Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 3, pp. 811–831
DOI : 10.47974/JIOS-1362

Compartmented multi-secret sharing scheme using elliptic curves

Mohan Chintamani [§]
School of Mathematics and Statistics
University of Hyderabad
Hyderabad 500046
Telangana
India

Prabal Paul [†]
Department of Mathematics
Birla Institute of Technology and Science Pilani
K K Birla Goa Campus
Goa 403726
India

Laba Sa [*]
School of Mathematics and Statistics
University of Hyderabad
Hyderabad 500046
Telangana
India

Abstract

Secret sharing is a tool that we use in numerous cryptographic protocols. In this paper, we have proposed a multi-secret sharing scheme using elliptic curves and bilinear pairings. Accordingly, we have also proposed a compartmented multi-secret sharing scheme. The schemes are verifiable and efficient. The fundamental reason for utilizing bilinear pairing with elliptic curves is to provide similar security (as in existing schemes) with smaller key sizes. The computational complexities of the proposed schemes have been determined. We have included explicit examples of the schemes using SageMath.

Subject Classification (2010): *94A60, 11T71.*

Keywords: *Elliptic curves, Bilinear pairings, Secret sharing, Compartmented access structure.*

[§] *E-mail:* **mohansspecial@gmail.com**
[†] *E-mail:* **prabal.paul@gmail.com**
[*] *E-mail:* **labasspecial@gmail.com (Corresponding Author)**

© Taru Publications

1. Introduction

Secret sharing scheme is now a vast area in the field of cryptography. It is a tool that is used in numerous cryptographic protocols. Secret sharing is typically used to lack confidence in a single individual or where a single person's duty must be assigned to a group of users when the person is absent. An access structure for a secret sharing scheme defines all subsets of users who can collectively recover the secret by pooling their individual shares. Any unauthorized set of users must not know any information about the secret. Many secret sharing schemes have been proposed in the literature, (see [2, 6, 15, 21], for example).

In a multi-secret sharing scheme (see [14, 18], for example), many secrets are distributed among the users in such a way that any authorized subset of users can reconstruct all the secrets. However, any unauthorized subset of users gets no information about any of the secrets. We study a multi-secret sharing scheme by D. Liu, D. Huang, P. Luo, and Y. Dai [14]. Accordingly, we have proposed a threshold multi-secret sharing scheme using elliptic curves and bilinear pairings. It uses a matrix whose any threshold number of rows forms a Vandermonde matrix [19]. In Liu et al. scheme, the number of secrets to be shared is limited to the threshold. In our scheme, any number of secrets can be shared among the users.

Secret sharing schemes for compartmented access structures must be carefully designed. In 1990, G. Simmons [23] introduced a compartmented secret sharing scheme. In a compartmented access structure, users are divided into disjoint compartments. If the total number of participants exceeds a global threshold and the number of participants from each compartment exceeds a predetermined compartment threshold, the secret can be reconstructed. Many compartmented secret sharing schemes have been proposed using polynomials [9, 20, 27] and Chinese Remainder Theorem [10], and many others [3, 4, 7, 24–26]. The method is advantageous when data has to be securely saved in a database to synchronize information provided to multiple groups from a single server.

In this paper, we have focused on a multi-secret sharing scheme and a compartmented multi-secret sharing scheme using elliptic curves [22], bilinear pairings [12, 16], and matrices [19]. The main purpose of using bilinear pairings and elliptic curves is that it gives similar security (as in existing schemes) with less key sizes.

The importance of our approach is that it overcomes some of the limitations of most existing schemes. Our schemes can handle an unlimited number of users. Our schemes are efficient and verifiable. The proposed

multi-secret sharing scheme requires $O(n^2)$ computations, and the compartmented multi-secret sharing scheme requires $O(mn^2)$ or $O(n^3)$ computations, where n is the number of users and m is the number of compartments. For example, our scheme is more efficient than [25]. We have also noticed that a secret sharing in compartmented groups proposed by Ghodosi, Pieprzyk and Safavi-Naini [9] does not work properly (the case $t > \sum t_i$). See Remark 2 for more details.

We have organized our article as follows. In Section 2, we recall the definitions of the elliptic curves and bilinear pairings. The proposed multi-secret sharing scheme has been described in Section 3, including security analysis, complexity, and an example of the scheme. In Section 4, we have proposed a compartmented multi-secret sharing scheme and its security analysis, and complexity are discussed. We provide an example for the illustration purpose using SageMath.

II. Preliminaries

Consider an elliptic curve $E: y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6$ over $\mathbb{F}_q$ with a non-zero discriminant, where q is prime power and $c_i \in \mathbb{F}_q$ for $i = 1,2,3,4,6$. The elliptic curve E can be changed to a normal form of elliptic curve $E': y^2 = x^3 + ax + b$ if the characteristic of $\mathbb{F}_q$ is not equal to 2 and 3. The discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$ of the elliptic curve E'. The points on the elliptic curve $E(\mathbb{F}_q)$ form a group with point at infinity $\mathcal{O}$ acting as an identity.

Definition 1 (Bilinear Pairings): Let G_A and G_M be an additive and a multiplicative cyclic group, respectively, with the same prime order ℓ (usually, one takes G_M to be a subgroup of a finite field). A bilinear pairing e is a map

$$\mathrm{e}: G_A \times G_A \to G_M$$

which satisfies the following conditions.

For $x_1,\ x_2,\ y_1,\ y_2 \in G_A$ and the identities $0 \in G_A,\ 1 \in G_M$,

- Bilinearity: $\mathrm{e}(x_1 + x_2, y_1) = \mathrm{e}(x_1, y_1)\mathrm{e}(x_2, y_1)$ and $\mathrm{e}(x_1, y_1 + y_2) = \mathrm{e}(x_1, y_1)\ \mathrm{e}(x_1, y_2)$.
- Non-degeneracy: For each $x_1 \neq 0$, there exists y_1 such that $\mathrm{e}(x_1, y_1) \neq 1$ and for each $y_1 \neq 0$, there exists x_1 such that $\mathrm{e}(x_1, y_1) \neq 1$.

- Computability: There exists an algorithm where e can be computed efficiently.

Following are some properties of the bilinear pairings. The bilinear pairing e which is symmetric satisfies, for all $x, y \in G_A$, $\mathrm{e}(x,0) = \mathrm{e}(0,y) = 1$ and $\mathrm{e}(ax,by) = \mathrm{e}(x,y)^{ab}$ for all $a,b \in \mathbb{Z}$. Also, if $\mathrm{e}(x,y) = 1$ for all $x \in G_A$, then $y = 0$. In addition, we also have $\mathrm{e}(x,y) = \mathrm{e}(x,y')$ iff $y = y'$ for any $x \neq 0$, $y, y' \in G_A$ (as both groups are cyclic and of same prime order).

For all $x, y \in G_A$,

- $\mathrm{e}(x,0) = \mathrm{e}(0,y) = 1$.
- $\mathrm{e}(ax,by) = \mathrm{e}(x,y)^{ab}$ for all $a,b \in \mathbb{Z}$.
- $\mathrm{e}(x,y) = \mathrm{e}(y,x)$.
- If $\mathrm{e}(x,y) = 1$ for all $x \in G_A$, then $y = 0$.

There are numerous pairings defined over the elliptic curves. For instance, let ℓ be a prime divisor of number of points on $E(\mathbb{F}_q)$ with gcd $(\ell, q) = 1$. The embedding degree of $E(\mathbb{F}_q)$ with respect to ℓ is denoted by k (that is, the least k such that $\ell \mid q^k - 1$). The set of ℓ-torsion points in $E(\mathbb{F}_{q^k})$ is denoted by $E[\ell]$. It is known that $E[\ell] \equiv \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. The *modified* Tate pairing e is a map $\mathrm{e} : E[\ell] \times E[\ell] \to \mu_\ell$, where μ_ℓ is the order-ℓ subgroup of $\mathbb{F}_{q^k}^*$. We refer to [8, 16] for further information. One can use modified Tate pairing, Weil pairing [17] and other similar kinds of pairings in our proposed scheme.

III. Proposed Multi-Secret Sharing Scheme

Consider an elliptic curve E over a finite field $\mathbb{F}_q$, where $q = p^{i_0}$ for some $i_0 \in \mathbb{N}$ and p is a large prime. Let $P \in E(\mathbb{F}_q)$ and $G_A = \langle P \rangle$ be a subgroup of order ℓ where ℓ is a large prime so that *elliptic curve discrete logarithm problem* (ECDLP) is hard to solve. Consider a pairing e as in the above definition. Suppose that there are n users, say, $u_1, u_2, \cdots, u_n$, and a trusted Dealer D. All the scheme parameters are generated and published by the Dealer. Furthermore, each user releases their public key while keeping their secret key private. The Dealer chooses g secret keys $K_1, K_2, \cdots, K_g \in [0, p-1]$ for the scheme.

- Dealer D chooses a matrix of order $n \times t$

$$B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \cdots & n^{t-1} \end{pmatrix}.$$

- D chooses t random integers $a_1, a_2, \cdots, a_t \in [0, \ell - 1]$ with $a_t \neq 0$ and computes

$$(b_1, b_2, \cdots, b_n)^T = B \cdot (a_1, a_2, \cdots, a_t)^T$$

  where T denotes the transpose of a matrix. D makes matrix B public.
- Each user u_i chooses a private key $x_i \in [1, \ell - 1]$ and makes $x_i P$ public.
- Then D computes $b_i x_i P$ and sends (publicly) to user u_i for $i = 1, 2, \cdots, n$.
- Each user u_i will get the share $b_i P$ by computing $x_i^{-1}(b_i x_i P)$.
- D computes $s_\lambda = \mathrm{e}(P, \lambda \cdot a_t P) + K_\lambda$, $1 \leq \lambda \leq g$, and makes them public.
- Also, each user u_i computes $z_i = \mathrm{e}(P, b_i P)$.

Suppose that t (or more) users, say $u_{r_1}, u_{r_2}, \cdots, u_{r_t}$, collaborate to reconstruct the secrets K_λ, $1 \leq \lambda \leq g$. Then each collaborating user pools their z_i value and supplementary information $x_i^{-1} P$ for the verification purpose. Then they compute $r = \prod_{j=1}^{t} z_{r_j}^{y_j}$, where $y_j = \left(\prod_{i=1, i \neq j}^{t} (r_j - r_i) \right)^{-1}$. Finally, they compute the secrets as $K_\lambda = s_\lambda - r^\lambda$.

Remark 1: We note that the above scheme works for any matrix whose any t rows form a Vandermonde matrix. For simplicity, we have taken the above matrix B. We also note that (see [16]), for any $P, Q \in E[\ell]$, $\mathrm{e}(P, Q) \in \mu_\ell \subseteq \mathbb{F}_{q^k}^* \subseteq \mathbb{F}_{q^k}$. Also, for any $K \in [0, p-1]$ we have $K \in \mathbb{F}_{q^k}$. Thus $\mathrm{e}(P, Q) + K$ is an element of $\mathbb{F}_{q^k}$.

Correctness: The correctness of the secret reconstruction can be observed as follows.

$$\begin{aligned} r &= \prod_{i=1}^{t} z_{r_i}^{y_i} = \prod_{i=1}^{t} \mathrm{e}(P, b_{r_i} P)^{y_i} \\ &= \prod_{i=1}^{t} \mathrm{e}(P, y_i b_{r_i} P) = \mathrm{e}\left(P, \left(\sum_{i=1}^{t} y_i b_{r_i} \right) P \right) = \mathrm{e}(P, a_t P). \end{aligned}$$

Here y_i's are the entries of the last row of the inverse of the Vandermonde matrix corresponding to collaborating set of users. We know that the last entry of the product of the inverse of Vandermonde matrix and the shares matrix gives the value a_tP (for more details, we refer to [19]). The partial secret a_tP is the last entry of the product $B_1^{-1} \cdot (b_1P, b_2P, \cdots, b_tP)^T$, where

$$B_1 = \begin{pmatrix} 1 & r_1 & r_1^2 & \cdots & r_1^{t-1} \\ 1 & r_2 & r_2^2 & \cdots & r_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & r_t & r_t^2 & \cdots & r_t^{t-1} \end{pmatrix}$$

is the matrix corresponding to collaborating set of users. Our scheme gives the partial secret key a_tP directly; however, some existing secret sharing schemes (see [21], for example) uses Lagrange interpolation to find the whole polynomial and get the secret.

Verification of the Shares: Users do not need to check the legitimacy of the shares as they are sent in an encrypted format, and the Dealer is trusted. The users can verify the shares of the other collaborating users at the time of reconstruction of the secret. Each collaborating user u_i transmits the share $b_{i'}P$ with supplementary information $x_i^{-1}P$ for verification at the time of the secret reconstruction. The validity of the equation $\mathrm{e}(x_i^{-1}P, b_ix_iP) = \mathrm{e}(P, b_{i'}P)$ ensures the originality of the share.

i. *Security Analysis of the Proposed Scheme*

Bilinear pairing behaves like a one-way function, which means it is easy to compute the image of inputs but difficult to find the pre-image of a given image. In our scheme, one important factor is that for distributing shares, the Dealer doesn't require any secure channel. Dealer encrypts the shares and sends them to the users publicly. We have assumed that the elliptic curve discrete logarithm problem is hard to solve for large order group G_A. From the users point of view, they send x_iP, $i = 1, 2, \cdots, n$, to Dealer D. So the Dealer or any adversary cannot know anything about the users secret key x_i. From the Dealer point of view, the shares b_iP, $i = 1, 2, \cdots, n$, are distributed to the respective users so that no attacker gets any information about the share(s).

We have the following observations.

Theorem 1: *For an attacker, the probability of choosing a random point* $a_{t'}P \in G_A$ *such that* $K_\lambda = s_\lambda - \mathrm{e}(P, a_{t'}P)$ *for* $1 \le \lambda \le g$ *is* $1/(\ell - 1)$.

Proof: It is clear that $K_\lambda = s_\lambda - \mathrm{e}(P, a_{t'}P)$ if and only if $\mathrm{e}(P, a_{t'}P) = \mathrm{e}(P, \lambda \cdot a_t P)$, which is true if and only if $a_{t'}P = \lambda a_t P$. Thus, the probability of choosing a point $a_{t'}P \in G_A$ such that $s_\lambda - \mathrm{e}(P, a_{t'}P) = K_\lambda$ is $1/(\ell - 1)$ as $a_{t'}P \neq \mathcal{O}$.

Theorem 2: *The honesty of at least* $n - t + 1$ *users ensures that any* $t - 1$ *(or less) users cannot get any information about any of the secrets* K_λ, $1 \le \lambda \le g$.

Proof: Suppose that any $t - 1$ (or less) users, say $u_{r_1}, u_{r_2}, \cdots, u_{r_{t-1}}$, collaborate to reconstruct the secret. They have the public information and their shares $b_{r_1}P$, $b_{r_2}P, \cdots$, $b_{r_{t-1}}P$. Also they can compute y_i, $i = 1, 2, \cdots, t$, and so $\sum_{i=1}^{t-1} y_i b_{r_i} P$ but not $y_t b_{r_t} P$ as they have no information about the share of u_{r_t}, where u_{r_t} is any user other than the $t - 1$ users. Note that $\sum_{i=1}^{t} y_i b_{r_i} P = a_t P$. For choosing the correct share $b_{r_t}P$ is as hard as choosing $a_t P$. Then $a_t P$ can be any element of G_A and without $a_t P$ they cannot compute $K_\lambda = s_\lambda - \mathrm{e}(P, a_t P)^\lambda$.

Theorem 3: *There is no loss of secrets information of collaborators for reconstructing the secrets* K_λ *for* $1 \le \lambda \le g$.

Proof: The collaborating users pools z_i and $x_i^{-1}P$ values. Finding x_i^{-1} from $x_i^{-1}P$ is equivalent to solving an ECDLP, which is assumed as hard to solve for a large order group. Hence they cannot get the users secret key x_i, $i = 1, 2, \cdots, t$. Moreover, the only point $x_{i'}P \in G_A$ satisfying $\mathrm{e}(x_{i'}P, b_i x_i P) = \mathrm{e}(P, b_i P)$ must satisfy $x_i' \equiv x_i^{-1} (\mathrm{mod}\ \ell)$. For

$$\begin{aligned} \mathrm{e}(x_i'P, x_i b_i P) = \mathrm{e}(P, b_i P) &\Leftrightarrow \mathrm{e}(P, b_i P)^{x_i' x_i} = \mathrm{e}(P, b_i P) \\ &\Leftrightarrow x_i' x_i \equiv 1 (\mathrm{mod}\ \ell) \\ &\Leftrightarrow x_i' \equiv x_i^{-1} (\mathrm{mod}\ \ell). \end{aligned}$$

ii. *Complexity of the proposed multi-secret sharing scheme*

The computational cost of the matrix multiplication of order $n \times t$ and $t \times 1$ takes nt operations. Using the *Double-and-Add algorithm* [5], the time for computing scalar multiplication of a point on elliptic curve is $O(\log_2 \ell)$, where ℓ is the order of the point. The number of scalar multiplications at the time of generating shares and reconstruction of the secret is n and t, respectively. For computing $t + g$ pairings, it takes $O((t + g)\log_2 \ell)$ (see [11, 17], for example). Additionally, the scheme requires $(t - 1)M + 1S$ operations, where M and S denote multiplication

and subtraction respectively. For computing y_i, $i=1,2,\cdots,t$, it takes $t((t-1)M+1S)$ operations. Hence the required time complexity for the scheme is $O(n^2)$.

Let T_{MM} = time for computing multiplication of matrices
T_{SM} = time for computing scalar multiplication of a point on elliptic curve
T_P = time for computing pairing.

Then the time for generating the shares is $T_{MM}+nT_{SM}$ and the required time for reconstructing the secret is $tT_P+tT_{SM}+(t-1)M$ where M denotes the multiplication. We have skipped the time for computing y_i's as it takes very less time.

An example of the proposed multi-secret sharing scheme using modified Tate pairing [16] is given below. The computations are done using SageMath.

Example 1: Consider an elliptic curve $E: y^2=x^3+5x+13$ over $\mathbb{F}_{29}$. The number of points on the curve is $26=2\times 13$ and $13\mid 29^3-1$. Thus, the embedding degree of $E(\mathbb{F}_{29})$ with respect to 13 is 3. We note that here $\ell=13$, $p=q=29$ and $k=3$. $\mathbb{F}_{29^3}$ is a finite field and $\#E(\mathbb{F}_{29^3})=24674$. The torsion group $E[13]\subseteq E(\mathbb{F}_{29^3})$. Suppose there are $n=6$ users, say, u_1,u_2,u_3,u_4,u_5,u_6, and $t=4$ be the threshold. Let $K_1=7$, $K_2=3$ and $K_3=24$ be the secret keys of the scheme. Dealer considers the matrix

$$B=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2^2 & 2^3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 6 & 6^2 & 6^3 \end{pmatrix}.$$

Suppose D chooses 4 integers $5,2,8,10\in[0,12]$ and computes

$$\begin{aligned}(b_1,b_2,b_3,b_4,b_5,b_6)^T &= B\cdot(5,2,8,10)^T \\ &= (25,121,353,781,1465,2465)^T \\ &\equiv (12,4,2,1,9,8)^T \bmod 13.\end{aligned}$$

Let D chooses a point $P=(5\gamma^2+2\gamma+7,\ 14\gamma^2+4)\in E[13]$ and computes $s_1=\mathrm{e}(P,10P)+7=\gamma^2+14\gamma+22$, $s_2=\mathrm{e}(P,2\times 10P)+3=21\gamma^2+18\gamma+23$ and $s_3=\mathrm{e}(P,3\times 10P)+25=23\gamma^2+26\gamma+2$ where γ is a root of an irreducible cubic polynomial over $\mathbb{F}_{29}$ (it follows that $\mathbb{F}_{29}(\gamma)=\mathbb{F}_{29^3}$) and the pairing e is the modified Tate pairing as in [16]. The Dealer makes P, s_1, s_2 and s_3 public. Each user $u_i, i=1,2,\cdots,6$, chooses

random integer, say $x_1 = 3,\ x_2 = 9,\ x_3 = 2,\ x_4 = 11,\ x_5 = 5,\ x_6 = 6$ and makes $x_i P$ public. We have

$$\begin{aligned}
x_1P &= 3P = (15\gamma^2 + 17\gamma + 4, 20\gamma),\\
x_2P &= 9P = (7\gamma^2 + 14\gamma + 25, 25\gamma^2 + 1),\\
x_3P &= 2P = (17\gamma^2 + 16\gamma + 17, 14\gamma^2 + 22\gamma + 10),\\
x_4P &= 11P = (17\gamma^2 + 16\gamma + 17, 15\gamma^2 + 7\gamma + 19),\\
x_5P &= 5P = (21\gamma^2 + 28\gamma + 9, 8\gamma^2 + 24\gamma + 23) \text{ and}\\
x_6P &= 6P = (19\gamma^2 + 14\gamma + 21, 13\gamma^2 + 4\gamma + 22).
\end{aligned}$$

Now Dealer computes $b_i x_i P$ and sends (publicly) to the user u_i, $i = 1, 2, \cdots, 6,$ where

$$\begin{aligned}
b_1x_1P &= 12 \times 3P = (15\gamma^2 + 17\gamma + 4, 9\gamma),\\
b_2x_2P &= 4 \times 9P = (15\gamma^2 + 17\gamma + 4, 9\gamma),\\
b_3x_3P &= 2 \times 2P = (7\gamma^2 + 14\gamma + 25, 4\gamma^2 + 28),\\
b_4x_4P &= 1 \times 11P = (17\gamma^2 + 16\gamma + 17, 15\gamma^2 + 7\gamma + 19),\\
b_5x_5P &= 9 \times 5P = (19\gamma^2 + 14\gamma + 21, 13\gamma^2 + 4\gamma + 22) \text{ and}\\
b_6x_6P &= 8 \times 6P = (7\gamma^2 + 14\gamma + 25, 25\gamma^2 + 1).
\end{aligned}$$

$$\begin{aligned}
b_1x_1P &= 12 \times 3P = (15\gamma^2 + 17\gamma + 4, 9\gamma),\\
b_2x_2P &= 4 \times 9P = (15\gamma^2 + 17\gamma + 4, 9\gamma),\\
b_3x_3P &= 2 \times 2P = (7\gamma^2 + 14\gamma + 25, 4\gamma^2 + 28),\\
b_4x_4P &= 1 \times 11P = (17\gamma^2 + 16\gamma + 17, 15\gamma^2 + 7\gamma + 19),\\
b_5x_5P &= 9 \times 5P = (19\gamma^2 + 14\gamma + 21, 13\gamma^2 + 4\gamma + 22) \text{ and}\\
b_6x_6P &= 8 \times 6P = (7\gamma^2 + 14\gamma + 25, 25\gamma^2 + 1).
\end{aligned}$$

We note that, in this example, all the inverses computed below are of modulo 13. Now each user u_i computes the share $b_i P$ as $x_i^{-1}(b_i x_i)P$, $i = 1, \cdots, 6.$ Thus the shares are

$$\begin{aligned}
b_1P = x_1^{-1}(b_1x_1)P &= 9(b_1x_1)P = (5\gamma^2 + 2\gamma + 7, 15\gamma^2 + 25),\\
b_2P = x_2^{-1}(b_2x_2)P &= 3(b_2x_2)P = (7\gamma^2 + 14\gamma + 25, 4\gamma^2 + 28),\\
b_3P = x_3^{-1}(b_3x_3)P &= 7(b_3x_3)P = (17\gamma^2 + 16\gamma + 17, 14\gamma^2 + 22\gamma + 10),\\
b_4P = x_4^{-1}(b_4x_4)P &= 6(b_4x_4)P = (5\gamma^2 + 2\gamma + 7, 14\gamma^2 + 4),\\
b_5P = x_5^{-1}(b_5x_5)P &= 8(b_5x_5)P = (7\gamma^2 + 14\gamma + 25, 25\gamma^2 + 1) \text{ and}
\end{aligned}$$

$$b_6P = x_6^{-1}(b_6x_6)P \quad = \quad 11(b_6x_6)P = (21\gamma^2 + 28\gamma + 9, 21\gamma^2 + 5\gamma + 6).$$

Suppose that u_2, u_3, u_5, u_6 want to reconstruct the secrets. They compute $z_i = \mathrm{e}(P, b_iP)$ and $x_i^{-1}P$, $i = 2,3,5,6$. Here

$$\begin{aligned}
z_2 &= \mathrm{e}(P, b_2P) = 23\gamma^2 + 26\gamma + 25 \text{ and } x_2^{-1}P = (15\gamma^2 + 17\gamma + 4, 20\gamma),\\
z_3 &= \mathrm{e}(P, b_3P) = 9\gamma + 24 \text{ and } x_3^{-1}P = (19\gamma^2 + 14\gamma + 21, 16\gamma^2 + 25\gamma + 7),\\
z_5 &= \mathrm{e}(P, b_5P) = 28\gamma^2 + 2\gamma + 17 \text{ and } x_5^{-1}P = (21\gamma^2 + 28\gamma + 9, 21\gamma^2 + 5\gamma + 6) \text{ and}\\
z_6 &= \mathrm{e}(P, b_6P) = 14\gamma^2 + 24\gamma + 1 \text{ and} x_6^{-1}P = (17\gamma^2 + 16\gamma + 17, 15\gamma^2 + 7\gamma + 19).
\end{aligned}$$

The collaborating users can verify the shares of other collaborating users as in the above proposed multi-secret sharing scheme. If the verification holds for all collaborating users, they calculate $r = z_2^{y_2} z_3^{y_3} z_5^{y_5} z_6^{y_6}$, where

$$\begin{aligned}
y_2 &= ((2-3)(2-5)(2-6))^{-1} = -12^{-1} \bmod 13 = 1,\\
y_3 &= ((3-2)(3-5)(3-6))^{-1} = 6^{-1} \bmod 13 = 11,\\
y_5 &= ((5-2)(5-3)(5-6))^{-1} = -6^{-1} \bmod 13 = 2 \text{ and}\\
y_6 &= ((6-2)(6-3)(6-5))^{-1} = 12^{-1} \bmod 13 = 12.
\end{aligned}$$

Thus, $r = \gamma^2 + 14\gamma + 15$ and they obtain the secrets $K_1 = s_1 - r = 7$, $K_2 = s_2 - r^2 = 3$ and $K_3 = s_3 - r^3 = 24$.

IV. Compartmented Secret Sharing Scheme

i. *Compartmented Access Structure*

Suppose that there is a set $U = \{u_1, u_2, \cdots, u_n\}$ of n users divided into m disjoint compartments $C_1, C_2, \cdots, C_m$. Let $t_i \geq 1$ be the threshold for C_i and let $t \geq \sum_{i=1}^{m} t_i$ be the global threshold. Any set of at least t users, having at least t_i users from C_i, $1 \leq i \leq m$, is qualified to reconstruct the secret. The access structure is the collection of all qualified sets of users. Mathematically, the access structure is

$$\Gamma = \{V \subseteq U : |V \cap C_i| \geq t_i \text{ for every } i = 1,2,\cdots,m, \text{ and } |V| \geq t\}.$$

ii. *Proposed Compartmented Multi-Secret Sharing Scheme*

Consider an elliptic curve E over a finite field $\mathbb{F}_q$, where $q = p^{i_0}$ for some $i_0 \in \mathbb{N}$ and p is a large prime. Let $P \in E(\mathbb{F}_q)$ and $G_A = \langle P \rangle$ be subgroup of order ℓ where ℓ is a large prime so that *elliptic curve discrete logarithm*

problem (ECDLP) is hard to solve. Consider the pairing e as defined above (Definition 1). Suppose that the scheme involves a set U of n users divided into m disjoint compartments $C_1, C_2, \cdots, C_m$ and a trusted Dealer D. Let $|C_i| = n_i$ and t_i be the threshold for C_i, $i = 1, 2, \cdots, m$. Dealer D chooses t_i random integers $a_{i1}, a_{i2}, \cdots, a_{it_i} \in [0, \ell - 1]$, with $a_{it_i} \neq 0$, for each compartment C_i, $1 \leq i \leq m$. D chooses g secret keys $K_1, K_2, \cdots, K_g \in [0, p-1]$ and computes $s_\lambda = \prod_{i=1}^{m} \mathrm{e}(P, \lambda \cdot a_{it_i} P) + K_\lambda$ (or, equivalently $s_\lambda = \mathrm{e}(P, \sum_{i=1}^{m} \lambda \cdot a_{it_i} P) + K_\lambda$), $1 \leq \lambda \leq g$. Dealer makes P and s_λ, $1 \leq \lambda \leq g$, public.

Let u_{ij} denote j^{th} user in the compartment C_i.

Let $t \geq \sum_{i=1}^{m} t_i$ be the global threshold for the scheme. We have the following two cases.

Case I: $t = \sum_{i=1}^{m} t_i$

We have the following access structure (in this case)

$$\Gamma = \{V \subseteq U : |V \cap C_i| \geq t_i \text{ for every } i, i = 1, 2, \cdots, m\}.$$

- Dealer D considers a matrix of order $n_i \times t_i$ for each C_i, $1 \leq i \leq m$, as

$$A_i = \begin{pmatrix} 1 & k_{i1} & k_{i1}^2 & \cdots & k_{i1}^{t_i - 1} \\ 1 & k_{i2} & k_{i2}^2 & \cdots & k_{i2}^{t_i - 1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & k_{in_i} & k_{in_i}^2 & \cdots & k_{in_i}^{t_i - 1} \end{pmatrix},$$

  where $k_{ij} \in [1, \ell - 1]$ and $k_{ij} \neq k_{ij'}$ for $j \neq j'$.
- D computes $(b_{i1}, b_{i2}, \cdots, b_{in_i})^T = A_i \cdot (a_{i1}, a_{i2}, \cdots, a_{it_i})^T$ for each C_i, $1 \leq i \leq m$, and makes A_i public.
- Each user u_{ij}, $j = 1, 2, \cdots, n_i$, in the compartment C_i, $1 \leq i \leq m$, chooses a secret/private key $x_{ij} \in [1, \ell - 1]$ randomly and makes $x_{ij} P$ public.
- Then D computes $b_{ij} x_{ij} P$ for each user in C_i and sends (publicly) to the respective users in C_i for $i = 1, 2, \cdots, m$.
- Each user u_{ij} in C_i will get the share $b_{ij} P$ by computing $x_{ij}^{-1}(b_{ij} x_{ij}) P$, $1 \leq j \leq n_i$.

Suppose t_i users from each compartment C_i, $1 \le i \le m$, come together to compute the secret keys K_λ, $1 \le \lambda \le g$. The t_i users in C_i can compute $r_i = \mathrm{e}(P, a_{it_i} P)$ as in previous multi-secret sharing scheme (Section III). Then they compute the secret keys $K_\lambda = s_\lambda - \prod_{i=1}^{m} r_i^{\lambda}$, $1 \le \lambda \le g$.

Case II: $t > \sum_{i=1}^{m} t_i$

We have the following access structure

$$\Gamma = \{V \subseteq U : |V \cap C_i| \ge t_i \text{ for every } i = 1, 2, \cdots, m, \text{ and } |V| \ge t\}.$$

Let $t_0 = t - \sum_{i=1}^{m} t_i$. Considers the matrix A_i for compartment C_i, $i = 1, 2, \cdots, m$, where

$$A_i = \begin{pmatrix} 1 & k_{i1} & k_{i1}^2 & \cdots & k_{i1}^{t_i-1} & k_{i1}^{t_i} & \cdots & k_{i1}^{t_i+t_0-1} \\ 1 & k_{i2} & k_{i2}^2 & \cdots & k_{i2}^{t_i-1} & k_{i2}^{t_i} & \cdots & k_{i2}^{t_i+t_0-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & k_{in_i} & k_{in_i}^2 & \cdots & k_{in_i}^{t_i-1} & k_{in_i}^{t_i} & \cdots & k_{in_i}^{t_i+t_0-1} \end{pmatrix}.$$

Choose t_0 values $\omega_1, \omega_2, \cdots, \omega_{t_0} \in [0, \ell - 1]$. Let $(b_{i1}, b_{i2}, \cdots, b_{in_i})^T = A_i \cdot (a_{i1}, a_{i2}, \cdots, a_{it_i}, \omega_1, \omega_2, \cdots, \omega_{t_0})^T$ for each compartment C_i, $1 \le i \le m$, and make A_i public. Then distribute the shares $b_{i1}P, b_{i2}P, \cdots, b_{in_i}P$ to the users in compartment C_i, $i = 1, 2, \cdots, m$, as in the Case-I.

Reconstruction of the secrets.

Suppose that t (or more) users collaborate, say α_1 from C_1, α_2 from C_2, ..., and $\alpha_i \ge t_i$, $1 \le i \le m$. Without loss of generality, aasume that the collaborating users are $u_{11}, \cdots, u_{1\alpha_1}, u_{21}, \cdots, u_{2\alpha_2}, \cdots, u_{m1}, \cdots, u_{m\alpha_m}$. Then they can construct the following system of $\alpha_1 + \alpha_2 + \cdots + \alpha_m$ linear equations.

$$\begin{aligned}
b_{11}P &= a_{11}P + k_{11}a_{12}P + \cdots + k_{11}^{t_1-1}a_{1t_1}P + k_{11}^{t_1}\omega_1 P + \cdots + k_{11}^{t_1+t_0-1}\omega_{t_0}P \\
b_{12}P &= a_{11}P + k_{12}a_{12}P + \cdots + k_{12}^{t_1-1}a_{1t_1}P + k_{12}^{t_1}\omega_1 P + \cdots + k_{12}^{t_1+t_0-1}\omega_{t_0}P \\
&\vdots \\
b_{1\alpha_1}P &= a_{11}P + k_{1\alpha_1}a_{12}P + \cdots + k_{1\alpha_1}^{t_1-1}a_{1t_1}P + k_{1\alpha_1}^{t_1}\omega_1 P + \cdots + k_{1\alpha_1}^{t_1+t_0-1}\omega_{t_0}P \\
&\vdots \\
b_{m1}P &= a_{m1}P + k_{m1}a_{m2}P + \cdots + k_{m1}^{t_m-1}a_{mt_m}P + k_{m1}^{t_m}\omega_1 P + \cdots + k_{m1}^{t_m+t_0-1}\omega_{t_0}P \\
b_{m2}P &= a_{m1}P + k_{m2}a_{m2}P + \cdots + k_{m2}^{t_m-1}a_{mt_m}P + k_{m2}^{t_m}\omega_1 P + \cdots + k_{m2}^{t_m+t_0-1}\omega_{t_0}P \\
&\vdots
\end{aligned}$$

$$b_{m\alpha_m}P = a_{m1}P + k_{m\alpha_m}a_{m2}P + \cdots + k_{m\alpha_m}^{t_m-1}a_{mt_m}P + k_{m\alpha_m}^{t_m}\omega_1 P + \cdots + k_{m\alpha_m}^{t_m+t_0-1}\omega_{t_0}P.$$

In matrix form, we have

$$\begin{pmatrix}
1 & k_{11} & \cdots & k_{11}^{t_1-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & k_{11}^{t_1} & \cdots & k_{11}^{t_1+t_0-1} \\
1 & k_{12} & \cdots & k_{12}^{t_1-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & k_{12}^{t_1} & \cdots & k_{12}^{t_1+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
1 & k_{1a_1} & \cdots & k_{1a_1}^{t_1-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & k_{1a_1}^{t_1} & \cdots & k_{1a_1}^{t_1+t_0-1} \\
0 & 0 & \cdots & 0 & 1 & k_{21} & \cdots & k_{21}^{t_2-1} & \cdots & 0 & 0 & \cdots & 0 & k_{21}^{t_2} & \cdots & k_{21}^{t_2+t_0-1} \\
0 & 0 & \cdots & 0 & 1 & k_{22} & \cdots & k_{22}^{t_2-1} & \cdots & 0 & 0 & \cdots & 0 & k_{22}^{t_2} & \cdots & k_{22}^{t_2+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 1 & k_{2a_2} & \cdots & k_{2a_2}^{t_2-1} & \cdots & 0 & 0 & \cdots & 0 & k_{2a_2}^{t_2} & \cdots & k_{2a_2}^{t_2+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & k_{m1} & \cdots & k_{m1}^{t_m-1} & k_{m1}^{t_m} & \cdots & k_{m1}^{t_m+t_0-1} \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & k_{m2} & \cdots & k_{m2}^{t_m-1} & k_{m2}^{t_m} & \cdots & k_{m2}^{t_m+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & k_{ma_m} & \cdots & k_{ma_m}^{t_m-1} & k_{ma_m}^{t_m} & \cdots & k_{ma_m}^{t_m+t_0-1}
\end{pmatrix}
\begin{pmatrix}
a_{11}P \\ \vdots \\ a_{1t_1}P \\ a_{21}P \\ \vdots \\ a_{2t_2}P \\ \vdots \\ a_{m1}P \\ \vdots \\ a_{mt_m}P \\ \omega_1 P \\ \vdots \\ \omega_{t_0}P
\end{pmatrix}
=
\begin{pmatrix}
b_{11}P \\ b_{12}P \\ \vdots \\ b_{1a_1}P \\ b_{21}P \\ b_{22}P \\ \vdots \\ b_{2a_2}P \\ \vdots \\ b_{m1}P \\ b_{m2}P \\ \vdots \\ b_{ma_m}P
\end{pmatrix}$$

We have to choose the matrices A_i (for Case-II) such that the above matrix corresponding to collaborating users is an invertible matrix. The above system of linear equations have $\sum_{i=1}^{m} t_i + t_0 = t$ unknowns and $\sum_{i=1}^{m} \alpha_i = t$ equations. Hence the system has a unique solution. After getting the values $a_{it_i}P,\ i = 1, 2, \cdots, m,$ they compute the sum $\sum_{i=1}^{m} a_{it_i}P$ and recover the secrets as $K_\lambda = s_\lambda - \mathrm{e}(P, \sum_{i=1}^{m} a_{it_i}P)^\lambda,\ 1 \le \lambda \le g.$

The verification procedure of the shares is the same as in the previous proposed multi-secret sharing scheme.

Remark 2: We note that the scheme proposed by Ghodosi, Pieprzyk and Safavi-Naini [9] has some limitations. For example, in the case $t > \sum_{i=1}^{m} t_i$, their scheme fails. We illustrate this by an example below.

Suppose that there are 2 compartments. Consider $n_1 = 5, n_2 = 5,$ $t_1 = 2, t_2 = 3$ and $\alpha_1 = 3, \alpha_2 = 4.$ Then the shares of the collaborating users are, say,

$$\begin{aligned}
s_{11} &= k_1 + a_{11}x_{11} + \omega_1 x_{11}^2 + \omega_2 x_{11}^3 \\
s_{12} &= k_1 + a_{11}x_{12} + \omega_1 x_{12}^2 + \omega_2 x_{12}^3 \\
s_{13} &= k_1 + a_{11}x_{13} + \omega_1 x_{13}^2 + \omega_2 x_{13}^3 \\
s_{21} &= k_2 + a_{21}x_{21} + a_{22}x_{21}^2 + \omega_1 x_{21}^3 + \omega_2 x_{21}^4 \\
s_{22} &= k_2 + a_{21}x_{22} + a_{22}x_{22}^2 + \omega_1 x_{22}^3 + \omega_2 x_{22}^4 \\
s_{23} &= k_2 + a_{21}x_{23} + a_{22}x_{23}^2 + \omega_1 x_{23}^3 + \omega_2 x_{23}^4 \\
s_{24} &= k_2 + a_{21}x_{24} + a_{22}x_{24}^2 + \omega_1 x_{24}^3 + \omega_2 x_{24}^4
\end{aligned}$$

where s_{ij} is the share of u_{ij} and k_1, k_2 are compartment secrets. In matrix form, we have

$$\begin{pmatrix} 1 & x_{11} & 0 & 0 & 0 & x_{11}^2 & x_{11}^3 \\ 1 & x_{12} & 0 & 0 & 0 & x_{12}^2 & x_{12}^3 \\ 1 & x_{13} & 0 & 0 & 0 & x_{13}^2 & x_{13}^3 \\ 0 & 0 & 1 & x_{21} & x_{21}^2 & x_{21}^3 & x_{21}^4 \\ 0 & 0 & 1 & x_{22} & x_{22}^2 & x_{22}^3 & x_{22}^4 \\ 0 & 0 & 1 & x_{23} & x_{23}^2 & x_{23}^3 & x_{23}^4 \\ 0 & 0 & 1 & x_{24} & x_{24}^2 & x_{24}^3 & x_{24}^4 \end{pmatrix} \begin{pmatrix} k_1 \\ a_{11} \\ k_2 \\ a_{21} \\ a_{22} \\ \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} s_{11} \\ s_{12} \\ s_{13} \\ s_{21} \\ s_{22} \\ s_{23} \\ s_{24} \end{pmatrix}.$$

For any choice of $x_{ij} \in \mathbb{F}_q$ satisfying the equation $x_{11} + x_{12} + x_{13} = x_{21} + x_{22} + x_{23} + x_{24}$ we observe that the coefficient matrix is not invertible.

V. Security analysis of the proposed compartmented multi-secret sharing scheme

The security analysis of the proposed compartmented multi-secret sharing scheme is similar to the previous proposed scheme (see Section i).

The shares are encrypted by the Dealer and sent to the users (publicly). For large order group G_A, we have assumed that the ECDLP is hard to solve [13]. When the Dealer distributes the shares $b_{ij}P$ to the users, an adversary cannot acquire it from $b_{ij}x_{ij}P$ as it is comparable to solving an ECDLP. Also, an adversary cannot get the user secret key x_{ij} from $x_{ij}P$. The probability of guessing points $a_{it_i}'P$, $1 \le i \le m$, (or, the sum) which satisfies the relation $K_\lambda = s_\lambda - \mathrm{e}(P, \sum_{i=1}^{m} a_{it_i}'P)^\lambda$, $1 \le \lambda \le g$, is negligible for a large prime order group G_A.

We have the following observation.

Theorem 4: *An unauthorized set of users cannot obtain any information about any of the secrets* K_λ *for* $1 \le \lambda \le g$.

Proof: Assume that V_1 is an unauthorized set, i.e., $V_1 \notin \Gamma$.

- In the case $t = \sum_{i=1}^{m} t_i$, there is at least one compartment U_i from which the number of users in V_1 is less than t_i that is $|V_1 \cap C_i| < t_i$. Hence they cannot compute compartment secrets a_{it_i} as observed by Theorem 2.
- In the case $t > \sum_{i=1}^{m} t_i$, there are two possibilities.

1. There is a compartment U_i for which $\alpha_i = |V_1 \cap C_i| < t_i$. This implies that the corresponding value a_{it_i} cannot be computed.
2. All $\alpha_i \geq t_i$ but $\sum_{i=1}^{m} \alpha_i < t$. This rules out the existence of the unique solution for $\omega_1 P, \omega_2 P, \cdots, \omega_{t_0} P$.

Hence an unauthorized set of users will get no information about the secrets K_λ for $1 \leq \lambda \leq g$.

Theorem 5 (Verification of shares): *The proposed scheme can detect and verify harmful activities in time.*

Proof: Users can verify the accuracy of other users shares at the time of secret reconstruction. Verification will be done using the public information $x_{ij} b_{ij} P$ and an additional information $x_{ij}^{-1} P$ given by the user u_{ij}. Assume that in order to reconstruct the secrets, the cooperating user u_{ij} works with the share $b_{ij}'P$. If $b_{ij}'P = b_{ij} P$, then the equation $e(P, b_{ij}'P) = e(P, b_{ij} P)$ is valid. Additionally, $e(P, b_{ij} P) = e(x_{ij}^{-1} P, x_{ij} b_{ij} P)$ may be used to calculate the value of $e(P, b_{ij} P)$ since $x_{ij} b_{ij} P$ is open to the public. As a result, it is possible to confirm the share of user u_{ij} by examining the correctness of the equation $e(x_{ij}^{-1} P, x_{ij} b_{ij} P) = e(P, b_{ij}'P)$.

We have given below an example of the proposed compartmented multi-secret sharing scheme using modified Tate pairing [16]. The computations are done using SageMath.

Example 2: Consider an elliptic curve $E: y^2 = x^3 + x + 38$ over the finite field $\mathbb{F}_{47}$. The $\#E(\mathbb{F}_{47}) = 61$ and $61 | 47^3 - 1$, i.e., the embedding degree of $E(\mathbb{F}_{47})$ with respect to 61 is 3. $\mathbb{F}_{47^3}$ is a finite field and $\#E(\mathbb{F}_{47^3}) = 104188$. The group $E[61] \subseteq E(\mathbb{F}_{47^3})$ is the set of torsion points. Let $Q = (4\gamma + 21, 4\gamma^2 + 15\gamma + 4) \in E[61]$ and $G_A = \langle Q \rangle$ where γ is a root of an irreducible cubic polynomial over $\mathbb{F}_{47}$. Suppose that there are 3 compartments. Assume that $t_1 = 2$, $t_2 = 2$, $t_3 = 3$, and $n_1 = 4$, $n_2 = 4$, $n_3 = 5$. Let the secrets $K_1 = 10$, $K_2 = 22$, $K_3 = 31$, $K_1 = 15$ and $a_{11} = 15$, $a_{12} = 20$, $a_{21} = 25$, $a_{22} = 30$, $a_{31} = 35$, $a_{32} = 40$, $a_{33} = 45$.

Assume that $A_1 = \begin{pmatrix} 1 & 4 \\ 1 & 8 \\ 1 & 11 \\ 1 & 13 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 & 3 \\ 1 & 5 \\ 1 & 9 \\ 1 & 14 \end{pmatrix}$ and $A_3 = \begin{pmatrix} 1 & 2 & 2^2 \\ 1 & 7 & 7^2 \\ 1 & 10 & 10^2 \\ 1 & 12 & 12^2 \\ 1 & 15 & 15^2 \end{pmatrix}$. Compute $s_1 =$

$e(Q, \sum_{i=1}^{3} a_{it_i} Q) + 10 = e(Q, 95Q) + 10 = e(Q, 34Q) + 10 = 15\gamma^2 + 29\gamma +$

52, $s_2 = e(Q, 2 \times 34Q) + 22 = 16\gamma^2 + 11\gamma + 26$, $s_3 = e(Q, 3 \times 34Q) + 31 = 2\gamma^2 + 32\gamma + 7$ and $s_4 = e(Q, 4 \times 34Q) + 15 = 45\gamma^2 + 30\gamma + 5$ where the pairing e is the modified Tate pairing as in [16]. Make Q, s_1, s_2, s_3 and s_4 public.

Case I: $t = 7$ (*i.e.* $t_1 + t_2 + t_3 = 7$).

Suppose that users u_{12}, u_{13}, u_{21}, u_{22}, u_{31}, u_{33}, u_{34} collaborate to reconstruct the secrets. Their shares are $(29\gamma^2 + 7\gamma + 7, 32\gamma^2 + 8\gamma + 19)$, $(25\gamma^2 + 14\gamma, 18\gamma^2 + 17\gamma + 37)$, $(14\gamma^2 + 24\gamma + 39, 32\gamma^2 + 30\gamma + 37)$, $(29\gamma^2 + 7\gamma + 7, 32\gamma^2 + 8\gamma + 19)$, $(12\gamma^2 + 10\gamma + 4, 10\gamma^2 + 2\gamma + 44)$, $(39\gamma^2 + 40\gamma + 40, 7\gamma^2 + 41\gamma + 44)$ and $(24\gamma^2 + 13\gamma + 46, 26\gamma^2 + 40\gamma + 18)$ respectively.

Now u_{12}, u_{13} can find their compartment secret $a_{12}Q = 20Q = (24\gamma^2 + 13\gamma + 46, 21\gamma^2 + 7\gamma + 29)$ using their shares (as illustrated by in Example 1). Similarly,

- u_{21}, u_{22} can find $a_{22}Q = 30Q = (8\gamma^2 + 33\gamma + 7, 35\gamma^2 + 36\gamma + 7)$.
- u_{31}, u_{33}, u_{34} can find $a_{33}Q = 40Q = (8\gamma^2 + 36\gamma + 13, 45\gamma^2 + 22\gamma + 41)$.

Then they compute the pairing $e(Q, 20Q + 30Q + 45Q) = e((4\gamma + 21, 4\gamma^2 + 15\gamma + 4), (42\gamma^2 + 33\gamma + 10, 20\gamma^2 + 31\gamma + 18)) = 15\gamma^2 + 29\gamma + 42$. Finally, the secrets can be reconstructed as $K_1 = s_1 - (15\gamma^2 + 29\gamma + 42) = 10$, $K_2 = s_2 - (15\gamma^2 + 29\gamma + 42)^2 = 22$, $K_3 = s_3 - (15\gamma^2 + 29\gamma + 42)^3 = 31$ and $K_4 = s_4 - (15\gamma^2 + 29\gamma + 42)^4 = 15$.

Case II: Consider $t = 9$.

We choose $t_0 = t - (t_1 + t_2 + t_3) = 2$ values $\omega_1 = 6$, $\omega_2 = 8$. Assume that $\alpha_1 = 2$, $\alpha_2 = 3$, $\alpha_3 = 4$. Suppose that the users u_{12}, u_{13}, u_{21}, u_{22}, u_{23}, u_{31}, u_{33}, u_{34} and u_{35} collaborate to reconstruct the secrets. The matrix corresponding to their shares is

$$\begin{pmatrix} 1 & 8 & 0 & 0 & 0 & 0 & 0 & 8^2 & 8^3 \\ 1 & 11 & 0 & 0 & 0 & 0 & 0 & 11^2 & 11^3 \\ 0 & 0 & 1 & 3 & 0 & 0 & 0 & 3^2 & 3^3 \\ 0 & 0 & 1 & 5 & 0 & 0 & 0 & 5^2 & 5^3 \\ 0 & 0 & 1 & 9 & 0 & 0 & 0 & 9^2 & 9^3 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2^2 & 2^3 & 2^4 \\ 0 & 0 & 0 & 0 & 1 & 10 & 10^2 & 10^3 & 10^4 \\ 0 & 0 & 0 & 0 & 1 & 12 & 12^2 & 12^3 & 12^4 \\ 0 & 0 & 0 & 0 & 1 & 15 & 15^2 & 15^3 & 15^4 \end{pmatrix} \begin{pmatrix} a_{11}Q \\ a_{12}Q \\ a_{21}Q \\ a_{22}Q \\ a_{31}Q \\ a_{32}Q \\ a_{33}Q \\ \omega_1 Q \\ \omega_2 Q \end{pmatrix} = \begin{pmatrix} (25\gamma^2 + 17\gamma + 24, 39\gamma^2 + 7) \\ (25\gamma^2 + 17\gamma + 24, 39\gamma^2 + 7) \\ (25\gamma^2 + 17\gamma + 24, 39\gamma^2 + 7) \\ (37\gamma^2 + 24\gamma + 41, 2\gamma^2 + 35\gamma + 44) \\ (31\gamma^2 + 25\gamma + 2, 27\gamma^2 + 37\gamma + 19) \\ (37\gamma^2 + 24\gamma + 41, 2\gamma^2 + 35\gamma + 44) \\ (17\gamma^2 + 44\gamma + 39, 41\gamma^2 + 5\gamma + 2) \\ (14\gamma^2 + 24\gamma + 39, 15\gamma^2 + 17\gamma + 10) \\ (22\gamma^2 + 4\gamma + 17, 20\gamma^2 + 6\gamma + 45) \end{pmatrix}.$$

The coefficient matrix of the above system of equations is invertible. The users compute the inverse of the coefficient matrix and multiply it with the shares matrix to get the unknowns. Then they compute the pairing $e(Q, 20Q + 30Q + 45Q) = e((4\gamma + 21, 4\gamma^2 + 15\gamma + 4), (42\gamma^2 + 33\gamma + 10, 20\gamma^2 + 31\gamma + 18)) = 15\gamma^2 + 29\gamma + 42$. Finally, the secrets can be reconstructed as $K_1 = s_1 - (15\gamma^2 + 29\gamma + 42) = 10$, $K_2 = s_2 - (15\gamma^2 + 29\gamma + 42)^2 = 22$, $K_3 = s_3 - (15\gamma^2 + 29\gamma + = 31$ and $K_4 = s_4 - (15\gamma^2 + 29\gamma + 42)^4 = 15$.

We observe that the 13×9 matrix

$$\begin{pmatrix}
1 & 4 & 0 & 0 & 0 & 0 & 0 & 4^2 & 4^3 \\
1 & 8 & 0 & 0 & 0 & 0 & 0 & 8^2 & 8^3 \\
1 & 11 & 0 & 0 & 0 & 0 & 0 & 11^2 & 11^3 \\
1 & 13 & 0 & 0 & 0 & 0 & 0 & 13^2 & 13^3 \\
0 & 0 & 1 & 3 & 0 & 0 & 0 & 3^2 & 3^3 \\
0 & 0 & 1 & 5 & 0 & 0 & 0 & 5^2 & 5^3 \\
0 & 0 & 1 & 9 & 0 & 0 & 0 & 9^2 & 9^3 \\
0 & 0 & 1 & 14 & 0 & 0 & 0 & 14^2 & 14^3 \\
0 & 0 & 0 & 0 & 1 & 2 & 2^2 & 2^3 & 2^4 \\
0 & 0 & 0 & 0 & 1 & 7 & 7^2 & 7^3 & 7^4 \\
0 & 0 & 0 & 0 & 1 & 10 & 10^2 & 10^3 & 10^4 \\
0 & 0 & 0 & 0 & 1 & 12 & 12^2 & 12^3 & 12^4 \\
0 & 0 & 0 & 0 & 1 & 15 & 15^2 & 15^3 & 15^4
\end{pmatrix}$$

has the property that the coefficient matrix corresponding to the shares of any set of (valid) collaborating users is invertible.

The computational complexity of the proposed scheme is examined in detail in the next section.

i. *Complexity of the proposed compartmented multi-secret sharing scheme*

For Case I, it is clearly seen that the time complexity for the scheme is $O(mn^2)$ as seen in Section ii. We compute the time complexity for Case II below. To compute the m matrix multiplications of order $n_i \times (t_i + t_0)$ and $(t_i + t_0) \times 1$, $i = 1, 2, \cdots, m$, we require $\sum_{i=1}^{m} (t_i n_i + n_i t_0)$ operations. Using the *Double-and-Add algorithm* [5], the time for computing scalar multiplication of a point on an elliptic curve is $O(\log_2 \ell)$, where ℓ is the order of the point. There are n scalar multiplications required which cost $O(n \log_2 \ell)$.

At the time of reconstruction, the time computation for finding the inverse of a coefficient matrix of order t, as in Example 2, is $O(t^3)$, which is at most $O(n^3)$. The scheme requires t more scalar multiplications at the time of reconstruction of the secrets. The computational cost for addition of two distinct points on elliptic curve is **I**+2**M**+**S** and for doubling **I**+2**M**+2**S** (see [1], for example), where **I**, **S**, **M** denotes inverse, squaring and multiplication respectively. We need $(m-1)$ additions of the points. So the required computational cost for all point additions is $O(m)$. The computational cost of a pairing is logarithmic in time (see [11, 17], for example) and we required $m+g$ pairing computations. We required g more 1**S** for reconstruction of the secrets K_λ, $1 \le \lambda \le g$. Combining all these, we conclude that the time complexity of the scheme is $O(n^3)$ for Case II.

Comparision with [25]: The paper [25] is based on MDS codes and requires $O(mn^3)$ time computation where n is the number of users and m is the number of compartments. Our scheme is based on elliptic curves and bilinear pairings, for which the scheme will work with less key sizes compared to [25]. Also, our scheme requires $O(mn^2)$ or $O(n^3)$ time computation which is less as compared to [25].

Let T_{MM} = time for computing multiplication of matrices
T_{SM} = time for computing scalar multiplication of a point on elliptic curve
T_{SE} = time for solving the system of equations
T_A = time for computing addition of points on elliptic curve
T_P = time for computing pairing.

Then the time for generating the shares is $mT_{MM} + nT_{SM}$ and the required time for reconstructing the secret is $tT_P + tT_{SM} + (m-1)T_A + T_P + \sum_{i=1}^{m}(t_i - 1)M + 1S$ for the case-I and $T_{SE} + (m-1)T_A + T_P + 1S$ for the case-II, where M denotes the multiplication and S denotes the subtraction. We have skipped the time for computing y_i's as it takes very less time for case-I.

VI. Concluding Remark

We have proposed a multi-secret sharing scheme and a compartmented multi-secret sharing scheme using elliptic curves and bilinear pairings. The proposed schemes are verifiable, which means that the collaborating users can verify the shares of the other collaborators. The required time complexity for the proposed multi-secret sharing scheme is $O(n^2)$ and for

the proposed compartmented multi-secret sharing scheme is either $O(mn^2)$ or $O(n^3)$. The compartmented multi-secret sharing scheme is computationally more efficient than [25].

Acknowledgements

The authors are thankful to the anonymous referees for their valuable comments and suggestions. The third author was supported in part by the Council of Scientific and Industrial Research, India, under award letter 09/414(1146)/2017-EMR-I.

References

[1] R. K. K. Ajeena and K. Hailiza, "The computational complexity of elliptic curve integer sub-decomposition (ISD) method, I," *AIP Conference Proceedings*, vol. 1605, no. 1, AIP (2014).

[2] M. Backes, A. Kate, and A. Patra, "Computational verifiable secret sharing revisited," in *Advances in Cryptology – ASIACRYPT 2011*, D. H. Lee and X. Wang, Eds. Lecture Notes in Computer Science, vol. 7073, Springer, Berlin, Heidelberg, pp. 7073 (2011).

[3] Q. Chen, C. Tang, and Z. Lin, "Efficient explicit constructions of compartmented secret sharing schemes," *Designs, Codes, and Cryptography*, vol. 87, no. 12, pp. 2913-2940 (2019).

[4] Q. Chen, C. Tang, and Z. Lin, "Compartmented secret sharing schemes and locally repairable codes," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 5976-5987 (2020).

[5] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in Proceedings of the 1st International Workshop on Cryptographic Hardware and Embedded Systems (CHES '99), vol. 1717 of Lecture Notes in Computer Science, Springer, pp. 292-302 (1999).

[6] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in 28th Annual Symposium on Foundations of Computer Science (SFCS 1987), pp. 427-438 (1987).

[7] O. Farras, J. Marti-Farre, and C. Padro, "Ideal multipartite secret sharing schemes," *Journal of Cryptology*, vol. 25, no. 3, pp. 434-463 (2012).

[8] G. Frey, M. Müller, and H.-G. Rück, "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1717-1718 (1999).

[9] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, "Secret sharing in multilevel and compartmented groups," in *Proc. ACISP 1998*, LNCS vol. 1438, Springer Verlag, pp. 367-378 (1998).

[10] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in E-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, pp. 67-84 (2007).

[11] S. Ionica and A. Joux, "Pairing computation on elliptic curves with efficiently computable endomorphism and small embedding degree," in *Pairing-Based Cryptography - Pairing 2010*, M. Joye, A. Miyaji, and A. Otsuka, Eds. Lecture Notes in Computer Science, vol. 6487, Springer, Berlin, Heidelberg (2010).

[12] A. Joux, "A one round protocol for tripartite Diffie-Hellman," in Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, vol. 1838, Springer, 2000, pp. 385-393. Full version: *Journal of Cryptology*, vol. 17, pp. 263-276 (2004).

[13] K. E. Lauter and K. E. Stange, "The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences," in *International Workshop on Selected Areas in Cryptography*, Springer: Berlin/Heidelberg, Germany, pp. 309-327 (2018).

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

[15] C. Mejia and J. A. Montoya, "On the information rates of homomorphic secret sharing schemes," *Journal of Information and Optimization Sciences*, vol. 39, no. 7, pp. 1463-1482 (2018), https://doi.org/10.1080/02522667.2017.1367513.

[16] A. Menezes, "An introduction to pairing-based cryptography," in *Recent Trends in Cryptography*, Contemp. Math., vol. 477, Amer. Math. Soc., Providence, RI, pp. 47-65 (2009).

[17] V. Miller, "The Weil pairing, and its efficient calculation," *Journal of Cryptology*, vol. 17, pp. 235-261 (2004), https://doi.org/10.1007/s00145-004-0315-8.

[18] A. Mishra and A. Gupta, "Multi secret sharing scheme using iterative method," *Journal of Information and Optimization Sciences*, vol. 39, no.

3, pp. 631-641 (2018), https://doi.org/10.1080/02522667.2017.1385161.

[19] E. A. Rawashdeh, "A simple method for finding the inverse matrix of Vandermonde matrix," *Matematički Vesnik*, vol. 71, pp. 207-213 (2019).

[20] A. A. Selcuk and R. Yilmaz, "Joint compartmented threshold access structures," *IACR Cryptology ePrint Archive*, 2013/054 (2013). [Online]. Available: https://eprint.iacr.org/2013/054.pdf.

[21] A. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, pp. 612-613 (1979).

[22] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer (1986).

[23] G. Simmons, "How to (really) share a secret," in *Advances in Cryptology - Proceedings of CRYPTO '88*, S. Goldwasser, Ed. Lecture Notes in Computer Science, vol. 403, Springer-Verlag, pp. 390-448 (1990).

[24] T. Tassa and N. Dyn, "Multipartite secret sharing by bivariate interpolation," *J. Cryptol.*, vol. 22, no. 2, pp. 227-258 (2009).

[25] A. N. Tentu, P. Paul, and V. Ch. Venkaiah, "Computationally perfect compartmented secret sharing schemes based on MDS codes," *Int. J. Trust Management in Computing and Communications*, vol. 2, no. 4, pp. 353-378 (2014).

[26] G. Xu, J. Yuan, G. Xu, and Z. Dang, "An efficient compartmented secret sharing scheme based on linear homogeneous recurrence relations," *Security and Communication Networks*, vol. 2021, Article ID 5566179 (2021). [Online]. Available: https://doi.org/10.1155/2021/5566179.

[27] Y. Yu and M. Wang, "A probabilistic secret sharing scheme for a compartmented access structure," in *Information and Communications Security*, Q. S. Susilo, W. Wang, G. Liu, Eds., Lecture Notes in Computer Science, vol. 7043, Springer, Berlin, Heidelberg (2011).

Received September, 2022