Tatra Mt. Math. Publ. **91** (2025), 1–22
DOI: 10.2478/tmmp-2025-0028

TATRA MOUNTAINS
Mathematical Publications

CONJUNCTIVE AND DISJUNCTIVE COMPARTMENTED SECRET SHARING SCHEMES USING ELLIPTIC CURVES

Mohan Chintamani [1] — Prabal Paul[2] — Laba Sa[3]

[1]School of Mathematics and Statistics, University of Hyderabad, Hyderabad - 500046, INDIA

[2]Department of Mathematics, BITS Pilani, K K Birla Goa Campus, Goa - 403726, INDIA

[3]Department of Mathematics, MATS University, Raipur - 493441, INDIA

ABSTRACT. This article considers two secret sharing schemes, namely, conjunctive compartmented and disjunctive compartmented. Suppose a group of companies having many compartments is working on a project. In the conjunctive compartmented scheme, a specified number of users from each compartment of every company has to collaborate to access the secret key. While in a disjunctive compartmented scheme, any company with a predetermined number of users from each compartment can get the secret key. The schemes we have proposed use elliptic curves and bilinear pairings. Our schemes are verifiable and efficient. The proposed schemes are illustrated in full detail by concrete examples using SageMath.

1. Introduction

A secret sharing scheme is a method to distribute a secret among the participants, each receiving a portion of the secret, called a share. A predetermined set of users, called an *authorized* set, pools their shares to reconstruct the secret. An access structure for a secret sharing scheme is the collection of all authorized subsets of users. Many secret sharing schemes have been proposed in the literature, see [5,17,24]. G. Simmons [19], in 1990, introduced a compartmented secret sharing scheme, which is a generalization of threshold secret sharing schemes. For more generalization of threshold secret sharing, we refer to [6]. In a compartmented secret sharing scheme, users are divided into distinct compartments.

2020 Mathematics Subject Classification: 11T71, 94A60, 94A62.
Keywords: elliptic curves, bilinear pairings, secret sharing, compartmented access structure.

If the overall number of participants reaches a global threshold and the number of participants from each compartment exceeds a predefined compartment threshold, the secret can be reconstructed. An access structure for the compartmented secret sharing scheme is defined below.

Compartmented access structure

Let $U = \{u_1, u_2, \ldots, u_n\}$ be a collection of n users, partitioned into m disjoint compartments $U_1, U_2, \ldots, U_m$. Let $t_i \geq 1$ be the threshold number for each compartment U_i and $t \geq \sum_{i=1}^{m} t_i$ be the global threshold number. The compartmented access structure is described as the collection of all subsets of t (or more) number of users with at least t_i users from compartment U_i, $1 \leq i \leq m$. Mathematically, the access structure is

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

Remark 1. In view of terminologies and notations as in [6], the access structure above is a m-partite access structure. It is completely described by the family $\min \Gamma$ of the minimal qualified subsets of Γ, where

$$\min \Gamma = \{u \in \mathbb{Z}_+^m \colon |u| = t \text{ and } u \geq (t_1, t_2, \ldots, t_m)\}.$$

For more detailed discussions on classification of ideal access structure using matroid theory, we refer to [7].

Many compartmented secret sharing schemes have been proposed using polynomials [9, 16, 23] and Chinese Remainder Theorem [10], and many others [3, 21, 22]. The scheme [3] is based on locally repairable codes. The paper [9] uses polynomials and needs a secure channel for distributing the shares. A computationally perfect compartmented secret sharing scheme has been proposed using MDS codes in [21]. In the paper [16], the authors introduced a joint compartmented threshold access structure, where the compartments are not necessarily disjoint.

In [20], the authors considered a compartmented secret sharing scheme with *an upper bound*. The access structure limits the number of participants from each compartment. Their scheme is based on a bivariate polynomial and uses the Schwartz-Zippel lemma about the number of zeros of a polynomial.

In this article, we propose the *conjunctive* and *disjunctive* compartmented schemes. The proposed scheme uses elliptic curves [18] and bilinear pairings [12, 13]. Our scheme is verifiable and computationally secure. For the illustration purpose, we give an explicit example.

Motivation

A group of companies wants to merge for a project. The companies have their individual and global secret keys. Each company has some compartments. In a conjunctive compartmented secret sharing scheme, if a particular (threshold) number of users from each compartment of every company collaborates, they can get the global secret. While in a disjunctive compartmented secret sharing scheme, a particular number of users from each compartment of any company are allowed to collaborate and reconstruct the global secret.

We have organized our article as follows. In Section 2, the elliptic curves and bilinear pairings are defined. Proposed conjunctive and disjunctive compartmented secret sharing schemes have been described in Section 3. Security analysis and examples of the proposed schemes are presented in Section 4. In Section 5, we discuss the complexity of the schemes.

2. Preliminaries

Consider an elliptic curve

$$E: y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6 \quad \text{over} \quad \mathbb{F}_q$$

with discriminant not equal to zero, where q is a prime power and

$$c_i \in \mathbb{F}_q \quad \text{for all} \quad i = 1, 2, 3, 4, 6.$$

The set $E(\mathbb{F}_q)$ of points on elliptic curve forms a group with the point at infinity $\mathcal{O}$ as its identity. If the characteristic of the field $\mathbb{F}_q$ is not equal to 2 and 3, then the elliptic curve E can be transformed into another form of the elliptic curve, namely, $E': y^2 = x^3 + ax + b$.

Definition 2.1 (Bilinear Pairings)**.** Let G_a, G_m be an additive cyclic group and a multiplicative cyclic group, respectively, with the same prime order ℓ. A bilinear pairing e is a map

$$e: G_a \times G_a \longrightarrow G_m$$

which satisfies the bilinearity, non-degeneracy and computability properties.

One of the important property of a bilinear pairing e is that, for $x, y \in G_a$ with $x \neq 0$, $\mathrm{e}(x, y) = \mathrm{e}(x, y')$ implies that $y = y'$.

For more discussion on bilinear pairings, we refer to [2, 13, 14].

Many pairings have been defined using elliptic curves. For example, suppose ℓ is a prime divisor of the 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 collection of ℓ-torsion points in $E(\mathbb{F}_{q^k})$ is denoted by $E[\ell]$. The *modified* Tate pairing e is a map $\mathrm{e} : E[\ell] \times E[\ell] \longrightarrow \mu_\ell$,

where μ_ℓ is the order-ℓ subgroup of $\mathbb{F}_{q^k}^*$. We refer to [8, 13] for more details. One can use modified Tate pairing, Weil pairing [14] and other similar kinds of pairings in our schemes.

3. Proposed conjunctive and disjunctive compartmented secret sharing schemes

3.1. Setting up and distribution of the parameters of the schemes

Consider an elliptic curve E over a finite field $\mathbb{F}_q$, where $q = p^r$ for some $r \in \mathbb{N}$ and p is a large prime number. Let $P \in E(\mathbb{F}_q)$ and $G_a = \langle P \rangle$ be a subgroup of $E(\mathbb{F}_q)$ of order ℓ, where ℓ is a prime number. We choose ℓ to be a large prime so that *elliptic curve discrete logarithm problem* (ECDLP) is hard to solve. That is, given the points P and bP on an elliptic curve, it is hard to find the integer b. Let $G_m = \mu_\ell$ where μ_ℓ is as above. Consider a bilinear pairing e as in the above definition.

Let $C_1, C_2, \ldots, C_m$ be m companies interested to merge for a project. Each company C_i has τ_i compartments, say $C_{i1}, C_{i2}, \ldots, C_{i\tau_i}$ for $1 \le i \le m$. Suppose there is a set U of n users divided disjointly into these compartments in the presence of a *trusted* Dealer. The Dealer has the authority to generate and publish the parameters for the schemes. Let n_{ij} be the number of users in the compartment C_{ij} for $1 \le i \le m$ and $1 \le j \le \tau_i$. Let $t_{ij} \ge 1$ be the threshold number for each C_{ij} and $t_i \ge \sum t_{ij}$ be the company threshold of C_i. We define the *conjunctive compartmented access structure* as

$$\Gamma_1 = \{A \subseteq U : \text{ for each } i, 1 \le i \le m, |A \cap C_i| \ge t_i \text{ and } |A \cap C_{ij}| \ge t_{ij} \text{ for all } j, 1 \le j \le \tau_i\}.$$

Similarly, the *disjunctive compartmented access structure* is defined as

$$\Gamma_2 = \{A \subseteq U : \text{ for some } i, 1 \le i \le m, |A \cap C_i| \ge t_i \text{ and } |A \cap C_{ij}| \ge t_{ij} \text{ for all } j, 1 \le j \le \tau_i\}.$$

Let $a_{j1}^{(i)}, a_{j2}^{(i)}, \ldots, a_{jt_{ij}}^{(i)} \in [0, \ell - 1]$ be t_{ij} random integers, with $a_{j1}^{(i)} \ne 0$, for each compartment

$$C_{ij},\ 1 \le i \le m \quad \text{and} \quad 1 \le j \le \tau_i.$$

Let $u_{jk}^{(i)}$ denote k^{th} user in the compartment C_{ij} of company C_i, where

$$1 \le i \le m,\ 1 \le j \le \tau_i \quad \text{and} \quad 1 \le k \le n_{ij}.$$

For both the conjunctive and the disjunctive cases shares are distributed the same way. We consider the following two cases.

Case I. $t_i = \sum_{j=1}^{\tau_i} t_{ij}$ (i.e., company threshold t_i is equal to sum of compartment thresholds in C_i).

- The Dealer chooses a matrix M_{ij} of order $n_{ij} \times t_{ij}$ for each C_{ij}, $1 \leq i \leq m$ and $1 \leq j \leq \tau_i$, having the following property. Any submatrix of M_{ij} consisting of t_{ij} rows is invertible. Such matrices are known as MDS matrices [15]. All the arithmetic is done modulo the prime ℓ.
- The Dealer computes
$$\left(b_{j1}^{(i)}, b_{j2}^{(i)}, \ldots, b_{jn_{ij}}^{(i)}\right)^T = M_{ij} \cdot \left(a_{j1}^{(i)}, a_{j2}^{(i)}, \ldots, a_{jt_{ij}}^{(i)}\right)^T$$
for each compartment C_{ij}, $1 \leq i \leq m$ and $1 \leq j \leq \tau_i$, where A^T denotes transpose of the matrix A.
- The users $u_{j1}^{(i)}, u_{j2}^{(i)}, \ldots, u_{jn_{ij}}^{(i)}$ in the compartment C_{ij} randomly choose private keys $x_{j1}^{(i)}, x_{j2}^{(i)}, \ldots, x_{jn_{ij}}^{(i)} \in [1, \ell - 1]$, respectively and make $x_{j1}^{(i)}P$, $x_{j2}^{(i)}P$, $\ldots$, $x_{jn_{ij}}^{(i)}P$ public.
- Then the Dealer computes $b_{j1}^{(i)}x_{j1}^{(i)}P$, $b_{j2}^{(i)}x_{j2}^{(i)}P$, $\ldots$, $b_{jn_{ij}}^{(i)}x_{jn_{ij}}^{(i)}P$ for users in each compartment C_{ij} of C_i and sends (publicly) to the respective users in C_{ij}.
- The users $u_{j1}^{(i)}, u_{j2}^{(i)}, \ldots, u_{jn_{ij}}^{(i)}$ in C_{ij} will get their respective shares $b_{j1}^{(i)}P$, $b_{j2}^{(i)}P$, $\ldots$, $b_{jn_{ij}}^{(i)}P$ by computing
$$x_{j1}^{(i)^{-1}}\left(b_{j1}^{(i)}x_{j1}^{(i)}P\right),\ x_{j2}^{(i)^{-1}}\left(b_{j2}^{(i)}x_{j2}^{(i)}P\right),\ \ldots,\ x_{jn_{ij}}^{(i)\ \ -1}\left(b_{jn_{ij}}^{(i)}x_{jn_{ij}}^{(i)}P\right).$$

Case II. $t_i > \sum_{j=1}^{\tau_i} t_{ij}$ (i.e., company threshold t_i is greater than sum of compartment thresholds in C_i).

Let $t_i' = t_i - \sum_{j=1}^{\tau_i} t_{ij}$. For each j, $1 \leq j \leq \tau_i$, the Dealer chooses a matrix A_{ij} of size $n_{ij} \times t_{ij}$ and a matrix B_i of size $\sum_{j=1}^{\tau_i} n_{ij} \times t_i'$, and considers the matrix

$$A_i = \left(\begin{array}{ccccc|c} A_{i1} & O & \cdots & O & O & \\ O & A_{i2} & \cdots & O & O & \\ \vdots & \vdots & \ddots & \vdots & \vdots & B_i \\ O & O & \cdots & A_{i(\tau_i-1)} & O & \\ O & O & \cdots & O & A_{i\tau_i} & \end{array}\right).$$

The choice of A_{ij}'s and B_i is such that the submatrix of A_i corresponding to any set of t_i collaborating users is invertible. We show the existence of such matrices by explicit computation. See Example 1 below. Using a simple counting argument, when the prime number ℓ is large enough, with overwhelming probability the matrix with randomly chosen entries will satisfy this property.

Similarly to the MDS case, constructing efficiently such matrices in general is an open problem.

The Dealer chooses t'_i random values $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{it'_i} \in [0, \ell - 1]$ for company C_i, $1 \le i \le m$. For each $1 \le i \le m$, $1 \le j \le \tau_i$ and $1 \le k \le n_{ij}$, let $b_{jk}^{(i)}$ be defined by

$$\left(b_{11}^{(i)}, b_{12}^{(i)}, \ldots, b_{1n_{i1}}^{(i)}, \ldots, b_{\tau_i 1}^{(i)}, b_{\tau_i 2}^{(i)}, \ldots, b_{\tau_i n_{i\tau_i}}^{(i)}\right)^T =$$
$$A_i \cdot \left(a_{11}^{(i)}, \ldots, a_{1t_{i1}}^{(i)}, \ldots, a_{\tau_i 1}^{(i)}, \ldots, a_{\tau_i t_{i\tau_i}}^{(i)}, \alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{it'_i}\right)^T$$

for users in each company C_i for $1 \le i \le m$. The Dealer distributes the shares $b_{jk}^{(i)} P$ to the users in C_{ij} as in Case I.

We consider e to be the modified Tate pairing as defined in [13].

For conjunctive compartmented secret sharing scheme

The Dealer chooses company secret keys $K_1, K_2, \ldots, K_m \in \mu_\ell$ (the target of the bilinear pairing) for C_1, C_2, $\ldots, C_m$, respectively and sets the global secret key $K = K_1 + K_2 + \cdots + K_m$. The Dealer computes

$$s_i = \prod_{j=1}^{\tau_i} \mathrm{e}\left(P, a_{j1}^{(i)} P\right) + K_i \quad \text{or equivalently} \quad s_i = \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)} P\right) + K_i.$$

Finally, the Dealer makes P, M_{ij}, A_i and s_i public.

For disjunctive compartmented secret sharing scheme

The Dealer chooses a global secret $K \in \mu_\ell$ and computes

$$s_i = \prod_{j=1}^{\tau_i} \mathrm{e}\left(P, a_{j1}^{(i)} P\right) + K \quad \text{or equivalently} \quad s_i = \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)} P\right) + K$$

for each company C_i. Finally, the Dealer makes P, M_{ij}, A_i and s_i public.

Remark 2. We note that (see [13]), for any $P_1, P_2 \in E[\ell]$, the pairing

$$\mathrm{e}(P_1, P_2) \in \mu_\ell \subseteq \mathbb{F}_{q^k}^* \subseteq \mathbb{F}_{q^k}.$$

Also, for any $K \in \mu_\ell$, we have $K \in \mathbb{F}_{q^k}$. Thus $\mathrm{e}(P_1, P_2) + K$ is in $\mathbb{F}_{q^k}$.

3.2. Reconstruction of the secret key

- *For conjunctive compartmented secret sharing scheme.*
  For Case I: suppose that t_{ij} (or more) users from each compartment C_{ij}, $1 \le j \le \tau_i$, of every company C_i, $1 \le i \le m$, collaborate. Without loss of generality, assume that the users $u_{j1}^{(i)}, u_{j2}^{(i)}, \ldots, u_{jt_{ij}}^{(i)}$ from each C_{ij} of C_i, $1 \le i \le m$, collaborate. Then the collaborating users from

the compartment C_{ij} can form an invertible submatrix M'_{ij} of M_{ij} (by assumption on M_{ij}, the submatrix M'_{ij} is invertible). The users in C_{ij} compute

$$\left(a_{j1}^{(i)}P, a_{j2}^{(i)}P, \ldots, a_{jt_{ij}}^{(i)}P\right)^T = M_{ij}'^{-1} \cdot \left(b_{j1}^{(i)}P, b_{j2}^{(i)}P, \ldots, b_{jt_{ij}}^{(i)}P\right)^T.$$

Thus the company secret K_i can be computed as

$$K_i = s_i - \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)}P\right)$$

and hence the global secret key K can be computed as

$$K = K_1 + K_2 + \cdots + K_m.$$

For Case II: suppose that at least t_{ij} users from each compartment C_{ij}, $1 \le j \le \tau_i$ and t_i users from each company C_i, $1 \le i \le m$, collaborate. Without loss of generality, assume that the users $u_{j1}^{(i)}$, $u_{j2}^{(i)}$, $\ldots$, $u_{j\beta_{ij}}^{(i)}$ from compartment C_{ij} of company C_i, $1 \le i \le m$, collaborate, where

$$\beta_{ij} \ge t_{ij} \text{ for all } i, j \quad \text{and} \quad \sum_{j=1}^{\tau_i} \beta_{ij} = t_i.$$

The collaborating users in C_i can form an invertible submatrix A'_i of A_i and compute

$$(a_{11}^{(i)}P, \ldots, a_{1t_{i1}}^{(i)}P, \ldots, a_{\tau_i 1}^{(i)}P, \ldots, a_{\tau_i t_{i\tau_i}}^{(i)}P, \alpha_{i1}P, \ldots, \alpha_{it'_i}P)^T =$$
$$A_i'^{-1}(b_{11}^{(i)}P, \ldots, b_{1\beta_{i1}}^{(i)}P, \ldots, b_{\tau_i 1}^{(i)}P, \ldots, b_{\tau_i \beta_{i\tau_i}}^{(i)}P).$$

Thus they can compute company secret K_i as

$$K_i = s_i - \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)}P\right), \quad 1 \le i \le m$$

and hence the global secret key K as $K = K_1 + K_2 + \cdots + K_m$.

- *For disjunctive compartmented secret sharing scheme.*
  The authorized set of users can compute $\sum_{j=1}^{\tau_i} a_{j1}^{(i)}P$, $1 \le i \le m$, as in the previous reconstruction of the secret key of the conjunctive compartmented secret sharing scheme. Then the users in any company C_i can compute the global secret key

$$K = s_i - \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)}P\right).$$

3.3. Verification of the shares

In the secret reconstruction phase, each collaborating user u_{ij} submits their share along with additional information $x_{ij}^{-1}P$ for verification. The legitimacy of the shares $b'_{ij}P$ sent by each user can be confirmed by validating the equation

$$\mathrm{e}(x_{ij}^{-1}P, b_{ij}x_{ij}P) = \mathrm{e}(P, b'_{ij}P).$$

The equation holds true if and only if $b'_{ij}b_{ij}^{-1} \equiv 1 \pmod{\ell}$, which is equivalent to $b'_{ij} \equiv b_{ij} \pmod{\ell}$ (as per [2, Remark 1]).

4. Security analysis of the proposed schemes

The security of the proposed schemes is based on the presence of a trusted Dealer, the hardness of ECDLP and the bilinear pairings. Bilinear pairing operates as a one-way function, which implies that computing the image of inputs is simple but finding the pre-image of a given image is challenging. The Dealer encrypts the shares before sending (publicly) them to the users. We have assumed that the ECDLP is difficult to solve for large order group G_a. So an attacker cannot obtain $b_{ij}^{(k)}P$ when the Dealer distributes the encrypted share $b_{ij}^{(k)}x_{ij}^{(k)}P$ as it is equivalent to solving an instance of ECDLP. By the property of pairing e, given a point P and a value S, for an adversary, the probability of guessing a point Q that satisfies $S - \mathrm{e}(P, Q) = K$ is $1/(\ell - 1)$. Also the probability of guessing a K' in μ_ℓ that is equal to K is $1/\ell$. Therefore, the probability of getting the secret is $\max\{1/(\ell-1), 1/\ell\}$. Since ℓ is very large, the probability is very small. Thus, the announcement of many public parameters has no effect on the security of the scheme.

We need the following (see [2]) basic result from linear algebra.

Proposition 4.1. *A system of linear equations over a finite field of order ℓ with t unknowns has either a unique solution, no solution or ℓ^λ solutions for some λ with $1 \le \lambda \le t$. Each solution is of equal probability for the case of ℓ^λ solutions.*

Theorem 4.2. *Any $t_i - 1$(or fewer) users from the company C_i cannot reveal the company secret K_i.*

Proof. Let $\mathcal{A}$ be a set of $t_i - 1$ (or less) users in the comapany C_i who try to get the company secret K_i. In the case $t_i = \sum_{j=1}^{\tau_i} t_{ij}$, there exists at least one compartment C_{ij} for which

$$|\mathcal{A} \cap C_{ij}| < t_{ij}.$$

Without loss of generality, assume that the users $u_{j1}^{(i)}, u_{j2}^{(i)}, \ldots, u_{j(t_{ij}-1)}^{(i)}$ from the compartment C_{ij} pool their shares. Then the shares of the users can

be written as the system of equations

$$\left(b_{j1}^{(i)}P, b_{j2}^{(i)}P, \ldots, b_{j(t_{ij}-1)}^{(i)}P\right)^T = M'_{ij} \cdot \left(a_{j1}^{(i)}P, a_{j2}^{(i)}P, \ldots, a_{jt_{ij}}^{(i)}P\right)^T,$$

where M'_{ij} is the submatrix (of M_{ij}) corresponding to the shares of the users in $\mathcal{A}$. The system will have many solutions by Proposition 4.1. Thus, the users cannot get $a_{j1}^{(i)}P$. Similarly, in the case $t_i > \sum_{j=1}^{\tau_i} t_{ij}$, there are two possibilities:

- There must be a compartment C_{ij} in which $\beta_{ij} = |\mathcal{A} \cap C_{ij}| < t_{ij}$. This implies that the unknowns $a_{j1}^{(i)}P$, $1 \le j \le \tau_i$, cannot be computed.
- All $\beta_{ij} \ge t_{ij}$ but $\sum_{j=1}^{\tau_i} \beta_{ij} < t_i$. Then the users can form a system of equations with t_i variables and less than t_i equations. Thus, by Proposition 4.1, users cannot get $a_{j1}^{(i)}P$, $1 \le j \le \tau_i$.

Hence they cannot get the company secret key K_i. □

Remark 3. We observe that any set $\mathcal{A}$ of unauthorized users cannot access the global secret K. For example, suppose that $\mathcal{A}$ is a set of unauthorized users. In case of conjunctive scheme, it means that $\mathcal{A} \notin \Gamma_1$. Thus either $|\mathcal{A} \cap C_i| < t_i$ for some i or else $|\mathcal{A} \cap C_{ij}| < t_{ij}$ for some i and j. By Theorem 4.2, the condition $|\mathcal{A} \cap C_i| < t_i$ implies that users in $\mathcal{A}$ cannot get the company secret K_i and hence the global secret K. In the later case ($|\mathcal{A} \cap C_{ij}| < t_{ij}$), the users in $\mathcal{A}$ need to solve a system of equations with more unknowns than the number of equations to get the secret K_i. By Proposition 4.1, this system has ℓ^λ many solutions for some $\lambda \ge 1$. As ℓ is large, the probability of getting K_i (and hence K) is negligible.

In case of disjunctive secret sharing scheme, we have the similar arguments.

Observation 4.3. *Let us choose $Q \in E[\ell]$ uniformly, K as described above, and compute $s = \mathrm{e}(P, Q) + K$. Then for any $\bar{s}$ the conditional distribution of K given $s = \bar{s}$ is the same as its original, unconditional distribution.*

The point $Q \in G_a \subseteq E[\ell]$ is chosen at random and the order of G_a is ℓ. For a given P, there is a unique point Q that satisfies

$$s_i - \mathrm{e}(P, Q) = K \quad \text{or} \quad s_i - \mathrm{e}(P, Q) = K_i.$$

We have given below an example of the proposed schemes using modified Tate pairing [13]. The computations are done using SageMath.

Example 1. Consider an elliptic curve $E: y^2 = x^3 + 2x + 15$ over the field $\mathbb{F}_{47}$. The number of points in $E(\mathbb{F}_{47})$ is 61. The embedding degree of $E(\mathbb{F}_{47})$ with respect to 61 is 3 as $61 | 47^3 - 1$. Then $\mathbb{F}_{47^3}$ is the extended finite field.

The number of points in $E(\mathbb{F}_{47^3})$ is 104188. Let γ be a root of an irreducible cubic polynomial over $\mathbb{F}_{47}$. The group $E[61] \subseteq E(\mathbb{F}_{47^3})$ is the set of all 61-torsion points [13]. Let

$$P = (15\gamma + 33, 9\gamma^2 + 22\gamma + 23) \in E[61] \quad \text{and} \quad G_a = \langle P \rangle.$$

We have $\ell = 61$ and all the matrix computations are done modulo ℓ.
Assume that there are two companies C_1 and C_2:

- company C_1 has thre compartments, namely, C_{11}, C_{12}, C_{13}, and
- company C_2 has three compartments, namely, C_{21}, C_{22}, C_{23}.

Suppose that

$$n_{11} = 3, \quad n_{12} = 4, \quad n_{13} = 5, \quad n_{21} = 3, \quad n_{22} = 3, \quad n_{23} = 4$$

and

$$t_{11} = 2, \quad t_{12} = 2, \quad t_{13} = 3, \quad t_{21} = 2, \quad t_{22} = 2, \quad t_{23} = 3.$$

Let

$$a_{11}^{(1)} = 32, \quad a_{12}^{(1)} = 23, \quad a_{21}^{(1)} = 14, \quad a_{22}^{(1)} = 19, \quad a_{31}^{(1)} = 37, \quad a_{32}^{(1)} = 52, \quad a_{33}^{(1)} = 43,$$

$$a_{11}^{(2)} = 25, \quad a_{12}^{(2)} = 36, \quad a_{21}^{(2)} = 51, \quad a_{22}^{(2)} = 28, \quad a_{31}^{(2)} = 8, \quad a_{32}^{(2)} = 4, \quad a_{33}^{(2)} = 7.$$

We choose company secret keys $K_1 = 25\gamma^2 + 44\gamma + 44, K_2 = 27\gamma^2 + 44\gamma + 41$ for C_1, C_2 respectively and the global secret key $K = 5\gamma^2 + 41\gamma + 38$.

Case I. For $t_1 = t_{11} + t_{12} + t_{13} = 7$ and $t_2 = t_{21} + t_{22} + t_{23} = 7$.
For company C_1, let

$$M_{11} = \begin{pmatrix} 8 & 3 \\ 11 & 60 \\ 12 & 22 \end{pmatrix}, \quad M_{12} = \begin{pmatrix} 3 & 9 \\ 15 & 42 \\ 9 & 20 \\ 20 & 34 \end{pmatrix} \quad \text{and} \quad M_{13} = \begin{pmatrix} 21 & 14 & 50 \\ 37 & 27 & 23 \\ 39 & 57 & 27 \\ 31 & 46 & 23 \\ 40 & 14 & 11 \end{pmatrix}.$$

We compute

$$\left(b_{11}^{(1)}, b_{12}^{(1)}, b_{13}^{(1)}\right)^T = M_{11} \cdot \left(a_{11}^{(1)}, a_{12}^{(1)}\right)^T = (20, 24, 36)^T.$$

The shares of the users in the compartment C_{11} of the company C_1 are

$$\begin{pmatrix} b_{11}^{(1)} P \\ b_{12}^{(1)} P \\ b_{13}^{(1)} P \end{pmatrix} = \begin{pmatrix} (20\gamma^2 + 41\gamma + 45, 37\gamma^2 + 19\gamma + 18) \\ (18\gamma^2 + 17\gamma + 21, 19\gamma^2 + 13\gamma + 11) \\ (15\gamma^2 + 27\gamma + 41, 18\gamma^2 + 36\gamma + 44) \end{pmatrix}.$$

Compute

$$\left(b_{21}^{(1)}, b_{22}^{(1)}, b_{23}^{(1)}, b_{24}^{(1)}\right)^T = M_{12} \cdot \left(a_{21}^{(1)}, a_{22}^{(1)}\right)^T = (30, 32, 18, 11)^T.$$

The shares of the users in the compartment C_{12} of the company C_1 are

$$\begin{pmatrix} b_{21}^{(1)}P \\ b_{22}^{(1)}P \\ b_{23}^{(1)}P \\ b_{24}^{(1)}P \end{pmatrix} = \begin{pmatrix} (44\gamma^2+27\gamma, 19\gamma^2+22\gamma+22) \\ (14\gamma^2+13\gamma+15, 18\gamma^2+5\gamma+29) \\ (17\gamma^2+6, 41\gamma^2+2\gamma+1) \\ (42\gamma^2+22\gamma+34, 24\gamma^2+27\gamma+34) \end{pmatrix}.$$

Compute

$$\left(b_{31}^{(1)}, b_{32}^{(1)}, b_{33}^{(1)}, b_{34}^{(1)}, b_{35}^{(1)}\right)^T = M_{13} \cdot \left(a_{31}^{(1)}, a_{32}^{(1)}, a_{33}^{(1)}\right)^T = (56, 41, 17, 14, 58)^T.$$

The shares of the users in the compartment C_{13} of the company C_1 are

$$\begin{pmatrix} b_{31}^{(1)}P \\ b_{32}^{(1)}P \\ b_{33}^{(1)}P \\ b_{34}^{(1)}P \\ b_{35}^{(1)}P \end{pmatrix} = \begin{pmatrix} (34\gamma^2+31\gamma+35, 39\gamma^2+3\gamma+42) \\ (20\gamma^2+41\gamma+45, 10\gamma^2+28\gamma+29) \\ (30\gamma^2+23\gamma, 19\gamma^2+17\gamma+27) \\ (26\gamma^2+7\gamma+12, 45\gamma^2+14\gamma+21) \\ (38\gamma^2+12\gamma+39, 32\gamma^2+24\gamma+34) \end{pmatrix}.$$

For company C_2, let

$$M_{21} = \begin{pmatrix} 13 & 47 \\ 25 & 15 \\ 16 & 12 \end{pmatrix}, \quad M_{22} = \begin{pmatrix} 42 & 56 \\ 32 & 48 \\ 17 & 45 \end{pmatrix} \quad \text{and} \quad M_{23} = \begin{pmatrix} 28 & 52 & 53 \\ 10 & 39 & 24 \\ 55 & 36 & 28 \\ 38 & 41 & 33 \end{pmatrix}.$$

We compute

$$\left(b_{11}^{(2)}, b_{12}^{(2)}, b_{13}^{(2)}\right)^T = M_{21} \cdot \left(a_{11}^{(2)}, a_{12}^{(2)}\right)^T = (4, 6, 39)^T.$$

The shares of the users in the compartment C_{21} of the company C_2 are

$$\begin{pmatrix} b_{11}^{(2)}P \\ b_{12}^{(2)}P \\ b_{13}^{(2)}P \end{pmatrix} = \begin{pmatrix} (46\gamma^2+46\gamma+29, 2\gamma^2+14\gamma+4) \\ (2\gamma^2+7\gamma+45, 8\gamma^2+14\gamma+22) \\ (15\gamma^2+7\gamma+3, 36\gamma^2+39\gamma+45) \end{pmatrix}.$$

Compute

$$\left(b_{21}^{(2)}, b_{22}^{(2)}, b_{23}^{(2)}\right)^T = M_{22} \cdot \left(a_{21}^{(2)}, a_{22}^{(2)}\right)^T = (50, 48, 53)^T.$$

The shares of the users in the compartment C_{22} of the company C_2 are

$$\begin{pmatrix} b_{21}^{(2)}P \\ b_{22}^{(2)}P \\ b_{23}^{(2)}P \end{pmatrix} = \begin{pmatrix} (42\gamma^2+22\gamma+34, 23\gamma^2+20\gamma+13) \\ (32\gamma^2+36\gamma+18, 32\gamma^2+38\gamma+35) \\ (30\gamma^2+13\gamma+8, 14\gamma^2+21\gamma+15) \end{pmatrix}.$$

Compute

$$\left(b_{31}^{(2)}, b_{32}^{(2)}, b_{33}^{(2)}, b_{34}^{(2)}\right)^T = M_{23} \cdot \left(a_{31}^{(2)}, a_{32}^{(2)}, a_{33}^{(2)}\right)^T = (10, 38, 48, 28)^T.$$

The shares of the users in the compartment C_{23} of the company C_2 are

$$\begin{pmatrix} b_{31}^{(2)}P \\ b_{32}^{(2)}P \\ b_{33}^{(2)}P \\ b_{34}^{(2)}P \end{pmatrix} = \begin{pmatrix} (25\gamma^2+34\gamma+14,\ 40\gamma^2+22\gamma+20) \\ (16\gamma^2+40\gamma+37,\ 30\gamma^2+5\gamma+36) \\ (32\gamma^2+36\gamma+18,\ 32\gamma^2+38\gamma+35) \\ (45\gamma^2+27\gamma+19,\ 45\gamma^2+6\gamma) \end{pmatrix}.$$

Case II. For $t_1 > t_{11}+t_{12}+t_{13} = 7$ and $t_2 > t_{21}+t_{22}+t_{23} = 7$. Let $t_1 = 9$ and $t_2 = 8$. Then $t_1' = 2$ and $t_2' = 1$. So choose

$$\alpha_{11} = 3, \alpha_{12} = 35 \quad \text{and} \quad \alpha_{21} = 47.$$

For company C_1, we choose a matrix

$$A_1 = \begin{pmatrix} 8 & 3 & 0 & 0 & 0 & 0 & 0 & 24 & 9 \\ 11 & 60 & 0 & 0 & 0 & 0 & 0 & 50 & 1 \\ 12 & 22 & 0 & 0 & 0 & 0 & 0 & 20 & 57 \\ 0 & 0 & 3 & 9 & 0 & 0 & 0 & 27 & 20 \\ 0 & 0 & 15 & 42 & 0 & 0 & 0 & 20 & 56 \\ 0 & 0 & 9 & 20 & 0 & 0 & 0 & 58 & 34 \\ 0 & 0 & 20 & 34 & 0 & 0 & 0 & 9 & 58 \\ 0 & 0 & 0 & 0 & 21 & 14 & 50 & 13 & 29 \\ 0 & 0 & 0 & 0 & 37 & 27 & 23 & 58 & 11 \\ 0 & 0 & 0 & 0 & 39 & 57 & 27 & 16 & 14 \\ 0 & 0 & 0 & 0 & 31 & 46 & 23 & 42 & 21 \\ 0 & 0 & 0 & 0 & 40 & 14 & 11 & 13 & 32 \end{pmatrix}$$

for users in company C_1. We compute

$$\begin{aligned} &\left(b_{11}^{(1)}, b_{12}^{(1)}, b_{13}^{(1)}, b_{21}^{(1)}, b_{22}^{(1)}, b_{23}^{(1)}, b_{24}^{(1)}, b_{31}^{(1)}, b_{32}^{(1)}, b_{33}^{(1)}, b_{34}^{(1)}, b_{35}^{(1)}\right)^T \\ &= A_1 \cdot \left(a_{11}^{(1)}, a_{12}^{(1)}, a_{21}^{(1)}, a_{22}^{(1)}, a_{31}^{(1)}, a_{32}^{(1)}, a_{33}^{(1)}, \alpha_{11}, \alpha_{12}\right)^T \\ &= (41, 26, 17, 18, 39, 40, 55, 12, 51, 6, 21, 58)^T. \end{aligned}$$

The shares of the users of the company C_1 are

$$\begin{pmatrix} b_{11}^{(1)}P \\ b_{12}^{(1)}P \\ b_{13}^{(1)}P \\ b_{21}^{(1)}P \\ b_{22}^{(1)}P \\ b_{23}^{(1)}P \\ b_{24}^{(1)}P \\ b_{31}^{(1)}P \\ b_{32}^{(1)}P \\ b_{33}^{(1)}P \\ b_{34}^{(1)}P \\ b_{35}^{(1)}P \end{pmatrix} = \begin{pmatrix} (20\gamma^2+41\gamma+45, 10\gamma^2+28\gamma+29) \\ (11\gamma^2+30\gamma+5, 15\gamma^2+37\gamma+2) \\ (30\gamma^2+23\gamma, 19\gamma^2+17\gamma+27) \\ (17\gamma^2+6, 41\gamma^2+2\gamma+1) \\ (15\gamma^2+7\gamma+3, 36\gamma^2+39\gamma+45) \\ (22\gamma^2+43, 4\gamma^2+28\gamma+32) \\ (2\gamma^2+7\gamma+45, 39\gamma^2+33\gamma+25) \\ (18\gamma^2+9\gamma+41, 14\gamma^2+46\gamma+32) \\ (25\gamma^2+34\gamma+14, 7\gamma^2+25\gamma+27) \\ (2\gamma^2+7\gamma+45, 8\gamma^2+14\gamma+22) \\ (22\gamma^2+43, 43\gamma^2+19\gamma+15) \\ (38\gamma^2+12\gamma+39, 32\gamma^2+24\gamma+34) \end{pmatrix}.$$

For company C_2, we choose a matrix

$$A_2 = \begin{pmatrix} 13 & 47 & 0 & 0 & 0 & 0 & 0 & 1 \\ 25 & 15 & 0 & 0 & 0 & 0 & 0 & 9 \\ 16 & 12 & 0 & 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 42 & 56 & 0 & 0 & 0 & 34 \\ 0 & 0 & 32 & 48 & 0 & 0 & 0 & 11 \\ 0 & 0 & 17 & 45 & 0 & 0 & 0 & 33 \\ 0 & 0 & 0 & 0 & 28 & 52 & 53 & 20 \\ 0 & 0 & 0 & 0 & 10 & 39 & 24 & 57 \\ 0 & 0 & 0 & 0 & 55 & 36 & 28 & 15 \\ 0 & 0 & 0 & 0 & 38 & 41 & 33 & 34 \end{pmatrix}$$

for each user in the company C_2. We compute

$$\begin{aligned} &\left(b_{11}^{(2)}, b_{12}^{(2)}, b_{13}^{(2)}, b_{21}^{(2)}, b_{22}^{(2)}, b_{23}^{(2)}, b_{31}^{(2)}, b_{32}^{(2)}, b_{33}^{(2)}, b_{34}^{(2)} \right)^T \\ &= A_2 \cdot \left(a_{11}^{(2)}, a_{12}^{(2)}, a_{21}^{(2)}, a_{22}^{(2)}, a_{31}^{(2)}, a_{32}^{(2)}, a_{33}^{(2)}, \alpha_{21} \right)^T \\ &= (51, 2, 35, 1, 16, 18, 35, 33, 21, 40)^T. \end{aligned}$$

The shares of the users of the company C_2 are

$$\begin{pmatrix} b_{11}^{(2)}P \\ b_{12}^{(2)}P \\ b_{13}^{(2)}P \\ Vb_{21}^{(2)}P \\ b_{22}^{(2)}P \\ b_{23}^{(2)}P \\ b_{31}^{(2)}P \\ b_{32}^{(2)}P \\ b_{33}^{(2)}P \\ b_{34}^{(2)}P \end{pmatrix} = \begin{pmatrix} (25\gamma^2+34\gamma+14, 7\gamma^2+25\gamma+27) \\ (11\gamma^2+35\gamma+28, 28\gamma+15) \\ (11\gamma^2+30\gamma+5, 32\gamma^2+10\gamma+45) \\ (15\gamma+33, 9\gamma^2+22\gamma+23) \\ (26\gamma^2+27\gamma+3, 31\gamma^2+36\gamma+26) \\ (17\gamma^2+6, 41\gamma^2+2\gamma+1) \\ (11\gamma^2+30\gamma+5, 32\gamma^2+10\gamma+45) \\ (45\gamma^2+27\gamma+19, 2\gamma^2+41\gamma) \\ (22\gamma^2+43, 43\gamma^2+19\gamma+15) \\ (22\gamma^2+43, 4\gamma^2+28\gamma+32) \end{pmatrix}.$$

For conjunctive compartmented scheme, compute

$$\begin{aligned} s_1 &= \mathrm{e}\Big(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\Big) + K_1 \\ &= \mathrm{e}\,(P, 22P) + K_1 = 6\gamma^2 + 42\gamma + 28 \end{aligned}$$

and

$$\begin{aligned} s_2 &= \mathrm{e}\Big(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\Big) + K_2 \\ &= \mathrm{e}\,(P, 23P) + K_2 = 25\gamma^2 + 12\gamma + 17 \end{aligned}$$

where e is the modified Tate pairing (see [13]). The Dealer makes

$$P, M_{11}, M_{12}, M_{13}, M_{21}, M_{22}, M_{23}, s_1 \quad \text{and} \quad s_2 \ \text{ public.}$$

For disjunctive compartmented scheme, compute

$$\begin{aligned} s_1 &= \mathrm{e}\Big(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\Big) + K \\ &= \mathrm{e}\,(P, 22P) + K = 33\gamma^2 + 39\gamma + 22 \end{aligned}$$

and

$$\begin{aligned} s_2 &= \mathrm{e}\Big(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\Big) + K \\ &= \mathrm{e}\,(P, 23P) + K = 3\gamma^2 + 9\gamma + 14. \end{aligned}$$

The Dealer makes P, A_1, A_2, s_1 and s_2 public.

Reconstruction of the secret key

For Case I: Suppose that the users

$u_{12}^{(1)}, u_{13}^{(1)}$ in compartment C_{11};

$u_{22}^{(1)}, u_{23}^{(1)}$ in compartment C_{12};

$u_{31}^{(1)}, u_{32}^{(1)}, u_{34}^{(1)}$ in compartment C_{13} of company C_1 and

$u_{11}^{(2)}, u_{12}^{(2)}$ in compartment C_{21};

$u_{22}^{(2)}, u_{23}^{(2)}$ in compartment C_{22};

$u_{31}^{(2)}, u_{32}^{(2)}, u_{34}^{(2)}$ in compartment C_{23}

of company C_2 collaborate to reconstruct the secret.

The users $u_{22}^{(1)}, u_{23}^{(1)}$ form a submatrix

$$M'_{11} = \begin{pmatrix} 11 & 60 \\ 12 & 22 \end{pmatrix} \text{ of } M_{11}$$

and compute the inverse

$$M'^{-1}_{11} = \begin{pmatrix} 51 & 55 \\ 11 & 56 \end{pmatrix}.$$

Then they compute

$$\begin{aligned} \left(a_{11}^{(1)}P, a_{12}^{(1)}P\right)^T &= M'^{-1}_{11} \cdot \left(b_{12}^{(1)}P, b_{13}^{(1)}P\right)^T \\ &= \big((14\gamma^2 + 13\gamma + 15, 18\gamma^2 + 5\gamma + 29), \\ &\qquad (16\gamma^2 + 40\gamma + 37, 17\gamma^2 + 42\gamma + 11)\big)^T. \end{aligned}$$

Similarly, the users

$u_{22}^{(1)}, u_{23}^{(1)}$ can compute the values of $a_{21}^{(1)}P, a_{22}^{(1)}P$.

$u_{31}^{(1)}, u_{32}^{(1)}, u_{34}^{(1)}$ can compute the values of $a_{31}^{(1)}P, a_{32}^{(1)}P, a_{33}^{(1)}P$.

$u_{11}^{(2)}, u_{12}^{(2)}$ can compute the values of $a_{11}^{(2)}P, a_{12}^{(2)}P$.

$u_{22}^{(2)}, u_{23}^{(2)}$ can compute the values of $a_{21}^{(2)}P, a_{22}^{(2)}P$.

$u_{31}^{(2)}, u_{32}^{(2)}, u_{34}^{(2)}$ can compute the values of $a_{31}^{(2)}P, a_{32}^{(2)}P, a_{33}^{(2)}P$.

For conjunctive compartmented scheme, the users compute the company secrets

$$K_1 = s_1 - \mathrm{e}\Big(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\Big) = 25\gamma^2 + 44\gamma + 44$$

and

$$K_2 = s_2 - \mathrm{e}\Big(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\Big) = 27\gamma^2 + 44\gamma + 41.$$

Then they compute the global secret key

$$K = K_1 + K_2 = 5\gamma^2 + 41\gamma + 38.$$

For disjunctive compartmented scheme, the collaborating users in C_1 can compute the global secret

$$K = s_1 - \mathrm{e}\Big(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\Big) = 5\gamma^2 + 41\gamma + 38.$$

Similarly, the collaborating users in C_2 can compute the global secret

$$K = s_2 - \mathrm{e}\Big(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\Big) = 5\gamma^2 + 41\gamma + 38.$$

For Case II: Suppose that the users

$u_{12}^{(1)}, u_{13}^{(1)}$ in compartment C_{11};

$u_{22}^{(1)}, u_{23}^{(1)}, u_{24}^{(1)}$ in compartment C_{12};

$u_{31}^{(1)}, u_{32}^{(1)}, u_{34}^{(1)}, u_{35}^{(1)}$ in compartment C_{13} of company C_1

and

$u_{11}^{(2)}, u_{12}^{(2)}, u_{13}^{(2)}$ in compartment C_{21};

$u_{22}^{(2)}, u_{23}^{(2)}$ in compartment C_{22};

$u_{31}^{(2)}, u_{32}^{(2)}, u_{34}^{(2)}$ in compartment C_{23} of company C_2

collaborate to reconstruct the secret.

The users in the company C_1 can form a submatrix A_1' of A_1 and compute the inverse $A_1'^{-1}$, where

$$A_1' = \begin{pmatrix} 11 & 60 & 0 & 0 & 0 & 0 & 0 & 50 & 1 \\ 12 & 22 & 0 & 0 & 0 & 0 & 0 & 20 & 57 \\ 0 & 0 & 15 & 42 & 0 & 0 & 0 & 20 & 56 \\ 0 & 0 & 9 & 20 & 0 & 0 & 0 & 58 & 34 \\ 0 & 0 & 20 & 34 & 0 & 0 & 0 & 9 & 58 \\ 0 & 0 & 0 & 0 & 21 & 14 & 50 & 13 & 29 \\ 0 & 0 & 0 & 0 & 37 & 27 & 23 & 58 & 11 \\ 0 & 0 & 0 & 0 & 31 & 46 & 23 & 42 & 21 \\ 0 & 0 & 0 & 0 & 40 & 14 & 11 & 13 & 32 \end{pmatrix},$$

and

$$A_1'^{-1} = \begin{pmatrix} 51 & 55 & 33 & 36 & 17 & 33 & 18 & 46 & 60 \\ 11 & 56 & 23 & 14 & 10 & 21 & 17 & 57 & 16 \\ 0 & 0 & 39 & 60 & 17 & 6 & 31 & 25 & 22 \\ 0 & 0 & 10 & 30 & 40 & 21 & 17 & 57 & 16 \\ 0 & 0 & 56 & 50 & 27 & 9 & 20 & 46 & 54 \\ 0 & 0 & 53 & 19 & 31 & 37 & 57 & 44 & 31 \\ 0 & 0 & 32 & 46 & 59 & 21 & 5 & 48 & 60 \\ 0 & 0 & 18 & 3 & 37 & 47 & 9 & 23 & 30 \\ 0 & 0 & 41 & 17 & 47 & 53 & 40 & 48 & 52 \end{pmatrix}.$$

Then the users compute

$$\left(a_{11}^{(1)}P, a_{12}^{(1)}P, a_{21}^{(1)}P, a_{22}^{(1)}P, a_{31}^{(1)}P, a_{32}^{(1)}P, a_{33}^{(1)}P, \alpha_{11}P, \alpha_{12}P\right)^T = A_1'^{-1} \cdot \left(b_{12}^{(1)}P, b_{13}^{(1)}P, b_{22}^{(1)}P, b_{23}^{(1)}P, b_{24}^{(1)}P, b_{31}^{(1)}P, b_{32}^{(1)}P, b_{34}^{(1)}P, b_{35}^{(1)}P\right)^T.$$

Similarly, the users in the company C_2 can form a submatrix A_2' of A_2 and compute the inverse $A_2'^{-1}$, where

$$A_2'^{-1} = \begin{pmatrix} 13 & 47 & 0 & 0 & 0 & 0 & 0 & 1 \\ 25 & 15 & 0 & 0 & 0 & 0 & 0 & 9 \\ 16 & 12 & 0 & 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 32 & 48 & 0 & 0 & 0 & 11 \\ 0 & 0 & 17 & 45 & 0 & 0 & 0 & 33 \\ 0 & 0 & 0 & 0 & 28 & 52 & 53 & 20 \\ 0 & 0 & 0 & 0 & 10 & 39 & 24 & 57 \\ 0 & 0 & 0 & 0 & 38 & 41 & 33 & 34 \end{pmatrix}$$

and

$$A_2'^{-1} = \begin{pmatrix} 41 & 13 & 57 & 0 & 0 & 0 & 0 & 0 \\ 60 & 2 & 32 & 0 & 0 & 0 & 0 & 0 \\ 46 & 34 & 1 & 25 & 14 & 0 & 0 & 0 \\ 36 & 16 & 22 & 38 & 11 & 0 & 0 & 0 \\ 44 & 6 & 54 & 0 & 0 & 51 & 28 & 53 \\ 48 & 1 & 9 & 0 & 0 & 43 & 40 & 22 \\ 16 & 41 & 3 & 0 & 0 & 8 & 53 & 54 \\ 3 & 42 & 12 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then the users compute

$$\left(a_{11}^{(2)}P, a_{12}^{(2)}P, a_{21}^{(2)}P, a_{22}^{(2)}P, a_{31}^{(2)}P, a_{32}^{(2)}P, a_{33}^{(2)}P, \alpha_{21}P\right)^T = A_2'^{-1} \cdot \left(b_{11}^{(2)}P, b_{12}^{(2)}P, b_{13}^{(2)}P, b_{22}^{(2)}P, b_{23}^{(2)}P, b_{31}^{(2)}P, b_{32}^{(2)}P, b_{34}^{(2)}P\right)^T.$$

For conjunctive compartmented scheme, the users compute the company secrets

$$K_1 = s_1 - \mathrm{e}\Big(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\Big) = 25\gamma^2 + 44\gamma + 44$$

and

$$K_2 = s_2 - \mathrm{e}\Big(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\Big) = 27\gamma^2 + 44\gamma + 41.$$

Then they compute the global secret $K = K_1 + K_2 = 5\gamma^2 + 41\gamma + 38$. For disjunctive compartmented scheme, the collaborating users in C_1 can compute the global secret

$$K = s_1 - \mathrm{e}\Big(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\Big) = 5\gamma^2 + 41\gamma + 38.$$

Similarly, the collaborating users in C_2 can compute the global secret

$$K = s_2 - \mathrm{e}\Big(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\Big) = 5\gamma^2 + 41\gamma + 38.$$

The computational complexity of the proposed conjunctive compartmented and disjunctive compartmented schemes are almost same and will be examined in detail in the next section.

5. Computational complexity of the proposed schemes

The number of operations for computing a matrix multiplication of order $n \times t$ and $t \times 1$ is nt. The time for computing scalar multiplication of a point on an elliptic curve is $O(\log_2 \ell)$ using the basic *Double-and-add algorithm* [4], where ℓ is the order of the point. Computing a pairing takes $O(\log_2 \ell)$ operations (see [11,14]). Adding two distinct points takes $\mathbf{I}$+2$\mathbf{M}$+$\mathbf{S}$ operations and doubling takes $\mathbf{I}$+2$\mathbf{M}$+2$\mathbf{S}$ operations (see [1]) where $\mathbf{I}$, $\mathbf{M}$, $\mathbf{S}$ denote inverse, multiplication and squaring respectively. To compute an inverse of a matrix of order t using the basic inversion method cost $O(t^3)$.

At the time of distribution of shares.

For Case I: The Dealer requires $\sum_{i=1}^{m} \tau_i$ matrix multiplications of order

$$n_{ij} \times t_{ij} \quad \text{and} \quad t_{ij} \times 1$$

which costs

$$\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij}t_{ij} \quad \text{operations.}$$

As

$$n_{ij} \geq t_{ij} \quad \text{and} \quad \sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij} = n,$$

the sum

$$\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij}t_{ij} \leq n^2.$$

For Case II: The Dealer requires m matrix multiplications of order

$$\left(\sum_{j=1}^{\tau_i} n_{ij}\right) \times t_i \quad \text{and} \quad t_i \times 1$$

which costs

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{\tau_i} n_{ij}\right) t_i \quad \text{operations.}$$

As

$$\sum_{j=1}^{\tau_i} n_{ij} \geq t_i \quad \text{and} \quad \sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij} = n,$$

the sum

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{\tau_i} n_{ij}\right) t_i \leq n^2.$$

In addition, the Dealer requires n scalar multiplications of points to encrypt the shares $b_{jk}^{(i)}x_{jk}^{(i)}P$ that costs $O(n\log_2\ell)$. To compute s_i, we need $\sum_{i=1}^{m}\tau_i$ point additions and m pairings which costs $O\left(m\log_2\ell\right)$.

At the time of reconstruction of the secret.

For conjunctive compartmented secret sharing scheme:

For Case I: the collaborating users need to find the inverse of $\sum_{i=1}^{m}\tau_i$ matrices of order t_{ij} that costs

$$\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} t_{ij}^3 \leq n^3 \quad \text{operations.}$$

To find the unknowns $a_{jk}^{(i)}P$, they require

$$\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} t_{ij}^2 \leq n^2 \quad \text{point additions.}$$

For Case II: they need to find the inverse of m matrices of order t_i that costs

$$\sum_{i=1}^{m} t_i^3 < n^3.$$

To find the unknowns $a_{jk}^{(i)}P$, the number of point additions required is

$$\sum_{i=1}^{m} t_i^2 \leq n^2.$$

In addition, to find K_i, we need $\sum_{i=1}^{m} \tau_i$ point additions and m pairing computations.

For disjunctive compartmented secret sharing scheme.

Suppose that the users in the company C_i want to reconstruct the secret.

For Case I: the collaborating users need to find the inverse of τ_i matrices of order t_{ij} that costs

$$\sum_{j=1}^{\tau_i} t_{ij}^3 < n^3 \quad \text{operations.}$$

To find the unknowns $a_{jk}^{(i)}P$, they require

$$\sum_{j=1}^{\tau_i} t_{ij}^2 < n^2 \quad \text{point additions.}$$

For Case II: they need to find the inverse of a matrix of order t_i that costs

$$[t_i^3 < n^3.$$

To find the unknowns $a_{jk}^{(i)}P$, the number of required point additions is

$$t_i^2 < n^2.$$

In addition, to find K, we need τ_i point additions and one pairing computation.

Hence, combining all, both the schemes required $O(n^3)$ operations. We also see that the time complexity of the disjunctive compartmented scheme is lower than that of the conjunctive compartmented scheme.

6. Concluding remark

In this article, we have proposed two schemes, namely, conjunctive compartmented and disjunctive compartmented secret sharing schemes. The schemes are verifiable. That is, during the reconstruction of the secret, each collaborating user can verify the shares of the other collaborating users. We have analyzed the security aspects of the schemes. The computational complexity of both schemes has been described.

Acknowledgement. The authors are very thankful to the anonymous referee for going through the manuscript meticulously and for his/her valuable comments and suggestions to improve the presentation of the paper.

REFERENCES

[1] AJEENA, R. K. K.—HAILIZA, K.: *The computational complexity of elliptic curve integer sub-decomposition (ISD) method*. In: AIP Conference Proceedings. Vol. 1605 (2014), no. 1, pp 557–562.

[2] CHINTAMANI, M.—PAUL, P.—SA, L.: *Conjunctive Hierarchical Multi-Secret Sharing Scheme using Elliptic Curves*, Indian J. Pure Appl. Math. **55** (2023), no. 4, 1456–1464. https://doi.org/10.1007/s13226-023-00450-x

[3] CHEN, Q.—TANG, C.—LIN, Z.: *Compartmented secret sharing schemes and locally repairable codes*, IEEE Transactions on Communications, **68** 2020, no. 10, 5976–5987.

[4] CORON, J.: *Resistance against differential power analysis for elliptic curve cryptosystems*. In: Proceedings of the 1st International Workshop on Cryptographic Hardware and Embedded Systems (CHES '99), Lecture Notes in Comput. Sci. Vol. 1717 (1999), pp. 292–302.

[5] FELDMAN, P.: *A practical scheme for non-interactive verifiable secret sharing*. In: 28th Annual Symposium on Foundations of Computer Science (sfcs 1987) IEEE Vol. (1987), pp. 427–438, https://ieeexplore.ieee.org/document/4568297

[6] FARRÀS, O.— PADRÓ, C.—XING, C.—YANG, A.: *Natural generalizations of threshold secret sharing*, IEEE Transactions on Information Theory, **60** (2014), no. 3, 1652–1664.

[7] FARRÀS, O.— MARTÍ-FARRÉ, J — PADRÓ, C.: *Ideal Multipartite Secret Sharing Schemes*, J. Cryptology, **25** (2012), 434–463, https://doi.org/10.1007/s00145-011-9101-6

[8] FREY, G.—MüLLER, M.—RüCK, H.-G.: *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Transactions on Information Theory, **45** (1999) no. 5, 1717–1718.

[9] GHODOSI, H.—PIEPRZYK, J.—SAFAVI-NAINI, R.: *Secret sharing in multilevel and compartmented groups*. In: Proc. ACISP 1998, Lectute Notes in Comput. Sci. Vol. 1438, (1998) pp. 367–378.

[10] IFTENE, S.: *General secret sharing based on the Chinese remainder theorem with applications in E-voting*, Electronic Notes in Theoretical Computer Science **186** (2007), 67–84, https://doi.org/10.1016/j.entcs.2007.01.065

[11] IONICA, S.—JOUX, A.: *Pairing computation on elliptic curves with efficiently computable endomorphism and small embedding degree*. In: (M. Joye, A. Miyaji, A. Otsuka, eds.) Pairing-Based Cryptography — Pairing 2010. Lecture Notes in Comput. Sci. Vol. 6487, (2010), https://doi.org/10.1007/978-3-642-17455-1_27.

[12] JOUX, A.: *A one round protocol for tripartite Diffie-Hellman*. In: Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, Vol. 1838 (2000), 385–393. Full version: J. Cryptology, **17** (2004), 263–276.

[13] MENEZES, A.: *An introduction to pairing-based cryptography*. Recent trends in Cryptography, Contemp. Math. **477** (2009), 47–65.

[14] MILLER, V.: *The Weil pairing, and its efficient calculation*. J. Cryptology **17**, (2004), 235–261. https://doi.org/10.1007/s00145-004-0315-8.

[15] ROMAN, S.: *Coding and Information Theory*. Springer-Verlag, Berlin, Heidelberg, 1992.

[16] SELÇUK, A. A.—YILMAZ, R.: *Joint compartmented threshold access structures*. IACR Cryptology ePrint Archive, 2013/054, 2013, 6 p. https://www.cs.bilkent.edu.tr/~selcuk/publications/JCAS_ICACM12.pdf

[17] SHAMIR, A.: *How to share a secret*, Comm. ACM **22** (1979), no. 11, 612–613. https://doi.org/10.1145/359168.359176

[18] SILVERMAN, J.: *The Arithmetic of Elliptic Curves*. Springer-Verlag, Berlin, 1986.

[19] SIMMONS, G.: *How to (really) share a secret*. In: Advances in Cryptology — Proceedings of CRYPTO '88 (S. Goldwasser, ed.), Lecture Notes in Computer Science Vol. 403 (1990), pp. 390–448.

[20] TASSA, T.—DYN, N.: *Multipartite secret sharing by bivariate interpolation*, J. Cryptology, **22** (2009), no. 2, 227–258.

[21] TENTU, A. N.—PAUL, P.—VENKAIAH, V. CH.: *Computationally perfect compartmented secret sharing schemes based on MDS codes*, Int. J. Trust Management in Computing and Communications, **2** (2014), no. 4, 353–378.

[22] XU, G.—YUAN, J.—XU, G.—DANG, Z.: *An efficient compartmented secret sharing scheme based on linear homogeneous recurrence relations*, Security and Communication Networks Vol. 2021 (2021), no 1, Art. 5566179, https://doi.org/10.1155/2021/5566179.

[23] YU, Y.—WANG, M.: *A probabilistic secret sharing scheme for a compartmented access structure*. In: Information and Communications Security. ICICS, 2011 (S. Qing, W. Susilo, G. Wang, D. Liu, eds.) Lecture Notes in Computer Science, Vol. 7043 (2011), pp. 136–142. https://doi.org/10.1007/978-3-642-25243-3_11

[24] YUAN, L.—LI, M.—GUO, C.—CHOO K-KR.—REN, Y.: *Novel Threshold Changeable Secret Sharing Schemes Based on Polynomial Interpolation*. PLoS ONE, 2016. https://doi.org/10.1371/journal.pone.0165512

Received August 11, 2022
Revised October 4, 2025
Accepted October 6, 2025
Publ. online December 20, 2025

Mohan Chintamani
School of Mathematics and Statistics
University of Hyderabad
Hyderabad–500046
INDIA
E-mail: mohansspecial@gmail.com

Prabal Paul
Department of Mathematics
BITS Pilani, K K Birla Goa Campus
Goa-403726
INDIA
E-mail: prabal.paul@gmail.com

Laba Sa
Department of Mathematics
MATS University
Raipur-493441
INDIA
E-mail: labasspecial@gmail.com