Journal of Algebraic Structures and Their Applications
ISSN: 2382-9761
www.as.yazd.ac.ir

Algebraic Structures and Their Applications Vol. 4 No. 2 (2017) pp 45-55.

AN EFFICIENT THRESHOLD VERIFIABLE MULTI-SECRET SHARING SCHEME USING GENERALIZED JACOBIAN OF ELLIPTIC CURVES

MOJTABA BAHRAMIAN* AND KHADIJEH ESLAMI

Communicated by B. Davvaz

Abstract. In a (t, n)-threshold secret sharing scheme, a secret s is distributed among n participants such that any group of t or more participants can reconstruct the secret together, but no group of fewer than t participants can do. In this paper we propose a verifiable (t, n)-threshold multi-secret sharing scheme based on Shao and Cao, and the intractability of the elliptic curve discrete logarithm problem (ECDLP) by using generalized Jacobian of elliptic curves. The proposed scheme has all the benefits of Shao and Cao, however, our scheme no need to a secure channel. Furthermore, we exploit the techniques via elliptic curves to perform the scheme. This can be very important, because the hardness of discrete logarithm problem on elliptic curves increases security of the proposed scheme.

1. Introduction

Secret sharing is a method for distributing one or more secrets by a person, named dealer, among a group of participants, such that only a predetermined subset of participants are able

DOI:http://dx.doi.org/10.29252/asta.4.2.45

MSC(2010): Primary: 94A62; Secondary: 14H52, 14H40.

Keywords: Secret Sharing, Elliptic Curves, Generalized Jacobians.

Received: 29 November 2017, Accepted: 18 July 2018

*Corresponding author

to recover the secret(s) and other categories don't have this ability.

In 1979 the first (t, n)-threshold secret sharing scheme was introduced by Shamir [14] and Blakley [3]. Shamir's secret sharing scheme is based on the Lagrange interpolating polynomial and Blakley's secret sharing scheme is based on linear projective geometry. In a (t, n)-threshold secret sharing scheme, a secret s is divided into n pieces $s_1, s_2, \cdots, s_n$ by the dealer and distributed among n participants such that any group of t or more participants can together reconstruct the secret, but no group of fewer than t participants can.

One of the problems in this schemes is that only one secret can be shared by dealer during every secret sharing process. Multi-secret sharing (MSS) is a new type of secret sharing in which several secrets are shared. The strategy is that multiple secrets are shared among several participants and any authorized subset of them will be able to recover it by pooling their information together. Another problem is that, in these secret sharing methods we assume that the dealer and the participants are honest but this may happens that a dishonest dealer distributes a fake shadow to the participants, or even that a cheater participant provides the others with a fake share.

This problem has been solved by Chore in [5] by presenting the verifiable secret sharing method, (VSS). Also, this secret sharing method is the one-time-use scheme. After a secret is reconstructed, the dealer must redistribute new shadow to every participant over a secure channel.

Furthermore, in 1995 Harn [8] and in 1997 Chen et al. [4] presented the verifiable multi-secret sharing method (VMSS). The disadvantage of their scheme is that, in order to check the validity of the secret, every participant has to verify a large number of equations. Benaloh and Leichter [1] and Ito, Saito, and Nishizeki [9] described a more general method of secret sharing. They showed how to realize a secret sharing scheme for any access structure, where an access structure is a family of all subsets of participants that are able to reconstruct the secrets.

In 2004, Yang et al. proposed a (t, n)-threshold multi-secret sharing scheme based on Shamir [18]. Shao and Cao added the verifiable property into Yang's scheme and presented a method based on the hardness of discrete logarithm problem in the multiplicative group of a finite field [15]. The aforementioned schemes need a secure channel to transfer the secrets to participants by the dealer. In this article we present a new approach, which follows closely that of Shao and Cao, that aims particularly at dropping the need to a secure channel in order to share a secret. Furthermore, we exploit the techniques via elliptic curves to prove the way towards our goal, so the hardness of discrete logarithm problem on elliptic curves, increases security of the proposed scheme.

In this direction, let as remark that elliptic curves have proved fruitful in cryptographic schemes and secret sharing in particular. For instance Liu et al. in [11] presented a new (t, n)-threshold multi-point sharing scheme using self-pairing on an elliptic curve. Also in 2015, V. P. Binu and A. Sreekumar [2] described a threshold multi-secret sharing scheme based on elliptic curves and bilinear pairing. They have used the method of point sharing and verification using self-pairing.

In order to provide a more comprehensive statement of our proposed approach, we just make a very brief overview of the methods applied by Shao and Cao.

1.1. **Review of Shao and Cao Scheme.** Our scheme is based on that of Shao and Cao [15]. In this section, we briefly introduce a scheme in which the dealer D wants to distribute secrets $P_0, P_1, \cdots, P_{k-1}$ between participants in such a way that any group of t participants can make all the secrets reconstruction.

Definition 1.1. The function $f(r, s)$ is called a two-variable one-way function, when it has the following properties:

(1) Given r and s, it is easy to compute $f(r, s)$;
(2) Given s and $f(r, s)$, it is hard to compute r;
(3) Having no knowledge of s, it is hard to compute $f(r, s)$ for any r;
(4) Given s, it is hard to find two different values r_1 and r_2 such that $f(r_1, s) = f(r_2, s)$;
(5) Given r and $f(r, s)$, it is hard to compute s;
(6) Given pairs of r_i and $f(r_i, s)$, it is hard to compute $f(r, s)$ for $r \neq r_i$.

We explain some notations of Shao and Cao: the function $f(r, s)$ denotes any two-variable one-way function that maps a secret shadow s and a value r into a bit string $f(r, s)$ of a fixed length. We put $P_0, P_1, \cdots, P_{k-1}$ as, k secrets to be shared among n participants, p is a safe prime, and g is a generator of order q of $GF(p)$, where q is a big prime such that $q \mid p - 1$. At first the dealer randomly chooses n distinct secret shadows $s_1, s_2. \cdots, s_n$ and distributes them among participants by a secure channel. Then, he randomly chooses an integer r and computes $f(r, s_1), f(r, s_2), \cdots, f(r, s_n)$.

1.1.1. *Construction phase.* The dealer will perform the following steps:

(1) If $k \leq t$
   - Chooses a prime q and constructs $(t-1)-$th degree polynomial $h(x) \mod q$, as follows; here $0 < P_0, P_1, \cdots, P_{t-1} < q$

     $$h(x) = P_0 + P_1 x + \cdots + P_{k-1} x^{k-1} + P_k x^k + \cdots + P_{t-1} x^{t-1} \mod q;$$

   - Computes $y_i = h(f(r, s_i)) \mod q$ for $i = 1, 2, \cdots, n$;
   - Computes $G_i = g^{p_i} \mod p$ for $i = 0, 1, \cdots, t-1$;

- Publishes $\{r, y_1, y_2, \cdots, y_n, G_0, G_1, \cdots, G_{t-1}\}$;
- Participant i verifies the validity of his/her shadow by checking the following equation:

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

(2) If $k > t$

- Chooses a prime q and construct $(k-1)$th degree polynomial $h(x) \mod q$, where $0 < P_0, P_1, \cdots, P_{k-1} < q$ as follows

$$h(x) = P_0 + P_1 x + \cdots + P_{k-1} x^{k-1} \mod q,$$

- Computes $y_i = h(f(r, s_i)) \mod q$ for $i = 1, 2, \cdots, n$;
- Computes $h(i) \mod q$ for $i = 1, 2, \cdots, k-t$;
- Computes $G_i = g^{p_i} \mod p$ for $i = 0, \cdots, k-1$;
- Publishes $\{r, y_1, y_2, \cdots, y_n, h(1), h(2), \cdots, h(k-t), G_0, G_1, \cdots, G_{k-1}\}$;
- Participant i verifies the validity of his/her shadow by checking the following equation:

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

1.1.2. *Recovery and verification phase.* When t participants pool their unreal shadows $f(r, s_i)$ for $i = 1, 2, \cdots, t$, each participant can check whether the other's secret shadows are valid by the following equations:

(1) If $k \leq t$

$$g^{y_j} = \prod_{l=0}^{t-1} (G_l)^{f(r,s_j)^l} \mod p, \ (j = 1, 2, \cdots, i-1, i+1, \cdots, t).$$

(2) If $k > t$

$$g^{y_j} = \prod_{l=0}^{k-1} (G_l)^{f(r,s_j)^l} \mod p, \ (j = 1, 2, \cdots, i-1, i+1, \cdots, t).$$

In this level we use the Lagrange interpolation polynomial to uniquely determine the polynomial $h(x)$ as follows:

(1) If $k \leq t$

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

(2) If $k > t$

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

In addition, the participants can check the validity of the secrets by the equation:

$$G_i = g^{P_i}, (i = 0, 1, \cdots, k-1).$$

1.2. **Elliptic Curves.** The use of elliptic curves in cryptography was suggested separately by Neal Koblitz [10] and Victor S. Miller [12] in 1985. Here, we will give the definitions and some properties of elliptic curves. For more information see [16] and [17].

Let K be a field. An elliptic curve E over K is the set of solutions $(x, y) \in \overline{K}^2$, where

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

is a smooth plane cubic curve and $a_1, a_2, a_3, a_4, a_6 \in K$, together with an extra point $\mathcal{O}$, which called the point at infinity. If $char(K) \neq 2, 3$, then the elliptic curve E has Weierstrass equation of the form $y^2 = x^3 + Ax + B$, where $4A^3 + 27B^2 \neq 0$. The $K-$rational points of E are the points on E whose coordinates all lie in K, together with the point at infinity. The set of $K-$rational points of E is denoted by $E(K)$. The elliptic curve E has an abelian group structure, $E(K)$ being a subgroup of it.

Group law. Let E be an elliptic curve over K, defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E. The addition $P_3 = P_1 + P_2 = (x_3, y_3)$ is defined as follows:

- If $x_1 = x_2$ and $y_1 \neq y_2$, then $P_3 = \mathcal{O}$.
- If $x_1 \neq x_2$, then $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.
- If $P_1 = P_2$ and $y_1 = 0$, then $P_3 = \mathcal{O}$.
- If $P_1 = P_2$, and $y_1 \neq 0$, then $x_3 = \lambda^2 - 2x_1$ and $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = \frac{3x_1^2 + A}{2y_1}$.

Hasse's theorem [16, V. Theorem 1.1] provides a bound on the order of the group associated to any elliptic curve over the finite field $\mathbb{F}_q$. This theorem says that the order of $E(\mathbb{F}_q)$ satisfies $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$. The quantity $a = q + 1 - \#E(\mathbb{F}_q)$ is called the trace of $E(\mathbb{F}_q)$.

Discrete Logarithm Problem on Elliptic Curves. Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$ and $P, Q \in E(\mathbb{F}_q)$, where $Q = kP$ for some integer k. The discrete logarithm problem on E aims at finding k. In general there is no polynomial time algorithm on $\log q$ to solve discrete logarithm problem on $E(\mathbb{F}_q)$. So, the hardness of discrete logarithm problem is the basis for the cryptographic schemes based on elliptic curves.

1.3. **Generalized Jacobian of Elliptic Curves.** Let E be an elliptic curve defined over an algebraically closed field K. The divisor group of E is the free abelian group generated by the points of E and is denoted by $Div(E)$. For a divisor $D = \sum_{P\in E} n_P(P)$, the degree and the support of D are defined by $\deg(D) = \sum_{P\in E} n_P$ and $supp(D) = \{P \in E \mid n_P \neq 0\}$, respectively. The set $Div^0(E)$ which contains all divisors of zero degree, is a subgroup of $Div(E)$. The divisor of a function $f \in \overline{K}(E)^*$, is defined as $div(f) = \sum_{P\in E} ord_P(f)(P)$, where $ord_P(f)$ is the order of f at the point P. A divisor D is called principal if $D = div(f)$ for some $f \in \overline{K}(E)^*$. The set of all principal divisors, $princ(E)$, is a subgroup of $Div^0(E)$. The quotient group $\frac{Div^0(E)}{Princ(E)}$ is called the Picard group or Jacobian group of E and is denoted by $Pic^0(E)$. We say that two divisors D and D' are linearly equivalent, $D \sim D'$, if $D-D' = div(f)$ for some $f \in K(E)^*$.

Now, let $\mathfrak{m} = \sum_{p\in E} m_P(P) \in Div(E)$ be an effective divisor (i.e., $m_P \geq 0$ for all $P \in E$), and let D and D' be two divisors of disjoint support with $\mathfrak{m}$. D and D' are said to be $\mathfrak{m}-$equivalent, $D \sim_{\mathfrak{m}} D'$, if there exists a function $f \in K(E)^*$ such that $div(f) = D - D'$ and $ord_P(1 - f) \geq m_P$ for each $P \in Supp(\mathfrak{m})$. It is clear that if D and D' are $\mathfrak{m}-$equivalent, then they are linearly equivalent.

Let $Div_{\mathfrak{m}}(E)$ be the subgroup of $Div(E)$ containing all divisors of E of disjoint support with $\mathfrak{m}$ and let $Div^0_{\mathfrak{m}}(E)$ be the subgroup of all divisors of $Div_{\mathfrak{m}}(E)$ which have zero degree. Also, let $Princ_{\mathfrak{m}}(E)$ be the subset of $Princ(E)$, contains all divisors which are $\mathfrak{m}-$equivalent to the zero divisor. It is clear that $Princ_{\mathfrak{m}}(E)$ is a subgroup of $Div^0_{\mathfrak{m}}(E)$. The quotient group $\frac{Div^0_{\mathfrak{m}}(E)}{Princ_{\mathfrak{m}}(E)}$ is called the generalized Jacobian group of E and is denoted by $Pic^0_{\mathfrak{m}}(E)$. In [13] Rosenlicht proved that there exists a commutative algebraic group $J_{\mathfrak{m}}(E)$ isomorphic to the group $Pic^0_{\mathfrak{m}}(E)$, such that if $\mathfrak{m} \neq 0$, then the dimension of $J_{\mathfrak{m}}(E)$ equals $\deg(\mathfrak{m})$. The algebraic group $J_{\mathfrak{m}}(E)$ is called the generalized Jacobian of E with respect to the modulus $\mathfrak{m}$. Dechene in [7] proved that if $\mathfrak{m} = (M) + (N)$ for distinct non-zero points $M, N \in E$, then there is a bijection of sets between $J_{\mathfrak{m}}(E)$ and $K^* \times E$. In other words, each element of $J_{\mathfrak{m}}(E)$ can be represented as a pair (k, P), where $k \in K^*$ and $P \in E$. Also if $(k_1, P_1), (k_2, P_2) \in J_{\mathfrak{m}}(E)$ such that $P_1, P_2, \pm(P_1 + P_2) \notin \{M, N\}$, then $(k_1, P_1) + (k_2, P_2) = (k_1k_2c_{\mathfrak{m}}(P_1, P_2), P_1 + P_2)$, where $c_{\mathfrak{m}}(P_1, P_2) = \frac{L_{P_1,P_2}(M)}{L_{P_1,P_2}(N)}$, $L_{P_1,P_2} = \frac{l_{P_1,P_2}}{l_{P_1+P_2,\mathcal{O}}}$, and $l_{P,Q}$ denotes the equation of the straight line passing through P and Q (tangent at the curve if $P = Q$). In other words, $div(L_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (\mathcal{O})$.

Now let $\alpha_t(P)$ be the first component of $t(1,P)$, for $(1,P) \in J_{\mathfrak{m}}(E)$ and the integer t. Then we have

$$\alpha_t(P) = c_{\mathfrak{m}}(P,P)c_{\mathfrak{m}}(P,2P)\cdots c_{\mathfrak{m}}(P,(t-1)P).$$

The following lemma, proved in [6], will be crucial in our proposed scheme.

Lemma 1.2. *Let P be a point of E and let m,n be integers. Then*

(1) $\alpha_{m+n}(P) = \alpha_m(P)\alpha_n(P)c_{\mathfrak{m}}(mP,nP)$,
(2) $\alpha_{mn}(P) = \alpha_n(P)^m\alpha_m(nP) = \alpha_m(P)^n\alpha_n(mP)$.

2. Proposed Scheme

We use D, $\{U_1,\cdots,U_n\}$, and $\{s_1,\cdots,s_n\}$ to denote the Dealer, set of participants, and set of secret shadows respectively. Also, $f(r,s), P_0, P_1, \cdots, P_{k-1}$ are the same as those of Shao and Cao scheme.

- The dealer chooses elliptic curve E over the finite field F_p such that the discrete logarithm problem in $J_{\mathfrak{m}}$ is infeasible.
- The dealer randomly chooses an integer d as private key and selects a point $G = (a,P) \in J_{\mathfrak{m}}$ of prime order q for $a \in \mathbb{F}_p^*$ and $P \in E$. Then, he computes $T = dG = (a^d\alpha_d(P), dP)$.
- Dealer D publishes $\{\mathbb{F}_p, J_m, T, G\}$.

2.1. Initialization Protocol.

In this level:

(1) Each participant U_i randomly chooses values $n_i \in \mathbb{Z}$ and $s_i \in \mathbb{F}_p^*$. n_i is his/her private key and s_i is his/her secret shadow.
(2) Participant U_i computes $G_i = n_iG = (a^{n_i}\alpha_{n_i}(P), n_iP)$ and $T_i = n_iT = (a^{n_id}\alpha_{n_id}(P), n_idP)$. Let W_i be the first component of T_i. He/She computes $E_i = s_iW_i$ and finally broadcasts (G_i, E_i).
(3) By using his/her own private key d and (G_i, E_i) the dealer computes: $dG_i = d(a^{n_i}\alpha_{n_i}(P), n_iP) = (a^{n_id}\alpha_{n_id}(P), n_idP)$ and $s_i = E_iW_i^{-1}$.
(4) The dealer accepts s_i, when D ensures that $s_i \neq s_j$ for all $i \neq j$. If $s_i = s_j$ for $i \neq j$, then D should tell these participants to choose another secret shadows until s_i's are different for $i = 1,2,\cdots,n$.
(5) The dealer chooses an integer r randomly and computes $f(r,s_i)$ for $i = 1,2,\cdots,n$.

2.2. Construction Protocol.

In this level the dealer performs the following steps:

(1) If $k \leq t$

- Chooses a prime q and constructs $(t-1)-$th degree polynomial $h(x) \mod q$ as follows; here $0 < P_0, P_1, \cdots, P_{k-1} < q$ are k secrets to be shared and $0 < P_k, P_{k+1}, \cdots, P_{t-1} < q$ are randomly chosen:

$$h(x) = P_0 + P_1 x + \cdots + P_{k-1}x^{k-1} + P_k x^k + \cdots + P_{t-1}x^{t-1} \mod q.$$

- Computes $y_i = h(f(r, s_i)) \mod q$ for $i = 1, 2, \cdots, n$.
- Computes $C_i = P_i G \mod p$ for $i = 0, 1, \cdots, t-1$.
- Publishes $\{r, y_1, y_2, \cdots, y_n, C_0, C_1, \cdots, C_{t-1}\}$.
- Participant i checks the equation:

$$y_i G = \sum_{j=0}^{t-1} f(r, s_i)^j C_j \mod p$$

to verify whether his/her secret shadow is valid.

(2) If $k > t$

- Chooses a prime q and constructs $(k-1)-$th degree polynomial $h(x) \mod q$ as follows; here $0 < P_0, P_1, \cdots, P_{k-1} < q$,

$$h(x) = P_0 + P_1 x + \cdots + P_{k-1}x^{k-1} \mod q.$$

- Computes $y_i = h(f(r, s_i)) \mod q$ for $i = 1, 2, \cdots, n$.
- Computes $h(i) \mod q$ for $i = 1, 2, \cdots, k-t$.
- Computes $C_i = P_i G \mod p$ for $i = 0, 1, \cdots, k-1$.
- Publishes $\{r, y_1, y_2, \cdots, y_n, h(1), h(2), \cdots, h(k-t), C_0, C_1, \cdots, C_{k-1}\}$.
- Participant i checks the equation

$$y_i G = \sum_{j=0}^{k-1} f(r, s_i)^j C_j \mod p$$

to verify whether his/her secret shadow is valid.

In this scheme, each participant chooses his/her shadow by himself/herself, so the dealer absolutely can't distribute fake shadows.

2.3. **Verification and Recovery Protocol.** Suppose t participants pool their unreal shadows $f(r, s_i)$ for $i = 1, 2, \cdots, t$ and each participant can check whether others' secret shadows are valid by the following equations:

(1) If $k \leq t$

$$y_j G = \sum_{l=0}^{t-1} f(r, s_j)^l C_l \mod p, \ (j = 1, 2, \cdots, i-1, i+1, \cdots, t).$$

(2) If $k > t$

$$y_j G = \sum_{l=0}^{k-1} f(r, s_j)^l C_l \mod p, \ (j = 1, 2, \cdots, i-1, i+1, \cdots, t).$$

In this level we use the Lagrange interpolation polynomial to uniquely determine the polynomial $h(x)$ as follows:

(1) If $k \leq t$

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

(2) If $k > t$

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

3. Performance and Security Analysis

In our scheme we have the following advantages:

- There is not any need to a secure channel between the dealer and participants.
- Each participant chooses himself/herself secret shadow, so it is impossible to distribute a fake shadow by the dealer.
- Our scheme also resist the participants' cheating behavior.
- Our scheme, needs to only publish $(n + t + 1)$ or $(2k + n - t + 1)$ values, where $k \leq t$ or $k > t$ respectively.
- Any subset of $(t - 1)$ (or fewer) participants can't recover the secrets.
- The dealer's secret information d cannot be obtained from public information $T = dG$, because if an attacker wants to compute d, he/she must solve an instance of the generalized Jacobian discrete logarithm problem which is hard by our assumption on the choice of the group.
- No attacker can try to obtain the participant's secret shadows s_i from given $f(r, s_i)$ and r, since it is very hard due to the property of two-variable one-way function.
- The participants' secret shadows s_i cannot be obtained from $E_i = s_i W_i$.
- If an attacker wants to obtain $P_0, P_1, \cdots, P_{k-1}$ from the public information $C_i = P_i G$, he/she would have to solve the generalized Jacobian discrete logarithm problem, which is assumed to be computationally hard.

TABLE 1. Comparison of some schemes

Scheme	Yang[18]	Shao and Cao[15]	Proposed
Multi-secret	Yes	Yes	Yes
Verifiability	No	Yes	Yes
No secure channel is needed	No	No	Yes
Underlying group	$\mathbb{F}_q^*$	$\mathbb{F}_q^*$	Elliptic Curve

Table 1 provides a comparison between the proposed scheme in this paper and some other schemes.

4. Acknowledgments

This research is partially supported by the University of Kashan under grant number 682460/002.

References

[1] C. Benaloh and J. Leichter, Generalized Secret Sharing and Monotone Functions, *Advances in Cryptology-CRYPTO' 88*, S. Goldwasser Ed., Lecture Notes in Computer Science, **403**, Springer-Verlag, Berlin, (1990), 27-35.

[2] V. P. Binu and A. Sreekumar, Threshold Multi Secret Sharing Using Elliptic Curve and Pairing, *International Journal of Information Processing*, **9**(4), (2015), 100-112.

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

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

[5] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, *26th Annual Symposium on Foundations of Computer Science*, IEEE, (1985), 383-395.

[6] H. Daghigh and M. Bahramian, Generalized Jacobian and Discrete Logarithm Problem on Elliptic Curves, *Iranian Journal of Mathematical Sciences and Informatics*, **4**(2), (2009), 55-64.

[7] I. Dechene, Arithmetic of generalized Jacobians,*Algorithmic Number Theory Symposium ANTS VII* (eds. F. Hess, S. Pauli and M. Post), **4076**, Springer-Verlag, (2006), 421-435.

[8] L. Harn, Efficient sharing (broadcasting) of multiple secrets [J], IEE Proc. Comput. Digit. Tech. **142**(3), (1995), 237-240.

[9] M. Ito, A. Saito, and T. Nishizeki, Secret Sharang Scheme Realizing General Access Structure, *Proceedings of IEEE Global Telecommunications Conference, Globecom 87, Tokyo, Japan*, (1987), 99-102.

[10] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48**(177), (1987), 203-209.

[11] 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.

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

[13] M. Rosenlicht, Generalized Jacobian varieties, *Annals of Mathematics*, **59**, (1954), 505-530.

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

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

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

[17] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, 2008.

[18] C.C. Yang, T.Y. Chang and M.S. Hwang, A (t, n) multi-secret sharing scheme* 1, *Applied Mathematics and Computation* **151** (2) (2004) 483-490.

Mojtaba Bahramian

Department of Pure Mathematics,

Faculty of Mathematical Sciences,

University of Kashan,

Kashan, I. R. Iran

bahramianh@kashanu.ac.ir

Khadijeh Eslami

Department of Pure Mathematics,

Faculty of Mathematical Sciences,

University of Kashan,

Kashan, I. R. Iran

kh.eslami@grad.kashanu.ac.ir