \dots & n^{t-1} \end{bmatrix}$$

2. The dealer randomly chooses t pairs of numbers $a'_i, b'_i \in [1, l-1]$ for $1 \le i \le t$.
3. D computes

$$\begin{aligned} (a_1, a_2, \dots, a_n)^T &= A \cdot (a'_1, a'_2, \dots, a'_t)^T, \\ (b_1, b_2, \dots, b_n)^T &= A \cdot (b'_1, b'_2, \dots, b'_t)^T. \end{aligned}$$

4. Finally, D sends (a_j, b_j) to user U_j through a secret channel for all $1 \le j \le n$.

3.3 Point sharing

After distributing the shadows, the dealer shares the points among all the participants through the following steps:

1. To share m different points $M_1, \ldots, M_m$, the dealer chooses $c_i, d_i \in [0, l-1]$ randomly and computes $Q_i = c_i G + d_i H$ for all $1 \leq i \leq m$.
2. The dealer computes $R_i = e_{\alpha,\beta}(Q_i, P'_t) + M_i$, for $1 \leq i \leq m$, where $P'_t = a'_t G + b'_t H$.
3. Finally, the dealer publishes $\{c_i, d_i, R_i\}$, for $1 \leq i \leq m$, in the public bulletin.

3.4 Point reconstruction

Without loss of generality, we may assume by a relabeling that the participants $U_1, U_2, \ldots, U_t$ want to reconstruct the secrets $M_1, M_2, \ldots, M_m$. Each participant computes the pseudo share from his secret share and the public information. The reconstructing procedure is as follows:

1. Each U_j downloads the pair of integers $\{c_i, d_i\}$ from the public bulletin board, where $1 \leq j \leq t$.
2. Each U_j computes $Q_{i,j} = e_{\alpha,\beta}(Q_i, P_j)$, where $P_j = a_j G + b_j H$ and $Q_i = c_i G + d_i H$, for $1 \leq i, j \leq t$.
3. Each U_j multicasts the pseudo shadow $Q_{i,j}$ to $U_1, \ldots, U_{j-1}, U_{j+1}, \ldots, U_t$, for $1 \leq j \leq t$.
4. Each participant U_i computes $T_i = \sum_{k=1}^{t} y_k Q_{i,k}$, where $y_k = (\prod_{j=1, j\neq k}^{t} (k-j))^{-1}$.
5. Each participant U_i downloads the point R_i from the public bulletin and recovers $M_i = R_i - T_i$.

4. Proposed scheme

Recall that the MSS scheme proposed by Liu was based on the elliptic curves cryptography, as pointed out earlier in the paper, is addressed to the fact that solving the discrete logarithm problem on the elliptic curves is really a challenging and far-reaching problem to treat and this provides the scheme with a rather high security in comparison to some of the other ones.

Nevertheless, from several points of view, it suffers from some deficiencies; namely it needs a secure channel, it is not verifiable, and also there exists some restrictions on the number of secrets to be shared. So it seems quite reasonable and natural to deal with new technique in order to make Liu's scheme into a more satisfactory one.

Here, we will make use of the elliptic curves and bilinear pairings to propose a new verifiable (t, n)-threshold MSS scheme. The procedure can be divided into four parts: Initialization phase, Point sharing phase, Point distribution phase, Secret reconstruction and Verification phase.

In our proposed scheme, which is based on that of Liu, we will drop the restriction on the number of secrets. Moreover, each participant will be able to identify cheaters in the reconstruction phase by using bilinear maps, and since any participant chooses his/her secret shadow by him/herself, there is no need to a secure channel and the dealer can never distribute a fake shadow.

Let $U_1, U_2, \ldots, U_n$ be the participants involved in the secret sharing process and let $K_1, K_2, \ldots, K_m$ be the secrets to be shared.

4.1 Initialization phase

In the initialization phase, the dealer D publishes some public information on the public bulletin which is accessible by every participant.

1. The Dealer D chooses an elliptic curve E over $\mathbb{F}_q$, $q = p^r$, where p is a large prime such that the DLP and ECDLP are hard respectively in $\mathbb{F}_q^*$ and $E(\mathbb{F}_q)$. The dealer then chooses $E[l]$, a torsion subgroup of a large prime order l. It is well-known that $E[l] \subseteq E(\mathbb{F}_{q^k})$, for some integer k.

2. D chooses a generating pair $\{G, H\} \subseteq E[l]$ and a pair of integers $\alpha, \beta \in [1, l-1]$. The dealer then forms the pairing (2.3) and then computes $W = \alpha G + \beta H$.

3. The dealer chooses a hash function $h : E[l] \to \mathbb{Z}_l^*$, and finally publishes $\{E, p, l, G, H, W, h\}$ on the public bulletin.

4.2 Point sharing phase

In this step, the dealer may use the following steps to distribute the shadows to the participants; this distribution is subject to the prescribed conditions, as pointed out before.

1. The dealer D maps the secrets $K_1, K_2, \ldots, K_m$ to a set of points $M_1, M_2, \ldots,$ M_m on the elliptic curve E.

2. D chooses private numbers $a_0, a_1, b_0, b_1 \in [1, l-1]$ and computes the points $Q_0 = a_0 G + b_0 H$ and $P_i = a_1^i G + b_1^i H$ for $i = 1, \ldots, m$.

3. Corresponding to the secret M_i, the dealer publishes $R_i = e_{\alpha,\beta}(Q_0, P_i) + M_i$ for $i = 1, \ldots, m$.

4.3 Point distribution phase

1. D chooses some $d \in \mathbb{Z}_l^*$ randomly and publishes $G' = dG$.

2. Each participant U_i selects the secret shadow s_i and publishes $G_i = s_iG$.
3. D considers the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2^2 & \dots & 2^{n+3} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & (n-t+4) & (n-t+4)^2 & \dots & (n-t+4)^{n+3} \end{bmatrix}. \tag{4.1}$$

4. The dealer computes ds_iG, and constructs the column vector $X = [h(ds_1G), h(ds_2G), \dots, h(ds_nG), a_0, b_0, a_1, b_1]^T$.
5. D publishes $[I_1, I_2, \dots, I_{n-t+4}]$ where

$$A \times X = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2^2 & \dots & 2^{n+3} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & (n-t+4) & (n-t+4)^2 & \dots & (n-t+4)^{n+3} \end{bmatrix} \begin{bmatrix} h(ds_1G) \\ \vdots \\ h(ds_nG) \\ a_0 \\ b_0 \\ a_1 \\ b_1 \end{bmatrix}$$

$$= \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_{n-t+4} \end{bmatrix}. \tag{4.2}$$

4.4 Secret reconstruction and verification phase

It is clear that Eq. (4.2) is a system of $(n-t+4)$ linear equations with $(n+4)$ unknowns. To reconstruct all the secrets, we need to know the values of a_0, a_1, b_0 and b_1. Suppose that t-out-of-n participants $U_1, \dots, U_t$ intend to reconstruct all the secrets. To this goal, assume U_i computes ds_iG for $i = 1, \dots, t$. Firstly, the combiner ensures verifiability of the shares by using the bilinearity property of the pairing maps and checks if $e_{\alpha,\beta}(ds_iG, G) = e_{\alpha,\beta}(dG, s_iG)$. Then, the combiner uses the public hash function h to compute $h(ds_iG)$, for $i = 1, \dots, t$ and generates the i-th row of the unknown's matrix. Therefore, t unknowns of Eq. (4.2) are computed and the combiner may now solve a system of $(n-t+4)$ equations and $(n-t+4)$ unknowns to reconstruct a_0, a_1, b_0 and b_1. Finally, the secrets can be obtained by putting $M_i = R_i - e_{\alpha,\beta}(Q_0, P_i)$, for $i = 1, \dots, m$.

5. Security analysis phase

The security analysis of the proposed scheme goes ahead through the following lines.

Theorem 5.1. *Any t or more participants are able to reconstruct all the secrets.*

Proof. Without loss of generality, we suppose that $U_1, U_2, \ldots, U_t$ share their secret shadows ds_iG for $i = 1, \ldots, t$. Then, Eq. (4.2) converts to a system of $n-t+4$ equations and $n-t+4$ unknowns with the invertible coefficients matrix

$$A' = \begin{bmatrix} 1 & \ldots & 1 \\ 2^t & \ldots & 2^{n+3} \\ \vdots & & \vdots \\ (n-t+4)^t & \ldots & (n-t+4)^{n+3} \end{bmatrix}. \tag{5.1}$$

(Indeed, the determinant of A' might be calculated via $det(A') = 2^t \times \cdots \times (n-t+4)^t \times det(A'')$, for some Vandermonde matrix A''.) Hence, the participants obtain the secrets by computing the inverse matrix of A'. □

Theorem 5.2. *Any group of less than t participants cannot compute any of the secrets.*

Proof. Suppose, to the contrary, that this is the case. Then Eq. (4.2) reduces to a system of $n-t+4$ equations and more than $n-t+4$ unknowns which has certainly an infinite set of solutions. □

The following theorem ensures that using a secure channel in order to share the secrets is in fact not mandatory.

Theorem 5.3. *The proposed scheme does not require a secure channel.*

Proof. We must make sure that no participant's shadow s_i might be grasped from s_iG. In fact, if an attacker wants to compute s_i from s_iG, he/she must solve a discrete logarithm problem in the elliptic curve E, which is hard according to our assumptions. □

Theorem 5.4. *The dealers private key d cannot be obtained from the public information dG.*

Proof. The theorem follows from the argument provided in Theorem 5.3. □

Finally, Theorem 5.5 below illustrates the verifiability of the proposed scheme.

Theorem 5.5. *The shares provided by the participants in the reconstruction phase can be verified.*

Proof. Suppose that the participant U_i provides ds_iG. During the reconstruction phase, this share can be verified, because as mentioned before, given s_iG and dG, it is infeasible to compute ds_iG in E; this follows from the hardness of the Diffie-Hellman problem. Therefore, only the dealer and the participant U_i are able to compute this value. By using the bilinearity property of the pairing maps, the combiner can check whether $e_{\alpha,\beta}(ds_iG, G) = e_{\alpha,\beta}(dG, s_iG)$ holds. If the verification passes, he/she accepts ds_iG. □

Table 1 provides a comparison between the proposed scheme in this paper and some other one's that are based on the techniques of elliptic curves and pairings.

Table 1: Comparison of some schemes based on elliptic curve and pairing

Scheme	Chen [9]	Liu [22]	Wang [27]	Proposed
Multi-secret	No	Yes	Yes	Yes
Number of secrets	1	t	t	unrestricted
Public parameters	$2n - t + 9$	$3m + 5$	$2n + 7$	$2n + m - t + 11$
Verifiability	Yes	No	Yes	Yes
Cheater detection	Yes	No	No	Yes
Cheater identification	Yes	No	No	Yes
Need a secure channel	No	Yes	No	No

Acknowledgments

This research was in part supported by the University of Kashan under grant number 682460/003.

References

[1] J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, In S. Goldwasser, editor, Advances in Cryptology - CRYPTO'88, 403 of Lecture Notes in Computer Science, 1990, 27-35.

[2] M. Bertilsson and I. Ingemarsson, *A construction of practical secret sharing schemes using linear block codes*, In J. Seberry and Y. Zheng, editors, Advances in Cryptology - AUSCRYPT '92, volume 718 of Lecture Notes in Computer Science, 1993, 67-79.

[3] G. Blakley, *Safeguarding cryptographic keys*, in: Proc. AFIPS Natl. Conf., New York, 1979, 313-317.

[4] D. Boneh, *The decision diffie-hellman problem*, In Algorithmic number theory, 1998, 48-63.

[5] E. F. Brickell, *Some ideal secret sharing schemes*, Journal of Combin. Math. and Combin. Comput., 6 (1989), 105-113.

[6] C.W. Chan and C.C. Chang, *A scheme for threshold multi-secret sharing*, Applied Mathematics and Computation, 166 (2005), 1-14.

[7] T.Y. Chang, M.S. Hwang and W.P. Yang, *A new multi-stage secret sharing scheme using one-way function*, ACM SIGOPS Operating Systems, 39 (2005), 48-55.

[8] L. Chen, D. Gollman, C.J. Mitchell and P. Wild, *Secret sharing with reusable polynomials*, Proceeding of the Second Australasian Conference on Information Security and Privacy-ACISP'97[C], ACISP, Australia, 1997.

[9] W. Chen, X. Long, Y. B. Bai, and X. P. Gao, *A new dynamic threshold secret sharing scheme from bilinear maps*, In International Conference on Parallel Processing Workshops 19, 2007.

[10] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, *Verifiable secret sharing and achieving simultaneity in the presence of faults [A]*, Proc of 26th IEEE Symposium on Foundations of Computer Science [C], IEEE, Portland, (1985), 251-260.

[11] Z. Eslami and S. K. Rad, *A new verifiable multi-secret sharing scheme based on bilinear maps*, Wireless Personal Communications, 63(2) (2012), 459-467.

[12] M. Fatemi, T. Eghlidos and M. Aref, *A multi-stage secret sharing scheme using all-or-nothing transform approach*, ICICS'09, LNCS, 5927 (2009), 449-458.

[13] L. Harn, *Comment: multistage secret sharing based on one-way function*, Electronics Letters, 31 (1995), 62-262.

[14] L. Harn, *Effcient sharing (broadcasting) of multiple secrets*, Proceeding of the IEE Comput. Digit. Tech., 142 (1995), 237-240.

[15] J. He and E. Dawson, *Multi-stage secret sharing scheme based on one-way function*, Electronic Letters, 30 (1994), 1591-1592.

[16] J. He and E. Dawson, *Multisecret-sharing scheme based on one-way function*, Electronic Letters, 31 (1995), 93-95.

[17] M. Ito, A. Saito, and T. Nishizeki, *Secret sharing schemes realizing general access structure*, In Proc. of the IEEE Global Telecommunication Conf., Globecom 87, 99-102, 1987. Journal version: Multiple assignment scheme for sharing secret. J. of Cryptology, 6 (1993), 15-20.

[18] W. A. Jackson, K.M. Martin and C.M. O'Keefe, *On sharing many secrets*, Asiacrypt, 94 (1994), 42-54.

[19] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, 48 (1987), 203-209.

[20] H. S. Lee, *A self-pairing map and its applications to cryptography*, Applied Mathematics and Computation, 151 (2004), 671-678.

[21] H.X. Li, C.T. Cheng and L.J. Pang, *An Improved Multi-Stage (t,n)-Threshold Secret Sharing Scheme*, WAIM05, Fan W., Wu Z., and Yang J., eds., LNCS, 3739 (2005), 267-274.

[22] D. Liu, D. Huang, P. Luo and Y. Da, *New schemes for sharing points on an elliptic curve*, Computers and Mathematics with Applications, 56 (2008), 1556-1561.

[23] V. Miller, *Use of elliptic curves in cryptography*, CRYPTO, Lecture Notes in Computer Science, 85 (1985), 417-426.

[24] A. Shamir, *How to share a secret*, Communications of the ACM, 22 (1979), 612-613.

[25] J. Shao and Z. F. Cao, *A new efficient (t,n) verifiable multi-secret sharing (VMSS) based on YCH scheme*, Applied Mathematics and Computation, 168 (2005), 135-140.

[26] J. H. Silverman, *The arithmetic of elliptic curves, Graduate Texts in Mathematics*, Springer-Verlag, New York, 106, 1986.

[27] S. J. Wang, Y. R. Tsai and C. C. Shen, *Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ecc*, Wireless Personal Communications, 56 (2011), 173-182.

[28] L. C. Washington, *Elliptic curves, number theory and cryptography*, CRC Press, Boca Raton, 2008.

[29] C. C. Yang, T. Y. Chang and M. S. Hwang, *A (t,n) multi-secret sharing scheme, Applied Mathematics and Computation*, 151 (2004), 483-490.

Accepted: 18.06.2018