Indian J Pure Appl Math (2024) 55:1456–1464
https://doi.org/10.1007/s13226-023-00450-x

ORIGINAL RESEARCH

Conjunctive Hierarchical Multi-Secret Sharing Scheme using Elliptic Curves

Mohan Chintamani · Prabal Paul · Laba Sa

Received: 26 December 2022 / Accepted: 14 June 2023 / Published online: 21 July 2023

Abstract A method in which a secret is distributed among the users and a predefined number of users collaborate to reconstruct the secret is known as a secret sharing scheme. In this article, we have proposed a conjunctive hierarchical multi-secret sharing scheme using elliptic curves and bilinear pairings. The motivation for utilizing bilinear pairing of elliptic curves is to provide a similar level of security as in many existing schemes while employing a smaller key size. The proposed scheme is efficient and verifiable. The computational cost of the scheme is determined. We have also given an explicit example of the proposed scheme.

Keywords Elliptic curves · Bilinear pairings · Secret sharing · Hierarchical access structures

Mathematics Subject Classification 11T71 · 94A60

1 Introduction

Secret sharing is a method of distributing a secret among the users and a predefined number (threshold number) of users work together to reconstruct the secret. A set of users who are allowed to reconstruct the secret is called an *authorized* set. The collection of all authorized subsets of users is referred to as an access structure. Secret sharing with many levels of hierarchy is known as hierarchical secret sharing. In a hierarchical secret sharing scheme (see Definition 1), a group of users is separated into several levels so that a user can be present at one of the levels. A secret is distributed among all the users at every level and an authorized set of users can only reconstruct the secret. Several schemes have been proposed for hierarchical and conjunctive hierarchical secret sharing schemes (see [3,6,10,17,19,21], for example).
Multi-secret sharing scheme is a method of sharing several secrets among the users in such a way that any authorized subset of users can recover all the secrets. However, any unauthorized subset of users gets no information about any of the secrets. Many multi-secret sharing schemes have been proposed (see [2,4,13]).

Communicated by Sanoli Gun.

Mohan Chintamani, Prabal Paul and Laba Sa have contributed equally to this work.

M. Chintamani (✉) · L. Sa
School of Mathematics and Statistics, University of Hyderabad, Hyderabad 500046, India
E-mail: mohansspecial@gmail.com

L. Sa
E-mail: labasspecial@gmail.com

P. Paul
BITS Pilani, K K Birla Goa Campus, Zuarinagar, Goa 403726, India
E-mail: prabal.paul@gmail.com

There are two types of hierarchical schemes, namely conjunctive and disjunctive (see Definition 1). In this paper, we have proposed a conjunctive hierarchical secret sharing scheme using elliptic curves [18] and bilinear pairings [14]. The primary rationale for using bilinear pairing with elliptic curves is to give similar security (to many existing schemes) while using a smaller key size. One important feature of our scheme is that the Dealer does not require any secure channel to distribute the secrets. The Dealer encrypts the secrets and distributes them to the users publicly.

The two types of hierarchical schemes are useful in many scenarios. For example, the project manager(s) and their team members may have access to the data/workplace according to different levels of authority. In a hospital, a doctor (or team of doctors) may have access to the medical record of every patient, however nurses of the hospital may have access to a limited number of patients' records.

Our proposed scheme is significant because it overcomes all of the limitations inherent in the majority of existing schemes. The proposed scheme can accommodate any number of users. Also, there are no limitations on the number of secrets to be shared. Moreover, our scheme is efficient and verifiable. The verifiability means the collaborating users (at the time of reconstruction) can use public information to check whether the information shared by the individual user is valid or not. For example, the schemes proposed in [2] and [22] are verifiable.

We have organized our article as follows. In Section 2, we define *elliptic curves* and *bilinear pairings*. The proposed hierarchical secret sharing scheme is described in Section 3. The security analysis and illustration by an example of the proposed scheme are given in Section 4 and Section 5, respectively. We discuss the complexity of the scheme in Section 6.

2 Preliminaries

There are two types of hierarchical access structures, namely, conjunctive and disjunctive. We have proposed a multi-secret sharing scheme using a conjunctive hierarchical access structure in the next section. The conjunctive and disjunctive hierarchical access structures (see [19,21], for example) are defined as follows.

Definition 1 (Conjunctive and disjunctive hierarchical access structure) Let U be a group of n users that is partitioned into m disjoint levels $L_1, L_2, \cdots, L_m$. Define L_i as higher level than L_j if $i < j$. Let t_i be the threshold for level L_i or higher and $t_1 \leq t_2 \leq \cdots \leq t_m$. Then, the *conjunctive hierarchical access structure* is defined as

$$\Gamma = \left\{ A \subseteq U : \left| A \cap \left(\bigcup_{j=1}^{i} L_j \right) \right| \geq t_i \text{ for all } i,\ 1 \leq i \leq m \right\}.$$

That is, a set of users can reconstruct the secret if it comprises at least t_i users from each level L_i or higher. When we replace 'for all' with 'for some', then we call it a *disjunctive hierarchical access structure*.

As our scheme involves elliptic curves and bilinear pairings, we recall its definition. 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 the discriminant not equal to zero, where q is a prime power. The group $E(\mathbb{F}_q)$ is the collection of points on the elliptic curve, and the point at infinity $\mathcal{O}$ is the identity element of the group. If the characteristic of the field $\mathbb{F}_q$ is not equal to 2 and 3, then the curve E can be rewritten as $E':\ y^2 = x^3 + ax + b$. The discriminant of E' is $\Delta = -16(4a^3 + 27b^2) \neq 0$. For more details, we refer to [14,18].

Definition 2 (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 satisfy the bilinearity, non-degeneracy and computability properties. That is, for any $x_1, x_2, y_1, y_2 \in G_a$ and the identities $0 \in G_a$, $1 \in G_m$:

- (Bilinearity) $e(x_1 + x_2, y_1) = e(x_1, y_1)e(x_2, y_1)$ and $e(x_1, y_1 + y_2) = e(x_1, y_1)e(x_1, y_2)$.
- (Non-degeneracy) there exists a $x_1 \neq 0$ such that $e(x_1, x_1) \neq 1$.
- (Computability) there exists an efficient algorithm for computing e. See [14,15], for example.

Remark 1 The map e is symmetric and also satisfies the following properties.

1. For any $x, y \in G_a$, $e(x, 0) = e(0, y) = 1$ and $e(ax, by) = e(x, y)^{ab}$ for all $a, b \in \mathbb{Z}$.
2. If $e(x, y) = 1$ for all $x \in G_a$, then $y = 0$.
3. For any $x \neq 0$, $y, y' \in G_a$, we have $e(x, y) = e(x, y')$ if and only if $y = y'$.

Many pairings are defined using elliptic curves. For instance, we recall a pairing as given in [14]. Let the number of points in $E(\mathbb{F}_q)$ be a multiple of ℓ, where ℓ is a prime and gcd(ℓ, q)=1. The embedding degree of $E(\mathbb{F}_q)$ with respect to ℓ is denoted as k (that is, the smallest k such that $\ell \mid q^k - 1$). The collection of ℓ-torsion points in $E(\mathbb{F}_{q^k})$ is denoted by $E[\ell]$. Let μ_ℓ be the order-ℓ subgroup of $\mathbb{F}^*_{q^k}$. The *(modified) Tate-pairing* e is a map $e : E[\ell] \times E[\ell] \longrightarrow \mu_\ell$ defined as follows. For $P, Q \in E[\ell]$, let f_P be a function such that $\text{div}(f_P) = \ell(P) - \ell(\mathcal{O})$. Then,

$$e(P, Q) = \left(\frac{f_P(Q + R)}{f_P(R)}\right)^{\frac{q^k-1}{\ell}},$$

where $R \notin \{\mathcal{O}, P, -Q, P - Q\}$.
For further information, see [7,14]. In our scheme, one can use (modified) Tate-pairing, Weil pairing [15], and other similar kinds of pairings.

3 Proposed Conjunctive Hierarchical Multi-Secret Sharing Scheme

3.1 Setting up and distribution of the parameters of the scheme

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. Let $P \in E(\mathbb{F}_q)$ be a point of order ℓ, where ℓ is a prime integer and $G_a = \langle P \rangle$, $G_m = \mu_\ell$. We assume that ℓ is large enough so that the *elliptic curve discrete logarithm problem* (ECDLP) [8] is hard to solve. Consider a bilinear pairing e as in the above definition. Suppose there is a set U of n users and a trusted Dealer D. The Dealer has the authority to generate and publish all the parameters of the scheme. The users are divided into m disjoint levels $L_1, L_2, \cdots, L_m$. Define L_i is a higher level than L_j if $i < j$. Let $\mid L_i \mid = n_i$ and t_i be the threshold for level L_i or higher for $i = 1, 2, \cdots, m$. The top level is L_1 and L_m is the lowest level. Assume that $t_1 \leq t_2 \leq \cdots \leq t_m$. Suppose that s secrets say $K_1, K_2, \cdots, K_s$ are to be shared among the users. Dealer makes P public.
We recall that a generating matrix M of size $k \times n$ of a *maximum distance separable* code (MDS code) $\mathcal{C}$ with parameters $[n, k, d]$ over $\mathbb{F}_q$ satisfies the property that any k columns of M are linearly independent (see [11, Theorem 2.4.3]). Such matrices are known as MDS matrices. We refer to [11] for more details.
We need the following two propositions to describe the scheme.

Proposition 1 *Let m_1, m_2 and t be positive integers. Suppose $b_1, b_2, \cdots, b_{m_1} \in \mathbb{F}_\ell$ be given. If $t > m_1$, then there exists an $m_1 \times t$ matrix A and an $m_2 \times t$ matrix B such that any t rows of the matrix $M = \begin{pmatrix} A \\ B \end{pmatrix}$ forms an invertible submatrix of M, and the system $AX = (b_1\ b_2\ \cdots\ b_{m_1})^T$ has many solutions $X \in \mathbb{F}_\ell^t$.*

Proof We choose an $(m_1 + m_2) \times t$ matrix M such that any t rows of M forms an invertible submatrix M. We let $M = \begin{pmatrix} A \\ B \end{pmatrix}$, where A is a $m_1 \times t$ and B is a $m_2 \times t$ submatrices. Since $t > m_1$, the rank of A is m_1. It follows that the system $AX = (b_1\ b_2\ \cdots\ b_{m_1})^T$ has many solutions, as required. □

Proposition 2 *Let m_1, m_2 and t be positive integers with $t \leq m_1$. Suppose $b_1, b_2, \cdots, b_{m_1} \in \mathbb{F}_\ell$ be given. For any integer t' satisfying $m_1 < t' \leq m_1 + m_2$, there exists a matrix $M = \begin{pmatrix} A & A' \\ B & B' \end{pmatrix}$, where A and B are matrices of size $m_1 \times t$ and $m_2 \times t$, A' and B' are matrices of size $m_1 \times (t' - t)$ and $m_2 \times (t' - t)$, such that the first t columns of any t rows of M form an invertible submatrix and the system $\begin{pmatrix} A & A' \end{pmatrix} X = (b_1\ b_2\ \cdots\ b_{m_1})^T$ has many solutions.*

Proof As before, we choose matrices A and B of size $m_1 \times t$ and $m_2 \times t$ respectively, such that any t rows of the matrix $\begin{pmatrix} A \\ B \end{pmatrix}$ form an invertible submatrix. Since $t \leq m_1$, the dimension of the column space of A is t. Let $v_1, v_2, \cdots, v_t \in \mathbb{F}_\ell^{m_1}$ be the column vectors of A. Let W be a subspace of $\mathbb{F}_\ell^{m_1}$ such that $\text{Span}\{v_1, v_2, \cdots, v_t\} + W = \mathbb{F}_\ell^{m_1}$ and the dimension of W is $m_1 - t$. By the hypothesis on t', we have $t' - t \geq m_1 - t$. Thus, we can select $t' - t$ column vectors $w_1, w_2, \cdots, w_{t'-t} \in \mathbb{F}_\ell^{m_1}$ which spans W.

Now, we let A' be the matrix formed by column vectors $w_1, w_2, \cdots, w_{t'-t}$ and B' to be any matrix of $m_2 \times (t'-t)$ size. As the columns of the matrices A and A' span all of $\mathbb{F}_\ell^{m_1}$, we have rank $\begin{pmatrix} A & A' \end{pmatrix}$ is m_1. Hence the system $\begin{pmatrix} A & A' \end{pmatrix} X = (b_1\ b_2\ \cdots\ b_{m_1})^T$ has many solutions. Letting $M = \begin{pmatrix} A & A' \\ B & B' \end{pmatrix}$, the proof is complete. □

Consider the conjunctive hierarchical access structure Γ as in Definition 1. Denote by u_{ij} the j^{th} user in the level L_i.

Level L_1.

- Consider a matrix M_1 of order $n_1 \times t_1$ such that any submatrix of M_1 consisting of any t_1 rows forms an invertible matrix. Such matrices are transpose of a standard MDS matrices.
- D chooses t_1 random integers $a_{11}, a_{12}, \cdots, a_{1t_1} \in [0, \ell - 1]$ and computes

$$(b_{11}\ b_{12}\ \cdots\ b_{1n_1})^T = M_1 \cdot (a_{11}\ a_{12}\ \cdots\ a_{1t_1})^T$$

  where T denotes the transpose of a matrix.
- Each u_{1j} in the level L_1, chooses $x_{1j} \in [1, \ell - 1]$ randomly and makes $x_{1j}P$ public.
- Then D computes $b_{1j}x_{1j}P$ for user u_{1j}, $j = 1, 2, \cdots, n_1$, and sends (publicly) to the respective user.
- Each u_{1j} will get their share $b_{1j}P$ by computing $x_{1j}^{-1}(b_{1j}x_{1j})P$.

In general for $i \geq 2$, we have the following.

Level L_i.

Case I. For $t_i > \sum_{k=1}^{i-1} n_k$, consider a matrix M_i of order $(n_1 + n_2 + \cdots + n_i) \times t_i$ such that any t_i rows form an invertible matrix. D chooses t_i values $a_{i1}, a_{i2}, \cdots, a_{it_i} \in [0, \ell - 1]$ and computes

$$(b_{11}\ \cdots\ b_{1n_1}\ b_{21}\ \cdots\ b_{2n_2}\ \cdots\ b_{i1}\ \cdots\ b_{in_i})^T = M_i \cdot (a_{i1}\ a_{i2}\ \cdots\ a_{it_i})^T,$$

in such a way that $b_{sj}, s = 1, 2, \cdots, i-1, j = 1, 2, \cdots, n_s$, are same as in the previous levels. This is possible in view of Proposition 1. Each u_{ij} in level L_i, chooses $x_{ij} \in [1, \ell - 1]$ randomly and makes $x_{ij}P$, $j = 1, 2, \cdots, n_i$, public. Then D computes $b_{ij}x_{ij}P$ for u_{ij} and sends (publicly) to the respective user. Then each u_{ij} will get their share $b_{ij}P$ by computing $x_{ij}^{-1}(b_{ij}x_{ij})P$.

Case II. For $t_i \leq \sum_{k=1}^{i-1} n_k$, consider a matrix M_i of order $(n_1 + n_2 + \cdots + n_i) \times t_i'$, where $\sum_{k=1}^{i-1} n_k < t_i' \leq \sum_{k=1}^{i} n_k$, such that the first t_i columns of any t_i rows form an invertible submatrix of M_i. D chooses t_i' values $a_{i1}, a_{i2}, \cdots, a_{it_i}, \cdots, a_{it_i'} \in [0, \ell - 1]$ and computes

$$(b_{11}\ \cdots\ b_{1n_1}\ \cdots\ b_{i1}\ \cdots\ b_{in_i})^T = M_i \cdot (a_{i1}\ a_{i2}\ \cdots\ a_{it_i}\ \cdots\ a_{it_i'})^T,$$

in such a way that b_{sj} for $s = 1, 2, \cdots, i-1$ and $j = 1, 2, \cdots, n_s$, are same as in the previous levels. This is possible in view of Proposition 2. As before, D keeps the first t_i values as secret and declares the rest $t_i' - t_i$ values as public. Each u_{ij} in the level L_i chooses $x_{ij} \in [1, \ell - 1]$ randomly and makes $x_{ij}P$ public. Then D computes $b_{ij}x_{ij}P$ for u_{ij} and sends (publicly) to the respective user. Then each u_{ij} will get their share $b_{ij}P$ by computing $x_{ij}^{-1}(b_{ij}x_{ij})P$.

Now D chooses secret keys $K_i \in [0, p - 1]$, $1 \leq i \leq s$, and computes $v_i = e(P, i \cdot Q) + K_i$ where $Q = \sum_{j=1}^{m} a_{j1}P$. Finally, D makes v_i, $1 \leq i \leq s$, and M_j, $1 \leq j \leq m$, public.

Remark 2 We note that (see [14]), for any $P_1, P_2 \in E[\ell]$, $e(P_1, P_2) \in \mu_\ell \subseteq \mathbb{F}_{q^k}^* \subseteq \mathbb{F}_{q^k}$. Also, for $K \in [0, p-1]$ we have $K \in \mathbb{F}_{q^k}$. Thus $e(P_1, P_2) + K$ is in $\mathbb{F}_{q^k}$. Therefore, the pairiing e of the elliptic curve is compatible in this case.

3.2 Reconstruction of the secrets

Without loss of generality, suppose that t_1 number of users $u_{11}, u_{12}, \cdots, u_{1t_1}$ from level L_1, $t_2 - t_1$ number of users $u_{21}, u_{22}, \cdots, u_{2(t_2-t_1)}$ from level L_2, $t_3 - t_2$ number of users $u_{31}, u_{32}, \cdots, u_{3(t_3-t_2)}$ from level $L_3, \ldots,$ and $t_m - t_{m-1}$ number of users $u_{m1}, \cdots, u_{m(t_m-t_{m-1})}$ from level L_m collaborate to reconstruct the secrets. The collaborating users from level L_1 will consider a submatrix M_1' of M_1 of order t_1 corresponding to their shares and find the inverse $M_1'^{-1}$. Then, the users compute $M_1'^{-1} \cdot \left(b_{11}P\ b_{12}P\ \cdots\ b_{1t_1}P\right)^T = \left(a_{11}P\ a_{12}P\ \cdots\ a_{1t_1}P\right)^T$. At level L_2, in Case I, the collaborating users from levels L_1 and L_2 can find $\left(a_{21}P, a_{22}P, \cdots, a_{2t_2}P\right)$ as above. In Case II, let $M_2 = \begin{pmatrix} A_2 & A_2' \\ B_2 & B_2' \end{pmatrix}$ (see Proposition 2). The collaborating users first compute

$$\begin{pmatrix} b_{11}'P \\ \vdots \\ b_{1t_1}'P \\ b_{21}'P \\ \vdots \\ b_{2(t_2-t_1)}'P \end{pmatrix} = \begin{pmatrix} b_{11}P \\ \vdots \\ b_{1t_1}P \\ b_{21}P \\ \vdots \\ b_{2(t_2-t_1)}P \end{pmatrix} - \begin{pmatrix} A_2'' \\ B_2'' \end{pmatrix} \begin{pmatrix} a_{2(t_2+1)}P \\ \vdots \\ a_{2t_2'}P \end{pmatrix},$$

where A_2'' and B_2'' are the submatrices of A_2' and B_2' respectively, corresponding to collaborating users. Then, they consider a submatrix M_2' consisting of the first t_2 columns of M_2 corresponding to their shares. Finally, they compute

$$M_2'^{-1} \cdot \left(b_{11}'P\ \cdots\ b_{1t_1}'P\ b_{21}'P\ \cdots\ b_{2(t_2-t_1)}'P\right)^T = \left(a_{21}P\ a_{22}P\ \cdots\ a_{2t_2}P\right)^T.$$

Similarly, the collaborating users from levels L_1, L_2 and L_3 can find $\left(a_{31}P, a_{32}P, \cdots, a_{3t_3}P\right)$ and so on. Then, the users compute $Q = \sum_{j=1}^{m} a_{j1}P$. Therefore, the secrets $K_i = v_i - e\,(P,\ i \cdot Q)$ for $1 \le i \le s$, are revealed.

3.3 Verification of the shares

Verification of shares is essential to avoid two types of problems: the Dealer may send incorrect shares to the users during distribution, and the user may provide incorrect shares during reconstruction. The first problem does not arise in our schemes since the shares are distributed in an encrypted way. The shares in the second problem can be verified in the following way.
During the secret reconstruction, each collaborating user u_{ij} provides their share $c_{ij}P$ with an extra information $x_{ij}^{-1}P$ for verification. Other collaborating users can verify the authenticity of the share by examining the validity of the equation $e(x_{ij}^{-1}P, b_{ij}x_{ij}P) = e(P, c_{ij}P)$. The above equation holds true if and only if $c_{ij}P = b_{ij}P$ as $e(x_{ij}^{-1}P, b_{ij}x_{ij}P) = e(P, b_{ij}P)$.

4 Security Analysis of the Proposed Scheme

Bilinear pairing e is a one-way function and can be calculated in two steps. The first is to use Miller's algorithm ([15, Lemma 2]) to determine the evaluation of a certain function at a specific divisor of the underlying elliptic curve E. The second step is the final exponentiation. We also refer to [9] for further information on how the pairing inversion problem and the individual steps (Miller inversion and inverting exponentiation) relate to one another. The one-wayness of the bilinear map is that, to find $P, Q \in G_a$ such that $e(P, Q) = g$ for a given pairing e and a value $g \in G_m$ is difficult. Also, to find $Q \in G_a$ for a given $P \in G_a,\ P \neq 0$ and $g \in G_m$ such that $e(P, Q) = g$ is difficult. The pairing e is non-degenerate and bilinear, and the groups G_a, G_m are cyclic with the same prime order. For $P \neq 0$, the equation $e(P, Q) = g = e(P, Q')$ implies that $e(P, Q - Q') = 1$. As P is a generator for G_a, it follows that $Q = Q'$. Hence, we have the following observation.

Table 1 Comparison with other schemes

Scheme	Binu [4]	Liu [13]	Tentu [21]	Proposed
Hierarchical	No	No	Yes	Yes
Multi-secret	Yes	Yes	No	Yes
Verifiability	Yes	No	No	Yes
Secure channel	Yes	Yes	No	No
Limitations on number of secrets	No	Yes	Yes	No
Underlying group	Elliptic curves	Elliptic curves	$\mathbb{F}_q$	Elliptic curves

Observation 3 *For a given pair $(P, g) \in G_a \times G_m$ with $P \neq 0$, there is a unique $Q \in G_a$ such that $e(P, Q) = g$.*

For given points P and aP, $a \in \mathbb{Z}$, on an elliptic curve E, finding the value of a is known as *Elliptic Curve Discrete Logarithm Problem (ECDLP)*. It is believed that ECDLP is computationally infeasible to solve for a suitable choice of elliptic curve E and points on E ([8]).
In our scheme, the Dealer does not require a secure channel to distribute the shares, which is a key aspect of our scheme. The Dealer encrypts the shares before sending them to the users. When the Dealer distributes the shares $b_{ij}P$ to the users, an adversary cannot obtain it from $b_{ij}x_{ij}P$ since it is equivalent to solving an instance of ECDLP. Also, an adversary cannot obtain the users secret key x_{ij} from $x_{ij}P$.

Observation 4 *The probability of getting secrets for an adversary is negligible.*

The probability of guessing level secrets $a_{i1}P$ for $1 \leq i \leq m$ (or $\sum_{i=1}^{m} a_{i1}P$) is $1/\ell$ and guessing the correct secret K_i is $1/p$. So the probability of getting secrets is $\max\{1/\ell, 1/p\}$. As ℓ and p are large primes, this probability is very small.
We need the following basic result (see [16, Theorem 5.3.6]) from linear algebra. For the sake of completeness, we include a brief sketch of the proof.

Proposition 5 *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 $1 \leq \lambda \leq t$. In the case of ℓ^{λ} solutions, each solution is of equal probability.*

Proof Consider a system $AX = \mathrm{b}$ with m equations and t unknowns. By elementary row operations, the above system is equivalent to the system $A'X = \mathrm{b}'$ where A' is the row reduced echelon form of the matrix A. We know that there exists a solution of the system if and only if the row rank of A' is equal to the row rank of the augmented matrix $[A' : \mathrm{b}']$. Suppose this is the case. Let $A' = (a_{ij})$. Since A' is in row reduced echelon form, there exist (column) indices $1 \leq n_1 < n_2 < \cdots < n_r \leq t$ such that

- for each $i = 1, 2, \cdots, r$, we have $a_{i1} = a_{i2} = \cdots = a_{in_i - 1} = 0$ and $a_{in_i} = 1$,
- for each $j = 1, 2, \cdots, r$, we have $a_{in_j} = 0$ for every $i \neq j$.

Let $\lambda = t - r$. Thus, λ is the number of free variables and hence the dimension of the solution space of the system ($AX = \mathrm{b}$) is λ. It follows that the number of solutions is ℓ^{λ} (in the case $t = r$, there is a unique solution). Moreover, as each free variable can assume any of the ℓ values (with probability $\frac{1}{\ell}$), the probability of each of the solution to the system is $\frac{1}{\ell^{\lambda}}$. □

Theorem 6 *The probability of receiving any of the secrets K_i by an unauthorized set of users is low.*

Proof Let A be an unauthorized set of users (i.e., $A \notin \Gamma$). Thus, $\left| A \cap \left(\bigcup_{j=1}^{i} L_j \right) \right| < t_i$, for some i, $1 \leq i \leq m$.
Let $t_i - 1$ (or less) number of users from Level L_i or higher collaborate to compute $a_{i1}P$. The users can form a system of less than t_i equations with t_i unknowns. Thus, by Proposition 5, the system has ℓ^{λ} many solutions for some λ, $1 \leq \lambda \leq t_i$. Suppose they choose a share $b_{uv}P \in G_a$ from level L_i or higher levels. Then they can form a square matrix and solve the system of equations with the share $b_{uv}P$. However, the probability of choosing the correct share $b_{uv}P$ is $1/\ell$. Also, the probability of choosing $b_{uv}P$ and $a_{i1}P$ is same. Hence, an unauthorized set of users cannot get any information about the secret. □

A comparison between the proposed scheme and some of the known schemes is shown in Table 1 (below).

5 An Example of the Scheme

We give an example of the conjunctive hierarchical scheme using modified Tate-pairing ([14]). Computations are based on SageMath.
Consider an elliptic curve $E: y^2 = x^3 + 4x + 15$ over the finite field $\mathbb{F}_{47}$. The number of points in $E(\mathbb{F}_{47})$ is 37 and $37 \mid 47^3 - 1$, i.e., the embedding degree of $E(\mathbb{F}_{47})$ with respect to 37 is 3. Then $\mathbb{F}_{47^3}$ is an extended finite field and the number of points in $E(\mathbb{F}_{47^3})$ is 104044. Let α be a root of any irreducible cubic polynomial (for example, x^3+x+4) over $\mathbb{F}_{47}$. The group $E[37] \subseteq E(\mathbb{F}_{47^3})$ is the set of torsion points. Let $P = (24\alpha+1, 22\alpha^2+10\alpha+23) \in E[37]$ and $G_a = \langle P \rangle$. We denote, by e, the modified Tate-pairing as given in ([14]). Consider the parameters $n_1 = 2, n_2 = 3, n_3 = 5$ and $t_1 = 1, t_2 = 3, t_3 = 4$. Put the secrets $K_1 = 8$, $K_2 = 15$, $K_3 = 22$, $K_4 = 11$.
Level L_1.

- Choose the matrix $M_1 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ and $t_1 = 1$ random integer $a_{11} = 11 \in [0, 36]$.
- Compute $(b_{11}\ b_{12})^T = M_1 \cdot (a_{11}) = (33\ 7)^T$ where T denotes the transpose of a matrix.
- Thus, the shares of users u_{11}, u_{12} are $33P = (\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28)$ and $7P = (42\alpha^2 + 45\alpha + 19, 28\alpha^2 + 2\alpha + 6)$ respectively.

Level L_2.

- As $t_2 > n_1$, choose the matrix $M_2 = \begin{pmatrix} 4 & 6 & 1 \\ 2 & 5 & 8 \\ 1 & 0 & 9 \\ 5 & 2 & 10 \\ 7 & 3 & 11 \end{pmatrix}$ and $t_2 = 3$ integers $a_{21} = 33, a_{22} = 32, a_{23} = 5$ from [0, 36].
- Compute $(b_{11}\ b_{12}\ b_{21}\ b_{22}\ b_{23})^T = M_2 \cdot (a_{21}\ a_{22}\ a_{23})^T = (33\ 7\ 4\ 20\ 12)^T$. We note that b_{11} and b_{12} are the same as in level L_1.
- Thus, the shares of users u_{21}, u_{22}, u_{23} are $4P = (\alpha^2 + 30\alpha + 40, 14\alpha^2 + 7\alpha + 19)$, $20P = (36\alpha^2 + 17\alpha + 11, 7\alpha^2 + 19\alpha + 20)$ and $12P = (7\alpha^2 + 29\alpha + 45, 26\alpha^2 + 6\alpha + 10)$ respectively.

Level L_3.

- As $t_3 < n_1 + n_2$, let $t_3' = 6$.
- Choose the matrix $M_3 = \begin{pmatrix} 3 & 1 & 5 & 7 & 1 & 9 \\ 2 & 4 & 9 & 3 & 6 & 1 \\ 5 & 2 & 11 & 7 & 10 & 2 \\ 1 & 1 & 2 & 3 & 5 & 7 \\ 2 & 9 & 6 & 15 & 12 & 16 \\ 10 & 0 & 3 & 1 & 2 & 4 \\ 4 & 5 & 1 & 7 & 2 & 9 \\ 3 & 2 & 8 & 0 & 5 & 3 \\ 1 & 7 & 11 & 12 & 10 & 4 \\ 4 & 8 & 9 & 2 & 3 & 1 \end{pmatrix}$ and $t_3' = 6$ integers $a_{31} = 6, a_{32} = 25, a_{33} = 8, a_{34} = 19, a_{35} = 7, a_{36} = 20$ from [0, 36]. We note that $b_{11}, b_{12}, b_{21}, b_{22}, b_{23}$ are the same as in levels L_1 and L_2. Make $a_{35} = 7$ and $a_{36} = 20$ public.
- Compute $(b_{11}\ b_{12}\ b_{21}\ b_{22}\ b_{23}\ b_{31}\ b_{32}\ b_{33}\ b_{34}\ b_{35})^T = M_3 \cdot (a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{35}\ a_{36})^T = (33\ 7\ 4\ 20\ 12\ 12\ 3\ 5\ 18\ 5)^T$.
- Thus, the shares of users $u_{31}, u_{32}, u_{33}, u_{34}, u_{35}$ are $12P = (7\alpha^2+29\alpha+45, 26\alpha^2+6\alpha+10)$, $3P = (14\alpha^2+20\alpha+21, 22\alpha^2+29\alpha+40)$, $5P = (4\alpha^2+9\alpha+39, 14\alpha^2+42\alpha+5)$, $18P = (17\alpha^2+6\alpha+22, 26\alpha^2+32\alpha+10)$ and $5P = (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5)$ respectively.

Now compute $Q = a_{11}P + a_{21}P + a_{31}P = 13P = (17\alpha^2+13\alpha+4, 8\alpha^2+22\alpha+9)$. Then $v_1 = e(P, Q) + K_1 = e(P, 13P) + 8 = 37\alpha^2 + 28\alpha + 12$, $v_2 = e(P, 2Q) + K_2 = e(P, 26P) + 15 = 28\alpha^2 + 7\alpha + 4$, $v_3 = e(P, 3Q) + K_3 = e(P, 2P) + 22 = 36\alpha^2 + 32\alpha + 23$, $v_4 = e(P, 4Q) + K_4 = e(P, 15P) + 11 = 42\alpha^2 + 5\alpha + 24$. Make $P, v_1, v_2, v_3, v_4, M_1, M_2, M_3$ public.
Suppose the users $u_{11}, u_{21}, u_{23}, u_{32}$ collaborate to reconstruct the secrets K_1, K_2, K_3 and K_4. Then, u_{11} computes level secret $a_{11}P = 3^{-1}b_{11}P = 25(\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28) = (18\alpha^2 + 27\alpha + 12, 36\alpha^2 + 20\alpha + 32)$. The users u_{11}, u_{21}, u_{23} form a 3×3 matrix, say $M_2' = \begin{pmatrix} 4 & 6 & 1 \\ 1 & 0 & 9 \\ 7 & 3 & 11 \end{pmatrix}$ from first, third and fourth rows of M_2 and compute the inverse $M_2'^{-1} = \begin{pmatrix} 24 & 19 & 26 \\ 36 & 0 & 27 \\ 22 & 35 & 30 \end{pmatrix}$. Then they compute $M_2'^{-1} \cdot (33P\ 4P\ 12P)^T = ((\alpha^2+30\alpha+40, 33\alpha^2 + 40\alpha + 28)\ (4\alpha^2 + 9\alpha + 39, 33\alpha^2 + 5\alpha + 42)\ (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5))^T$. Thus, the level secret is

$a_{21}P = (\alpha^2 + 30\alpha + 40, 33\alpha^2 + 40\alpha + 28)$. In level L_3, the users $u_{11}, u_{21}, u_{23}, u_{32}$ know the entries of the corresponding rows of M_3. As $a_{35} = 7$ and $a_{36} = 20$ are public, first they compute

$$\begin{aligned}
b_{11}P - (a_{35}P + 9a_{36}P) &= 31P = (18\alpha^2 + 42\alpha + 8, 40\alpha^2 + 18\alpha + 46),\\
b_{21}P - (10a_{35}P + 2a_{36}P) &= 5P = (4\alpha^2 + 9\alpha + 39, 14\alpha^2 + 42\alpha + 5),\\
b_{23}P - (12a_{35}P + 16a_{36}P) &= 15P = (31\alpha^2 + 10\alpha + 24, 11\alpha^2 + 23\alpha + 44),\\
b_{32}P - (2a_{35}P + 9a_{36}P) &= 31P = (18\alpha^2 + 42\alpha + 8, 40\alpha^2 + 18\alpha + 46).
\end{aligned}$$

Then they take submatrix $M_3' = \begin{pmatrix} 3 & 1 & 5 & 7 \\ 5 & 2 & 11 & 7 \\ 2 & 9 & 6 & 15 \\ 4 & 5 & 1 & 7 \end{pmatrix}$ of M_3 and compute the inverse matrix $M_3'^{-1} = \begin{pmatrix} 16 & 36 & 23 & 15 \\ 26 & 35 & 7 & 35 \\ 21 & 7 & 22 & 20 \\ 1 & 1 & 21 & 6 \end{pmatrix}$. Now, we have

$$M_3'^{-1} \cdot \begin{pmatrix} 31P \\ 5P \\ 15P \\ 31P \end{pmatrix} = \begin{pmatrix} (18\alpha^2 + 42\alpha + 8, 7\alpha^2 + 29\alpha + 1) \\ (7\alpha^2 + 29\alpha + 45, 21\alpha^2 + 41\alpha + 37) \\ (18\alpha^2 + 12\alpha + 8, \alpha^2 + 38\alpha + 44) \\ (17\alpha^2 + 6\alpha + 22, 21\alpha^2 + 15\alpha + 37) \end{pmatrix}.$$

Thus, the level secret is $a_{31}P = (18\alpha^2 + 42\alpha + 8, 7\alpha^2 + 29\alpha + 1)$. Finally, they compute $Q = a_{11}P + a_{21}P + a_{31}P = 13P$ and reconstruct the secrets as $K_1 = v_1 - e(P, Q) = 8$, $K_2 = v_2 - e(P, 2Q) = 15$, $K_3 = v_3 - e(P, 3Q) = 22$, $K_4 = v_4 - e(P, 4Q) = 11$.

6 Complexity

The number of operations involved in the multiplication of a $n_i \times t_i$ matrix with $t_i \times 1$ matrix is $t_i n_i$. The time required to compute the scalar multiplication of a point on an elliptic curve using the *Double-and-Add algorithm* method [5] is $O(\log_2 \ell)$, where ℓ is the order of the point. The time computation for finding the inverse of a matrix of order t_i is t_i^3. The computational cost for the addition of two distinct points on an elliptic curve is **I**+2**M**+**S** and for doubling **I**+2**M**+2**S** (see [1]), where **I**, **S**, **M** denote inverse, squaring and multiplication, respectively. There are many pairings that cost logarithmic time (see [12,15], for example).
At the time of secret distribution. For computing m matrices of different order in our scheme, the Dealer requires $O(mn^2)$ operations. There are n scalar multiplications required to compute $b_{ij}x_{ij}P$, which costs $O(n\log_2 \ell)$. Dealer also requires m additions of points to compute Q that costs $O(m)$ and s pairings to compute v_i.
At the time of secrets reconstruction. The collaborating users need to find the inverse of m matrices of order t_i, $1 \le i \le m$, which takes $\sum_{i=1}^{m} t_i^3$ operations. For $t_i \le n_i$ and as $\sum_{i=1}^{m} n_i = n$, the sum $\sum_{i=1}^{m} t_i^3 \le n^3$. To find the level secret $a_{i1}P$, the users need t_i^2 points additions for Case I and $t_i'^2$ points additions for Case II. Furthermore, they required m additions of points to compute Q and s pairings to compute v_i, $1 \le i \le s$.
Hence, combining all these, the computational complexity of the scheme is $O(n^3)$.

The hierarchical scheme proposed in [23] is based on *linear homogeneous recurrences*. The complexity of their scheme is $O(n^{k_m - 1}\log n)$ where k_m is the threshold of the last level, which is an improvement over the complexity of the scheme proposed by Tassa [20]. However, the complexity of our scheme is $O(n^3)$.

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.

Funding The authors declare no special funding for the research work for this article.

References

1. R.K.K. Ajeena and K. Hailiza, *The computational complexity of elliptic curve integer sub-decomposition (ISD) method*, AIP Conference Proceedings, 1605 (2014) 557-562.
2. M. Bahramian and K. Eslami, *A new verifiable multi-secret sharing scheme based on elliptic curves and pairings*, Italian Journal of Pure and Applied Mathematics, n 41 (2019) 456-468.
3. M. Belenkiy, *Disjunctive multi-level secret sharing*, IACR Cryptology ePrint Archive 18 (2008).

4. V.P. Binu and A. Sreekumar, *Threshold Multi Secret Sharing Using Elliptic Curve and Pairing*, International Journal of Information Processing, 9(4) (2015) 100-112.
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, pp. 292-302 Springer, (1999).
6. O. Farras and C. Padro, *Ideal Hierarchical Secret Sharing Schemes*, IEEE Transactions on Information Theory, 58 (2012) 3273-3286.
7. 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, 45 (1999) 1717-1718.
8. S.D. Galbraith and N.P. Smart, *Evaluation report for CRYPTREC: security level of cryptography-ECDLP mathematical problem*. https://www.cryptrec.go.jp/exreport/cryptrec-ex-1029-2001.pdf (2001).
9. S.D. Galbraith, F. Hess, and F. Vercauteren, *Aspects of Pairing Inversion*, IEEE Transactions on Information Theory, Vol. 54 (12) (2008) 5719-5728.
10. H. Ghodosi, J. Pieprzyk and R. Safavi-Naini, *Secret sharing in multilevel and compartmented groups*, Proc. ACISP 1998, Lecture Notes in Comput. Sci., 1438 (1998) 367-378.
11. W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press (2012).
12. S. Ionica and A. Joux, *Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree*, In: Joye, M., Miyaji, A., Otsuka, A. (eds) Pairing-Based Cryptography - Pairing 2010. Pairing 2010. Lecture Notes in Computer Science, vol 6487. Springer, Berlin, Heidelberg, (2010).
13. D. Liu, D. Huang, P. Luo and Y. Da, *New schemes for sharing points on an elliptic curve*, Computers and Mathematics with Applications, 56 (2008) 1556-1561.
14. A. Menezes, *An introduction to pairing-based cryptography*, Recent trends in Cryptography, Contemp. Math., 477 (2009) 47-65, Amer. Math. Soc., Providence, RI, 2009.
15. V. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology, 17 (2004) 235-261.
16. A.R. Rao and P. Bhimasankaram, *Linear Algebra, 2nd Ed.*, Texts and Readings in Mathematics (TRIM) 19, Hindustan Book Agency (2000).
17. A. Shamir, *How to share a secret*, Comm. ACM, 22 (1979) 612-613.
18. J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, (1986).
19. G. Simmons, *How to (really) share a secret*, in Advances in Cryptology - Proceedings of CRYPTO-88 (S. Goldwasser, ed.) Lecture Notes in Comput. Sci., 403 (1990) 390-448.
20. T. Tassa, *Hierarchical threshold secret sharing*, Journal of Cryptology 20 (2007) 237-264.
21. A.N. Tentu, P. Paul and V.Ch. Venkaiah, *Conjunctive hierarchical secret sharing scheme based on MDS codes*, Combinatorial Algorithms, Lecture Notes in Comput. Sci., 8288, Springer (2013) 463-467.
22. S.J. Wang, Y.R. Tsai and C.C. Shen, *Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ecc*, Wireless Personal communications, 56 (2011) 173-182.
23. J. Yuan, J. Yang, C. Wang, X. Jia, F.-W. Fu and G. Xu, *A New efficient hierarchical multi-secret sharing scheme based on linear homogeneous recurrence relations*, Information Sciences 592 (2022) 36-49.