Number Theoretic Cryptography

A thesis submitted during 2023 to the University of Hyderabad in partial fulfilment for the award of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

Laba Sa

(Reg. No. 17MMPP01)

Under the supervision of

Dr. Mohan Chintamani

School of Mathematics and Statistics

University of Hyderabad

(P.O.) Central University, Gachibowli,
Hyderabad - 500 046,
Telangana, India

CERTIFICATE

This is to certify that the thesis entitled "**Number Theoretic Cryptography**" by **Laba Sa** bearing Reg. No. 17MMPP01 in partial fulfillment of the requirements for the award of **Doctor of Philosophy in Mathematics** is a bonafide work carried out by him under my supervision and guidance.

The thesis has not been submitted previously in part or in full to this or any other University or Institution for the award of any degree or diploma.

Further, the student has the following publication(s) before submission of the thesis for adjudication and has produced evidence for the same in the form of acceptance letter or the reprint in the relevant area of his research:

1. M. Chintamani and **L. Sa**, *A Blind Signature Scheme Based on Bilinear Pairings*, Proceedings of the Seventh International Conference on Mathematics and Computing, Advances in Intelligent Systems and Computing, vol 1412, Springer, Singapore, 1-8 (2022).

2. M. Chintamani, P. Paul and **L. Sa**, *Compartmented Multi-Secret Sharing Schemes using Elliptic Curves*, Journal of Information and Optimization Sciences (accepted).

3. M. Chintamani, P. Paul and **L. Sa**, *Conjunctive and Disjunctive Compartmented Secret Sharing Schemes using Elliptic Curves*, Tatra Mountains Mathematical Publications (submitted). An extended abstract of the paper is published in the Proceedings of Central European Conference on Cryptology (CECC '22), 34-37 (2022).

4. M. Chintamani, P. Paul and **L. Sa**, *Conjunctive Hierarchical Multi-Secret Sharing Scheme using Elliptic Curves*, Indian Journal of Pure and Applied Mathematics (submitted).

and

has made presentations in the following conferences:

1. A Blind Signature Scheme Based on Bilinear Pairings, *Seventh International Conference on Mathematics and Computing (ICMC 2021)*, IIEST Shibpur, India, March 02-05, 2021.

2. Conjunctive and Disjunctive Compartmented Secret Sharing Schemes using Elliptic Curves, *22nd Central European Conference on cryptography (CECC 2022)*, Smolenice, Slovakia, June 26-29, 2022.

Further, the student has passed the following courses towards fulfillment of course-work requirement for Ph.D. degree:

	Course Code	Course Name	Credits	Pass/Fail
1.	MM 801	Algebra	5	Pass
2.	MM 802	Analysis	5	Pass
3.	MM 810	Research Methodology and Ethics	4	Pass
4.	MM 816	Number Theory	5	Pass

Dr. MOHAN N CHINTAMANI
Assistant Professor
School of Mathematics & Statistics
University of Hyderabad
HYDERABAD-500 046. T.S.

Supervisor:

Dr. Mohan Chintamani

Dean of the School:

Prof. R. Radha 31/5/2023

संकाय-अध्यक्ष / DEAN
गणित और सांख्यिकी संकाय
School of Mathematics & Statistics
हैदराबाद विश्वविद्यालय/University of Hyderabad
हैदराबाद/Hyderabad-500 046. तेलंगाना, T.S.

TARU PUBLICATIONS

(Publishers of Scientific Books & Periodicals)

G-159, Pushkar Enclave, Pashchim Vihar, New Delhi - 110063, INDIA

Phone: +91-11-47234452 * Fax(USA): +1-610-980-5937 * E-mail: info@tarupublications.com

---

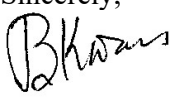
Date: 01-05-2023

Dr. Mohan Chintamani
School of Mathematics and Statistics
University of Hyderabad
Hyderabad-500046
India

Dear Dr Chintamani,

I am happy to inform you that on the recommendations of the referees, your paper titled "Compartmented Multi-Secret Sharing Scheme using Elliptic Curves " co-authored with Prabal Paul and Laba Sa Ref. No. JIOS-T- 1362 (2209069) has been accepted for publication in the Journal of Information and Optimization Sciences.

Sincerely,



Prof. (Dr.) B K Dass
Chief Editor

DECLARATION

I, **Laba Sa**, hereby declare that this thesis entitled "**Number Theoretic Cryptography**" submitted by me under the guidance and supervision of **Dr. Mohan Chintamani** is a bonafide research work. I also declare that it has not been submitted previously in part or in full to this University or any other University or Institution for the award of any degree or diploma.

Date: 31.05.2023

Laba Sa

Laba Sa

(Reg. No. 17MMPP01)

ACKNOWLEDGEMENTS

I had a big dream of taking Ph.D. admission in such a reputed university. I feel grateful to have here. I am extremely grateful to everyone who has supported me throughout my Ph.D. journey. This remarkable accomplishment would not have been possible without your help.

First and foremost, I would like to convey my sincere gratitude to my supervisor Dr. Mohan Chintamani for his continuous guidance and supervision throughout my Ph.D. journey. I am fortunate to have come in contact with him, who generously offered me many more hours of his valuable time each month. I will always be grateful to him for his inspirational guidance and constructive criticism, which helped me learn a lot about doing research and presenting it. Besides research work, I have learned many things from him, which will help me in my personal life. Dear sir, it has been a privilege to work with you and learn from you. I simply want to say, *"thank you for everything!"*

I would also like to express my deepest gratitude to Dr. Prabal Paul for overseeing my Ph.D. work and continuing to be a mentor to me. I owe him for his kind assistance with my research problems and insightful advices. This thesis would not have been completed without the constant support of both Dr. Mohan Chintamani and Dr. Prabal Paul. I would also thank both of them for advising and allowing me to visit IIT Ropar during my first year of Ph.D. and work with Dr. Tapas Chatterjee, where I learned some topics on elliptic curves and their application in number theory.

I am greatly thankful to my Research Advisory Committee (RAC) members Dr. M. Sumanth Datt, Dr. Sankar Ilangovan and Dr. Nageswara Rao Vemuri for their feedback, encouragement, and support throughout this journey.

I am deeply grateful to the teachers Prof. G. L. Reddy, Dr. M. Sumanth Datt, Dr. Abhay Soman and Dr. Anjana S., who taught me during my Ph.D. coursework. Their enthusiasm and passion for the subject matter were contagious, and I learned so much from their lectures, assignments, and discussions.

I want to thank all our School Deans since 2017, Prof. B. Sri Padmavati, Prof. G. L. Reddy, Prof. Arun Agarwal, Prof. C. Raghavendra Rao and Prof. R. Radha, for their kind assistance in fulfilling all administrative needs whenever required. I also want to thank the other faculty members of the School for

providing a welcoming and supportive environment for me to pursue my research.

I am thankful to the office bearer of our School and the Administration. They all are incredibly supportive. I sincerely appreciate their willingness to help me every time I needed it.

I also want to express my sincere appreciation to the MH-E Annex and NRS hostel staff for their exceptional work in providing an enjoyable, comfortable, and safe stay.

Thank you, University of Hyderabad, for providing such a wonderful campus where we can see the lovely peacock and roam many beautiful places like mushroom rock, high rock, temple rock, buffalo lake, etc.

I gratefully acknowledge the Council of Scientific and Industrial Research(CSIR), India, for providing me financial support under award letter 09/414(1146)/2017-EMR-I.

I am writing to express my gratitude to fellow research scholars of our School for their encouragement and support. As we prepare to embark on the next chapter of our lives, I wish you all the best in your future endeavors. I am confident that you will continue to achieve great things and make meaningful contributions to your respective fields. Thank you for the memories, the laughs, and the friendships that will last a lifetime.

Apart from our School, I have many friends in the University with whom I spent many memorable times. I want to thank all of them for their love, care, support, and encouragement.

Finally, I would like to express my gratitude to all my family members for their unwavering support and understanding during this time. Their love and encouragement have been a source of inspiration for me.

I apologize to the people whom I forgot to mention here and received support from their direct or indirect involvement. Thank you all for your support, encouragement, and assistance throughout my Ph.D. journey.

Dedicated to my parents

Late **Mrs. Koushalya Sa & Mr. Janekram Sa**

Second mother **Mrs. Jashoda Sa**

ABSTRACT

This thesis consists of five chapters.

In Chapter 1, some of the basics of elliptic curves and cryptography have been discussed. We mainly recall elliptic curve cryptography, basic signature schemes and bilinear pairings to the extent which is relevant to the thesis.

In Chapter 2, we discuss a blind signature scheme given by K. Chakraborty and J. Mehta (*A stamped blind signature scheme based on elliptic curve discrete logarithm problem*, International Journal of Network Security 14(6), 316-319 (2012)). We also discuss two attacks on it given by M. Tian, Y. Zhu and Z. Chen. By modifying a pairing (Lee's pairing), we defined a self-pairing map and proposed a blind signature scheme based on it. Our scheme avoids above said attacks.

The rest of the thesis contains our work in Elliptic Curve Cryptography, mainly in secret sharing schemes based on elliptic curves and bilinear pairings. The main purpose of using elliptic curves and bilinear pairings is that it gives similar security (as in existing schemes) with less key sizes.

Chapter 3 is devoted to our work on a multi-secret sharing scheme and a compartmented multi-secret sharing scheme. In Chapter 4, we have presented our work on conjunctive and disjunctive compartmented secret sharing schemes. We presented our work on a conjunctive hierarchical multi-secret sharing scheme in Chapter 5. All our schemes are verifiable (i.e., each collaborating user can verify the shares of other collaborating users at the time of reconstruction of the secret) and computationally secure. We have provided an example (computations are done using SageMath) of each of the schemes for illustration purposes. Moreover, we have done security analysis and complexity computations of our schemes.

Contents

Notations and Acronyms

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
$\mathbb{F}$	a field
$\mathbb{F}_q$	the finite field with q elements with characteristic p, p is prime
E	an elliptic curve
$E(\mathbb{F})$	the set of points on elliptic curve over $\mathbb{F}$
$E(\mathbb{F}_q)$	the set of points on elliptic curve over $\mathbb{F}_q$
$\#E(\mathbb{F}_q)$	the number of elements in $E(\mathbb{F}_q)$
$\mathcal{O}$	The point at infinity on an elliptic curve
$E[r]$	the set of r-torsion points on E
G_a	an additive cyclic group
G_m	a multiplicative cyclic group
Δ	the discriminant
$A \cong B$	A is isomorphic to B
$A \equiv B \pmod{n}$	A is congruent to B modulo n
$\mathbb{Z}_n$	the set of integers modulo n
$\mathbb{Z}_n^\times$	the set of invertible elements in $\mathbb{Z}_n$
$\mathbb{R}^+$	positive real numbers

AES	Advanced Encryption Standard
BDHP	Bilenear Diffie-Hellman Problem
DES	Data Encryption Standard
DL	Discrete Logarithm
DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECC	Elliptic Curve Cryptograophy
ECDDHP	Elliptic Curve Decisional Diffie-Hellman Problem
ECDHP	Elliptic Curve Diffie-Hellman Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
MDS	Maximum Distance Separable
RSA	Rivest-Shamir-Adleman

Introduction

We are now in a digital era. Everyone is involved in technology directly or indirectly. In this digital era, secret sharing and signatures are most commonly used to protect data, get permission from higher authorities to do specific work, etc. Cryptography is a vast subject that requires knowledge of various mathematical concepts, such as Group Theory, Number Theory, as well as Linear Algebra, Information Theory, and Probability.

Cryptography has been used to help in providing confidential communications between mutually trusted parties. The trusted parties communicate over a possibly insecure (public) channel so that an adversary cannot obtain what is being communicated. To communicate, they require cryptographic tools such as Hash functions, Signature and Secret Sharing schemes, etc., to achieve specific security objectives. In the 1970s, Diffie-Hellman introduced the concept of *public-key cryptography*. Their idea was to design a cryptosystem with two distinct keys, one is *public* and other is *private*. The public key would be used for encrypting the message, while the private key would be used for decrypting the encrypted message. The public key is accesible to everyone, but only one person, who will receive the encrypted message, has access to the private key. The cryptosystem developed by Rivest, Shamir and Adleman (RSA Cryptosystem), is the earliest and most popular example of a public-key cryptosystem.

Elliptic curves are of great importantance both in Number Theory and Cryptography. It has many applications in Number Theory, such as in proving Fermat's Last Theorem, integer factorization algorithms, etc. While in Cryptography, it is used primarily to secure cryptographic schemes with small key sizes. One of the advantages of using elliptic curves in cryptographic systems is that key sizes are smaller and thus, the cryptographic algorithms run faster.

In this thesis, we mainly worked on Elliptic Curve Cryptography, Signature schemes and Secret Sharing Schemes using elliptic curves. We follow closely

[20, 31, 41, 60, 67].

The thesis consists of five chapters.

Chapter 1. *Preliminaries*

In Chapter 2, we discuss some of the basics of elliptic curves and cryptography. We recall elliptic curve cryptography, basic signature schemes and bilinear pairings to the extent which is relevant to the thesis.

Chapter 2. *A blind signature scheme*

In this chapter, we discuss our work [17] on an analogous/modified version of a scheme given by K. Chakraborty and J. Mehta [10]. The Chakraborty-Mehta's scheme is not secure, which is proved by M. Tian, Y. Zhu and Z. Chen [65] by giving two simple but powerful attacks. Our blind signature scheme is secure and avoids the attacks given by M. Tian, Y. Zhu and Z. Chen. The scheme is based on self-pairing map. An anti-symmetric self-pairing was defined by H.-S. Lee [38]. Based on that, a symmetric self-pairing is defined in [17]. The scheme is based on symmetric self-pairing and elliptic curves.

Chapter 3. *Compartmented secret sharing scheme*

We have focused on our work [14] on a multi-secret sharing scheme and a compartmented multi-secret sharing scheme in this chapter. In a compartmented secret sharing scheme, a group of participants is partitioned into several compartments. A share of a secret is distributed among all the participants. At a later time, if required, a threshold number of participants from each compartment and a total of global threshold participants collaborate to reconstruct the secret.

Chapter 4. *Conjunctive and disjunctive compartmented secret sharing schemes*

In this chapter, we have studied conjunctive and disjunctive compartmented secret sharing schemes. This contains our work [15].

Chapter 5. *Conjunctive Hierarchical Multi-Secret Sharing Schemes*

We presented our work [16] on a conjunctive hierarchical multi-secret sharing scheme in this chapter. In a conjunctive hierarchical secret sharing scheme, the participants are divided disjointly into several levels. A secret is distributed to all the participants by a trusted Dealer in a way so that a predetermined number of participants from each level and/or with the cooperation of higher levels can reconstruct the secret.

The schemes which we presented in Chapter 3, 4 and 5 are based on elliptic curves and bilinear pairings. The schemes are verifiable and computationally efficient. We have provided security analysis of all the schemes and complexity aspects are also discussed. For the illustrations, we have given an example of each of the schemes. The computations are done using SageMath.

Chapter 1

Preliminaries

In this chapter, we discuss some of the basics of elliptic curves and cryptography. We recall elliptic curve cryptography, basic signature schemes and bilinear pairings to the extent which is relevant to the thesis.

1.1 Basics of Elliptic Curves

We assume the basic knowledge of group theory, ring theory and fields which are needed to define elliptic curves. We refer to [19, 28, 39] for a more detailed discussion of this.

Elliptic curves are described as the set of solutions to an equation in two variables.

Definition 1.1.1 A *Weiestrass* equation over a field $\mathbb{F}$ is an equation of the form

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

We define the following terms

$$\begin{aligned} r_2 &= a_1^2 + 4a_2, \\ r_4 &= 2a_4 + a_1a_3, \\ r_6 &= a_3^2 + 4a_6, \\ r_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= r_2^2 - 24r_4 \\ \text{and } \Delta &= -r_2^2r_8 - 8r_4^3 - 27r_6^2 + 9r_2r_4r_6. \end{aligned}$$

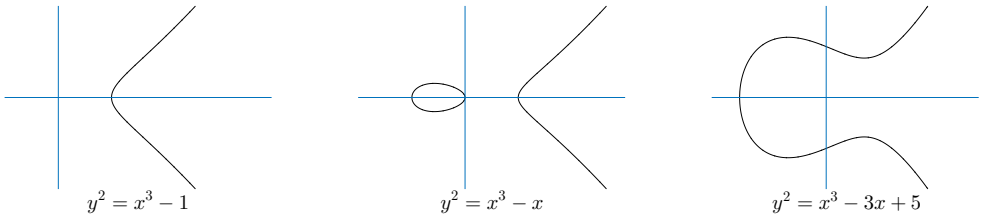


Figure 1.1: Examples of elliptic curve over $\mathbb{R}$.

Δ is called the discriminant of the curve E. If $\Delta \neq 0$, then the set of solutions of Equation 1.1 is called an *elliptic curve*.

If the characteristic of $\mathbb{F}$ is greater than 2, replacing y by $y - \frac{1}{2}(a_1x + a_3)$, Equation 1.1 can be reduced to

$$E' : \ y^2 = x^3 + a_2'x^2 + a_4'x + a_6'. \tag{1.2}$$

Furthermore, if characteristic of $\mathbb{F}$ is not equal to 3, replacing x by $x - \frac{1}{3}a_2'$, Equation 1.2 can be reduced to

$$E'' : \ y^2 = x^3 + a_4''x + a_6''. \tag{1.3}$$

Equation 1.3 is called the *normal form* of the elliptic curve.

By $E(\mathbb{F})$, we denote the set of all the points on E over $\mathbb{F}$ along with a point at infinity $\mathcal{O}$. Example of elliptic curves over $\mathbb{R}$ is depicted in Figure 1.1.

1.1.1 The group structure on $E(\mathbb{F})$

Consider an elliptic curve

$$E : \ y^2 = x^3 + ax + b \tag{1.4}$$

over $\mathbb{F}$ where $a, b \in \mathbb{F}$ with non-zero discriminant. We define the addition of points as follows.

Definition 1.1.2 ([36]) Let $E : \ y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{R}$ and $P, Q \in E(\mathbb{R})$ be two points on the curve. We define the sum $P + Q$ and the negative of P by the following rules.

1. If $P = (x, y)$, then $-P = (x, -y)$. That is, the negative of P is the reflection of P about the x-axis.

2. If $Q \neq \pm P$ and $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$, then draw a line L passing through P and Q which intersect the curve at one more point $\overline{P+Q}$. The reflection of $\overline{P+Q}$ about x-axis is $P+Q$.

3. If $P = Q$ and $P \neq -P$, draw a tangent line L to the curve at P. If $\overline{2P}$ is the point intersection of the line L and the curve, the reflection of $\overline{2P}$ about x-axis is $2P$.

4. If $Q = \mathcal{O}$, then $P+Q = P+\mathcal{O} = P$. In this case, the line L passing through P and Q is a vertical line. The point $\mathcal{O}$ acts as the additive identity.

5. If $Q = -P$, then $P + Q = \mathcal{O}$.

The point at infinity $\mathcal{O}$ is the point of intersection where the y-axis and a vertical line meet. An example of the point addition and doubling on an elliptic curve over $\mathbb{R}$ is illustrated in Figure 1.2.

Now we will see why the line L passing through the points P and Q intersects the curve in at most one more point. We will also derive the formula for the sum $P + Q$.

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P + Q = (x_3, y_3)$. Our aim is to write x_3 and y_3 in terms of x_1, x_2, y_1, y_2. Suppose that $P \notin \{\pm Q, \mathcal{O}\}$ and $Q \neq \mathcal{O}$. Then the equation of L is $y = \lambda x + c$ where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ and $c = y_1 - \lambda x_1$. The point $(x, \lambda x + c)$ lies in $E(\mathbb{R})$ if and only if $(\lambda x + c)^2 = x^3 + ax + b$. If $P = (x_1, \lambda x_1 + c)$ and $Q = (x_2, \lambda x_2 + c)$, then we have two roots x_1 and x_2 of the above equation as the points are on the curve. If x_3 is the remaining root of the cubic equation, the third point of the intersection of L and the curve E is $\overline{P+Q} = (x_3, -y_3)$. Hence the sum $x_1 + x_2 + x_3$ is λ^2. Thus, $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$. In terms of x_1, x_2, y_1, y_2, we have

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \end{aligned} \tag{1.5}$$

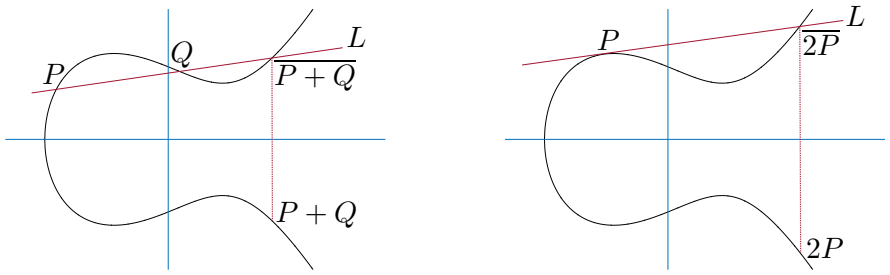


Figure 1.2: Point addition and doubling on elliptic curve E over $\mathbb{R}$.

If $P = Q$ and $P \neq -P$, the slope λ of the tangent line L at P is the derivative dy/dx of Equation 1.4 at P. Then $\lambda = (3x_1^2 + a)/2y_1$, and we obtain the formula for $2P = (x_3, y_3)$ where

$$\begin{aligned} x_3 &= \left(\frac{3x^2 + a}{2y_1}\right)^2 - 2x_1, \\ y_3 &= \left(\frac{3x^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \end{aligned} \tag{1.6}$$

The set of all points on an elliptic curve E over $\mathbb{F}$ satisfy the following properties. For given P, Q and R in $E(\mathbb{F})$,

1. Closure: $P + Q \in E(\mathbb{F})$.
2. Associativity: $(P + Q) + R = P + (Q + R)$.
3. Existence of identity: $P + \mathcal{O} = \mathcal{O} + P = P$.
4. Existence of inverses: $P + (-P) = (-P) + P = \mathcal{O}$.

It also satisfies the commutative property. Thus, the set $E(\mathbb{F})$ forms an commutative group.

1.1.2 Elliptic curves over finite field

Elliptic curves defined over a finite field are important in public-key cryptography (see Section 1.2). The elliptic curve over $\mathbb{F}_q$, in the normal form, where characteristics greater than 3 is defined as follows.

Definition 1.1.3 Let $a, b \in \mathbb{F}_q$ with $4a^3 + 27b^2 \neq 0$. The set of solutions (x, y) of the equation

$$E: \ y^2 = x^3 + ax + b. \tag{1.7}$$

is defined as elliptic curve over $\mathbb{F}_q$.

Throughout the thesis, we consider the elliptic curve as in Equation 1.7.

We need the following well known results on elliptic curves.

Theorem 1.1.4 ([67, p.97]) *We have*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_m \quad or \quad \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$$

for some $m \in \mathbb{N}$, or for some m_1, $m_2 \in \mathbb{N}$ with $m_1 | m_2$.

Theorem 1.1.5 (Hasse [67, p.97]) *Let $\#E(\mathbb{F}_q) = n$. Then n satisfies*

$$|q + 1 - n| \leq 2\sqrt{q}.$$

Theorem 1.1.6 ([67, p.98]) *Let $\ell = p^i$ for $i \in \mathbb{N}$, where p is a prime and let $n = \ell + 1 - a$. Then there exists an elliptic curve E defined over $\mathbb{F}_\ell$ such that $\#E(\mathbb{F}_\ell) = n$ if and only if $|a| \leq 2\sqrt{\ell}$ and a satisfies one of the following:*

1. *gcd(a, p)=1,*
2. *$2 \mid i$ and $a = \pm 2\sqrt{\ell}$,*
3. *$2 \mid i$, $p \not\equiv 1 \pmod 3$, and $a = \pm\sqrt{\ell}$,*
4. *$2 \nmid i$, $p = 2$ or 3, and $a = \pm p^{(i+1)/2}$,*
5. *$2 \mid i$, $p \not\equiv 1 \pmod 4$, and $a = 0$,*
6. *$2 \nmid i$ and $a = 0$.*

1.2 Cryptography

Cryptography is an intriguing field of study as it combines elegant mathematics with many cutting-edge fields of computer science and engineering to find the solutions that affect many parts of life in the digital era. It is about the algorithms

and protocols that can be used to provide the core security services of secrecy, data integrity, source authentication, and digital signatures (see [43], for example).

Definition 1.2.1 (see [55]) A *cryptographic algorithm* is a well-defined transformation that, given an input value, generates an output value while satisfying specific security objectives. A distributed method that properly describes the interactions among two or more participants while meeting specific security objectives is known as a *cryptographic protocol*. A *cryptographic scheme* is a collection of associated cryptographic algorithms and protocols that aims to meet certain security requirements.

In a cryptographic scheme, participants interact by sending their messages to each other through communication channels. Communication channels are frequently assumed to offer specific security guarantees. A communication channel is either *private* or *public*. Suppose that two participants **A** and **B** agreed on a secret key. Suppose **A** wishes to communicate a secret message to **B** over a public/private channel. The original message, also known as *plaintext*, is converted into a chaotic form, known as *ciphertext*, using the secret key unreadable to anyone who does not have the secret key. This is known as *encryption*. Then participant **B** will get the original message by converting the ciphertext using the secret key. This process is known as *decryption*. The keys and the methods for using them to encrypt and decrypt the data are fully specified by a *cryptosystem*. An *adversary* is an alliance of an attacker and/or one or more of the participants.

Security goals. The communications between entities (or participants) must satisfy some security goals to keep their communications secret. The following fundamental objectives have to be scrutinized for secure communications. Let **A** and **B** be two communicating entities, and **X** be an adversary.

1. *Confidentiality*: limiting access to data to those who are allowed to see it, i.e., **X** can not read the message.

2. *Data integrity*: making sure that an adversary has not altered the data, i.e., data sent by **A** that has been altered by **X** should be detectable by **B**.

3. *Data origin authentication*: confirming the original source of data, i.e., **B** can verify that the message is actually originated from **A**.

Cryptographic systems are classified as *symmetric-key (secret-key) cryptography* and *public-key cryptography*. In symmetric-key cryptography, the participants first agree on secret and authentic keying data. Then, to ensure confidentiality, a symmetric-key encryption may be used. Data integrity and data origin authentication may also be achieved using a MAC (message authentication code) algorithm. While in public-key cryptographic schemes, the communicating entities only exchange authentic keying material and not the secret. Each participant chooses a pair (e_k, d_k) comprised of a private key e_k and a corresponding public key d_k. It is computationally infeasible to figure out the private key with the knowledge of the public key.

The security of commonly used public-key schemes is based on the intractability of some of well known number-theoretic problems. For example,

1. Integer factorization problem: the security of RSA public-key encryption and signature methods depends on the complexity of it.

2. Discrete logarithm problem: the security of the ElGamal public-key encryption and signature schemes and its variations, like the Digital Signature Algorithm (DSA), depends on its hardness.

3. Elliptic curve discrete logarithm problem: the security of all elliptic curve cryptographic schemes depends on the hardness of it.

In 1977, a public-key cryptographic scheme was proposed by Rivest, Shamir and Adleman [52], called RSA scheme. The scheme chooses two large distinct primes p and q and set $n = pq$. Let e_k be an encryption exponent such that $1 < e_k < \varphi(n)$ and $\gcd(e_k, \varphi(n))= 1$, where $\varphi(n) = (p-1)(q-1)$. We note that n is public, and p and q are secrets. Let d_k be the decryption exponent such that $1 < d_k < \varphi(n)$ and $e_k d_k \equiv 1 \pmod{\varphi(n)}$.

The RSA scheme use the fact that $m^{e_k d_k} \equiv m \pmod{n}$, $\forall m \in \mathbb{Z}$. The encryption of a message m is done by computing the ciphertext $c \equiv m^{e_k} \pmod{n}$. The ciphertext c can be decrypted by computing $c^{d_k} \equiv (m^{e_k})^{d_k} \equiv m \pmod{n}$. Here we assume the hardness of the integer factorization problem. It is computationally infeasible to find the factors of n using e_k.

1.3 Threshold Cryptography

In many cases, one participant shouldn't have sole authority over access to a valuable asset. For instance, opening a bank requires two keys, one maintained by the owner and the other by a bank employee. The access to secret key should not be limited to a single participant in an ideal cryptographic schemes. Instead, it must be distributed among several participants such that a sufficient number of participants can collaboratively access the key.

Threshold cryptography consists of strategies for distributing basic cryptographic schemes among multiple participants. The secret sharing scheme is a basis of threshold cryptography. The secret is partitioned into many parts. Each part is called a *share* of the secret. The reconstruction of the secret is possible/allowed whenever a sufficient number of shares are available. Otherwise, the secret cannot be reconstructed. A secret sharing scheme involves a set of participants and a trusted Dealer.

Definition 1.3.1 (Trusted Dealer) In a secret sharing scheme, a trusted Dealer is a participant who is trusted by all other participants to perform a particular service properly. The Dealer has the authority to set up a scheme and distribute the shares among the participants.

Definition 1.3.2 (Access structure) Suppose there are n participants in a secret sharing scheme, and out of n, if at least t participants collaborate, they are allowed to reconstruct the secret key. Then the number t is called a *threshold* number. The set of participants who are allowed to reconstruct the secret key is known as an *authorized set*. The collection of all authorized sets is called the *access structure*.

Secret sharing scheme. A secret sharing scheme comprises of distribution and reconstruction protocols. In distribution protocol, a share of a secret is distributed to each participant. While in reconstruction protocol, any set of participants from access structure pools their shares and collaborate to reconstruct the secret.

In some secret sharing schemes, verifying the shares by any participant can allow them to know their originality and avoid attacks.

Verifiable secret sharing scheme. Verifiable secret sharing (VSS) is an important primitive of secret sharing scheme that permits sharing a secret in the

presence of an adversary. The uniqueness of a VSS scheme is that everyone can verify the consistency of the shares, having no idea about the secret. A verifiable secret sharing scheme is necessary to resist the following.

1. At the time of distribution of shares, a dealer may transmit incorrect or inconsistent shares to some of the participants.

2. At the time of reconstruction of the secret, participants provide incorrect shares.

Many secret sharing schemes have been proposed in the literature (see [2, 9, 21, 33, 35, 37, 56, 59, 70]). Secret sharing schemes are not limited to a group of participants; they are extended to multiple groups of participants, such as compartmented and hierarchical structures.

1.3.1 Hierarchical secret sharing scheme

In a hierarchical secret sharing scheme, the group of participants is partitioned into multiple levels. The participants in a level have more priority than the participants in the lower level. This means that if some participants are absent and the participants are not in threshold numbers at a level, they take the help of higher-level participants to reconstruct the secret. So a higher-level participant can collaborate with the lower-level participants to reconstruct the secret. For examples,

1. to validate an electronic payments transfer, a bank may demand an agreement of two assistant managers or three tellers. An assistant manager can substitute for an absent teller, if the need arise.

2. a company would require the consent of two managers or three assistant managers to authorize a digital locker. If there are only two assistant managers present, a manager can fill in for the missing one.

There are two types of hierarchical access structures, namely, conjunctive and disjunctive access structures (see [59, 63], for example).

Definition 1.3.3 (Hierarchical access structures) Suppose that there is a set U of n participants divided into m disjoint levels $L_1, L_2, \cdots, L_m$. Define L_i as a higher level than L_j if $i < j$. Let t_i be the threshold for level L_i or higher and $t_1 \leq t_2 \leq \cdots \leq t_m$.

1. The conjunctive hierarchical access structure is defined as

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

   A set of participants is authorized to reconstruct the secret provided the set contains at least t_i participants from each level L_i or higher.

2. If we replace "for all" with "for some" in the above, then we call it the disjunctive hierarchical access structure.

1.3.2 Compartmented secret sharing scheme

In a compartmented access structure, the group of participants is partitioned into disjoint compartments. The secret is partitioned so that it can be recovered with the cooperation of the participants if the number of participants from every compartment exceeds a predefined compartment threshold and the total number of participants exceeds the global threshold. For example, suppose that two states decide to to regulate the use of a common asset which may lead to joint action. At least two ministers from each state and a total of five ministers must work together.

The compartmented secret sharing scheme was introduced by Simmon [59]. The access structure for the compartmented secret sharing scheme (see [29, 64]) is defined as follows.

Definition 1.3.4 (Compartmented access structure) Suppose that there is a set U of n participants partitioned into 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 participants, with at least t_i participants from C_i, $1 \leq i \leq m$, is authorized to reconstruct the secret. Mathematically, the compartmented access structure is is defined as

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

1.4 Elliptic Curve Cryptography(ECC)

Elliptic curves have been progressively important in number theory and related topics such as cryptography over the last four decades. In the 1980s, elliptic curves

Security level (bits) →	80 SKIPJACK	112 Triple-DES	128 AES-Small	192 AES-Medium	256 AES-Large
EC parameter n DL parameter q	160	224	256	384	512
RSA modulus n DL modulus p	1024	2048	3072	8192	15360

Table 1.1: Comparison of key sizes

were first used in cryptography. The algorithms for factorization and primality testing of an integer were developed using elliptic curves. In the 1980s and 1990s, elliptic curves played a crucial role in proving Fermat's Last Theorem.

While deciding on a public key scheme for a specific use, one needs to look into some of the parameters carefully. For example,

1. *Functionality.* Is the scheme capable of providing the necessary results?
2. *Security.* What guarantees are there that the scheme is secure?
3. *Performance.* Do the protocols fulfill performance criteria for the intended level of security?

The fundamental reason to use elliptic curves in a cryptographic scheme is to provide similar security with a smaller key size. An example of the comparison is given in Table 1.1 (see [31, p.19]), which shows that lower key parameters can be used in ECC comapred to other systems with same level of security. The variation in key size is more noticeable as security levels increases. Smaller parameters can provide advantages such as faster computations and smaller keys and certificates. The advantages offered by ECC are significant in contexts where storage, speed of processing, bandwidth is limited.

Elliptic curve key generetion. Let $P \in E(\mathbb{F}_q)$ be a point of prime order r. The elliptic curve E, the integers q, r, the point P are the public domain parameters. An integer a chosen arbitrarily from $[1, r-1]$ is a private key. The corresponding public key is $Q = aP$.

Some of the hardness assumptions that are commonly used in cryptographic schemes based on elliptic curves are given below.

Definition 1.4.1 (Elliptic curve discrete logarithm problem (ECDLP)) The *elliptic curve discrete logarithm problem* is to find the integer a from given points P and aP.

Definition 1.4.2 (Elliptic curve Diffie-Hellman problem (ECDHP)) Given points P, aP and bP for $a, b \in \mathbb{Z}$, the problem of computing abP is called as *elliptic curve Diffie-Hellman problem.*

Definition 1.4.3 (Elliptic curve decisional Diffie-Hellman problem (ECDDHP)) Given points P, aP, bP and cP for $a, b, c \in \mathbb{Z}$, the *elliptic curve decisional Diffie-Hellman problem* is to determine whether $abP = cP$.

An application of ECDHP is used in key exchange protocol. For instance, suppose $\mathcal{A}$ and $\mathcal{B}$ are two entities that want to create a common secret K by sending their messages to each other through a public channel. Suppose they agreed upon a group $G = \langle P \rangle$ of prime order r where P is a point on an elliptic curve $E(\mathbb{F}_q)$. $\mathcal{A}$ chooses at random some $a \in [1, r-1]$ and sends the point aP to $\mathcal{B}$. Similarly, $\mathcal{B}$ chooses at random some $b \in [1, r-1]$ and sends the point bP to $\mathcal{A}$. Then they both can compute secret key $K = abP$ by using their private keys. Here the key K remains unknown to any attacker even if he knows P, aP and bP.

There are some known attacks on ECDLP. D. Shanks [57] developed a method, called *Baby Step, Giant Step*, that requires $\sqrt{r}$ steps and around $\sqrt{r}$ storage. As a result, it is only suitable for r of moderate size. The Baby Step, Giant Step method has a drawback in requiring a lot of storage. *Pollard's* ρ method [47] runs in about the same amount of time as Baby Step, Giant Step, but requires less storage. For more details and attacks on ECDLP, we refer to [67].

1.5 Bilinear Pairings

Bilinear pairing is a one-way mapping. It means that computing the pairing of given inputs is easy, however finding the preimage of a given image is difficult. We recall the definition as given in [41].

Definition 1.5.1 (Bilinear Pairings) "Let G_a and G_m be an additive cyclic group and a multiplicative cyclic group, respectively, with the same prime order

r. A bilinear pairing e is a map

$$\mathrm{e} : G_a \times G_a \longrightarrow G_m$$

which satisfy the bilinearity, non-degeneracy and computability properties. That is, 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 $\mathrm{e}(x_1, y_1) \neq 1$. Similarly, 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".

Remark 1.5.2 Following are some of the properties of the bilinear pairings. For all $x, y \in G_a$,

1. $\mathrm{e}(x, 0) = \mathrm{e}(0, y) = 1$.
2. $\mathrm{e}(mx, ny) = \mathrm{e}(x, y)^{mn}, \forall m, n \in \mathbb{Z}$.
3. $\mathrm{e}(x, y) = \mathrm{e}(y, x)$.
4. If $\mathrm{e}(x, y) = 1, \forall x \in G_a$, then we have $y = 0$. (This is equivalent to the non-degeneracy condition).

We have the following easy observation, which is useful in the security analysis of our schemes.

Observation 1.5.3 *For any $x, y, y' \in G_a$ and $x \neq 0$, we have $\mathrm{e}(x, y) = \mathrm{e}(x, y')$ iff $y = y'$.*

Proof. Suppose $x, y, y' \in G_a$, $x \neq 0$. Since G_a is cyclic of prime order r and $x \neq 0$, there exists $a, a' \in \mathbb{Z}$ such that $y = ax$, $y' = a'x$. Suppose $\mathrm{e}(x, y) = \mathrm{e}(x, y')$, i.e. $\mathrm{e}(x, ax) = \mathrm{e}(x, a'x) \implies \mathrm{e}(x, x)^a = \mathrm{e}(x, x)^{a'}$. As $x \neq 0$ and also e is non-degenerate, we have $\mathrm{e}(x, x) \neq 1$. Thus, $a \equiv a' \pmod{r}$. Hence $y = y'$.

The one-wayness of the bilinear map is that, to find $x, y \in G_a$ such that $\mathrm{e}(x, y) = g$ for a given pairing e and a value $g \in G_m$ is difficult. Also, to find $y \in G_a$ for a given $x \in G_a$ and $g \in G_m$ such that $\mathrm{e}(x, y) = g$ is difficult.

The intractability of the following (see [41]) problem determines the security of many pairing-based protocols.

Definition 1.5.4 (Bilinear Diffie-Hellman problem (BDHP)) "Let e be a bilinear pairing on (G_a, G_m). The *bilinear Diffie-Hellman problem (BDHP)* is to compute $e(x,x)^{abc}$ for given x, ax, bx, $cx \in G_a$".

1.5.1 Divisors

Let $c(x,y)$ be the polynomial defining E (see Equation 1.1). Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$. A rational function f on E is an element of the field of fractions of the ring $\overline{\mathbb{F}}_q[x,y]/(c(x,y))$.

A *divisor* D on $E(\overline{\mathbb{F}}_q)$ is a formal sum of points $D = \sum_{P \in E(\overline{\mathbb{F}}_q)} \nu_P[P]$ where ν_P are integers such that $\nu_P = 0$ for all but finitely many P. The sum $\sum_{P \in E(\overline{\mathbb{F}}_q)} \nu_P$ is called as the degree ($\deg(D)$) of the divisor D. If $\deg(D)= 0$, then D is known as a zero divisor. The set of points P for which $\nu_P \neq 0$ is known as the support of D. The divisor of a non-zero rational function f is defined as $\mathrm{div}(f)= \sum_{P \in E(\overline{\mathbb{F}}_q)} \mathrm{ord}_P(f)[P]$ where $\mathrm{ord}_P(f)$ is the order of P as a root/pole of f. The divisors of rational functions are also called *principal divisors*. It is well known that a divisor $D = \sum_{P \in E(\overline{\mathbb{F}}_q)} \nu_P[P]$ is principal if and only if D is a zero divisor and $\sum_{P \in E(\overline{\mathbb{F}}_q)} \nu_P P = \mathcal{O}$.

If $P = (x,y)$, then $f(P) = f(x,y)$. If f is a rational function and D is a divisor such that $\mathrm{div}(f)$ and D have disjoint support, then we define $f(D)$ to be $\prod_{P \in E(\overline{\mathbb{F}}_q)} f(P)^{\nu_P}$. For more details on divisors, we refer to [20, 67].

1.5.2 The Tate pairing

Before defining Tate pairing, we recall the following definitions as in [41].

Definition 1.5.5 (Embedding degree [41]) "Let E be an elliptic curve over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_q)$ be a point of prime order r. Assume that $\gcd(r,q)= 1$. Then the *embedding degree* of $G = \langle P \rangle$ is the least $k \in \mathbb{Z}^+$ such that $r \mid q^k - 1$".

Definition 1.5.6 (Torsion points) Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. Let r be a prime divisor of $\#E(\mathbb{F}_q)$. The r-torsion points of E, denoted by $E[r]$, is the set $E[r] = \{P \in E(\overline{\mathbb{F}}_q) : rP = \mathcal{O}\}$.

The following theorem says that, $E[\ell]$ forms a group of rank at most 2.

Theorem 1.5.7 ([67, p.79]) *Let $\ell \in \mathbb{Z}^+$. If the characteristic of $\mathbb{F}$ is not equal to 0 or does not divide ℓ, then*

$$E[\ell] \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell.$$

According to the above theorem, if $\gcd(r, q) = 1$ then $E[r] \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$.

Example 1.5.8 Let E be an elliptic curve $y^2 = x^3 + 4x + 2$ over $\mathbb{F}_5$. Then $E(\mathbb{F}_5) = \{\mathcal{O}, (3,1), (3,4)\}$ and $\#E(\mathbb{F}_5) = 3$. Now $\gcd(3,5) = 1$ and $3 \mid 5^2 - 1$, i.e., the embedding degree of $E(\mathbb{F}_5)$ is 2. Let $\mathbb{F}_{5^2} = \mathbb{F}_5[\gamma]/(\gamma^2 + \gamma + 1)$. Then $E(\mathbb{F}_{5^2})$ and the 3-torsion points $E[3]$ are as follows.

$$\begin{aligned} E(\mathbb{F}_{5^2}) \;=\; & \{\mathcal{O}, (3,1), (3,4), (0,1+2\gamma), (0,4+3\gamma), (1,1+2\gamma), (1,4+3\gamma), \\ & (2,3+\gamma), (2,2+4\gamma), (4,1+2\gamma), (4,4+3\gamma), (3+4\gamma,1), \\ & (3+4\gamma,4), (4+\gamma,1), (4+\gamma,4), (2\gamma,3+2\gamma), (2\gamma,2+3\gamma), \\ & (4\gamma,2\gamma), (4\gamma,3\gamma), (1+\gamma,2+2\gamma), (1+\gamma,3+3\gamma), (2+\gamma,3+\gamma), \\ & (2+\gamma,2+4\gamma), (1+4\gamma,3+\gamma), (1+4\gamma,2+4\gamma), (3+3\gamma,4+2\gamma), \\ & (3+3\gamma,1+3\gamma)\} \end{aligned}$$

and

$E[3] = \{\mathcal{O}, (3,1), (3,4), (1,1+2\gamma), (1,4+3\gamma), (1+\gamma,2+2\gamma), (1+\gamma,3+3\gamma), (4\gamma,2\gamma), (4\gamma,3\gamma)\}$.

Let $S = (3,1)$ and $T = (4\gamma, 2\gamma)$. Then every point of $E[3]$ can be written as a linear combination of S and T. For example $0S + 0T = \mathcal{O}$, $0S + 1T = (4\gamma, 2\gamma)$, $0S + 2T = (4\gamma, 3\gamma)$, $1S + 0T = (3,1)$, $1S + 1T = (1, 4+3\gamma)$, $1S + 2T = (1+\gamma, 3+3\gamma)$, $2S + 0T = (3,4)$, $2S + 1T = (1+\gamma, 2+2\gamma)$, $2S + 2T = (1, 1+2\gamma)$. Hence, we observe that $E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Let $\#E(\mathbb{F}_q) = vr$, where r is a prime integer and $r \nmid q-1$. Then, $k > 1$. Then $E[r] \subseteq E(\mathbb{F}_{q^k})$, and so $r^2 | \#E(\mathbb{F}_{q^k})$ (see [4]). We further assume that $\gcd(v, r)=1$, then $r \nmid \#E(\mathbb{F}_{q^k})/r^2$. We denote μ_r, the order-r subgroup of $\mathbb{F}_{q^k}^*$. Then the (modified) Tate pairing is defined as follows.

Definition 1.5.9 ([41]) "Let P, $Q \in E[r]$ and f_P be a function with $\mathrm{div}(f_P) = r[P] - r[\mathcal{O}]$. Let $R \in E[r]$ such that $R \notin \{\mathcal{O}, P, -Q, P - Q\}$, and $D_Q = [Q +$

$R] - [Q]$. Note that the choice of R ensures that D_Q and $\text{div}(f_P)$ have disjoint support. Then the (modified) *Tate pairing* is a map

$$\text{e} : \ E[r] \times E[r] \longrightarrow \mu_r$$

defined as $\text{e}(P,Q) = f_P(D_Q)^{(q^k-1)/r} = (f_P(Q+R)/f_P(R))^{(q^k-1)/r}$".

The value $\text{e}(P,Q)$ is independent of the choice of the function f_P and the point R, indicating that the Tate pairing is well-defined. It also satisfies the bilinearity and non-degeneracy properties.

There are some effective algorithms to compute Tate pairing, such as Miller's algorithm (see [44]). Miller's algorithm takes $O(\log r)$ operations. For improvements and further reduction in number of operations, we refer to [6, 7, 25], for example.

A similar pairing, namely Weil pairing is defined which is used in cryptography. One may refer to [44, 67] for more details.

Remark 1.5.10 In all of the proposed schemes (Chapter 3, 4 and 5), one can use any of the bilinear pairings (for example, Tate pairing, Weil pairing, etc.).

1.6 Hash Function

Hash functions (see [48, 67]) are used to compress arbitrary length string to a string of fixed length. This helps to allocate storage for the records of a file as consistently as feasible. Cryptographic hash functions can be used to secure large amounts of data by ensuring the integrity of a short string, the hash value.

We recall the definition of hash function as in [55].

Definition 1.6.1 (Hash function [55]) "Let $k \geq 0$ be a fixed integer. A *hash function* h is a map $h : \ \{0,1\}^* \longrightarrow \{0,1\}^k$, mapping bit strings of arbitrary length to the fixed length k. A hash function h is said to be a *cryptographic hash function* if it is easy to compute $h(M)$ for a given string M, and at least one of the following is satisfied.

- *Preimage resistance (one-wayness)*: For a given hash value m it is computationally hard to find a bit string M such that $h(M) = m$.

- *2nd-preimage resistantance (weak collision resistance)*: For a given bit string M, it is computationally hard to find a bit string $M' \neq M$ such that $h(M') = h(M)$.
- *Collision resistantance (strong collision resistance)*: It is computationally hard to find two distinct bit strings M_1 and M_2 such that $h(M_1) = h(M_2)$".

In practice, cryptographic hash functions satisfy all the above three requirements. MD5, SHA-1, and SHA-256 are practical examples of cryptographic hash functions, with output lengths of k = 128, k = 160, and k = 256, respectively. For more details, we refer to [42].

1.7 Signature Schemes

A signature is used in every situation where we need permission from an authority. A signature specifies that the person is responsible who is signing the message/document. For example, a signature is required to sign a contract, withdraw money from a bank, write a letter, etc. A digital signature scheme is a method of signing an electronic message. The signed message can be sent over a computer network. The fundamental feature of a digital signature scheme is that it provides message authentication, which enables a private key holder to create signatures on any message.

A signature scheme consists of two protocols called signing and verification. The signing protocol is carried out by the author of the message and the signer, and the verifier carries out the verification protocol. In the signing protocol, the author asks for a signature on a message x, and the signer signs the message using a (private) signing algorithm sig_K that depends on a secret key K. In the verification protocol, the verifier can verify the resulting signature $sig_K(x)$ using a public verification algorithm ver_K. Let (x, y) be a message-signature pair. The verification algorithm gives a result of *true* provided y is a legitimate signature, otherwise of *false* .

We recall the definition of a signature scheme as in [60].

Definition 1.7.1 (Signature scheme [60]) "A *signature scheme* is five-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, where the following conditions are satisfied.

1. $\mathcal{P}$ is finite set of possible messages

2. $\mathcal{A}$ is a finite set of possible signatures

3. $\mathcal{K}$, the keyspace, is a finite set of possible keys

4. for each $K \in \mathcal{K}$, there is a signing algorithm $sig_K \in \mathcal{S}$ and a corresponding verification algorithm $ver_K \in \mathcal{V}$. Each $sig_K : \mathcal{P} \longrightarrow \mathcal{A}$ and $ver_K : \mathcal{P} \times \mathcal{A} \longrightarrow \{true, false\}$ are functions such that the following equation is satisfied for every message $x \in \mathcal{P}$ and for every signature $y \in \mathcal{A}$,

$$ver_K(x, y) = \begin{cases} true & \text{if } y = sig_K(x) \\ false & \text{if } y \neq sig_K(x). \end{cases}$$

The *signed message* is a pair (x, y) with $x \in \mathcal{P}$ and $y \in \mathcal{A}$."

In some cases, the author may ask for a signature on a message without reavailing the content of the message to the signer for security purposes. Such signature schemes are called *blind signature schemes*. The application of the blind signature scheme is used in securing electronic payment systems, electronic voting systems, etc.

A signature scheme possesses *unforgeability* property for the basic security requirement. That is, the only practical method for an adversary to get a valid message-signature pair $(x, sig_K(x))$ is to run the signing protocol with the private key K.

Signature schemes are often used along with a secure cryptographic hash function. There are well-known class signature schemes such as the RSA signature scheme, DSA, ElGamal signature scheme, etc. For more details, we refer to [60]. An example of the digital signature scheme using elliptic curves is given below.

Elliptic Curve Digital Signature Algorithm (ECDSA).

Let $P \in E(\mathbb{F}_p)$ be a point of large prime order n such that the ECDLP in $\langle P \rangle$ is hard. Let $\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \mathbb{Z}_n^\times \times \mathbb{Z}_n^\times$, and define $\mathcal{K} = \{(p, n, E, P, a, Q) : Q = aP\}$, where $0 \leq a \leq n-1$. The values p, n, E, P, and Q are public, and a is a private key.

For a random integer k, $1 \leq k \leq n-1$, define

$$sig_K(x, k) = (u, v),$$

as follows:

$$\begin{aligned} kP &= (r, s), \\ u &= r \pmod{n}, \text{ and} \\ v &= k^{-1}(h(x) + au) \pmod{n}, \text{ where } h \text{ is a hash function.} \end{aligned}$$

If either of u or v is 0, then a new value of k should be selected.

For $x \in \{0,1\}^*$ and $u, v \in \mathbb{Z}_n^\times$, the signature can be verified by the following computations:

$$\begin{aligned} &w = v^{-1} \pmod{n}, \\ &i = w \times h(x) \pmod{n}, \\ &j = wu \pmod{n}, \\ &(r, s) = iP + jQ, \\ &ver_K(x, (u, v)) = true \Longleftrightarrow r \pmod{n} = u. \end{aligned}$$

1.8 Time Complexity of Algorithms

The time complexity of an algorithm indicates how long it takes to run in a computer and how efficient it is. An algorithm is a procedure that produces certain output on a given input in a specific amount of time. The number of steps required for an algorithm to complete can be considered a time measure. We use the following notation (see [36]) to measure the time complexity.

Definition 1.8.1 (Big-O notation) "Let $f, g : \mathbb{N} \longrightarrow \mathbb{R}^+$ be two functions. Suppose that $g(x)$ is the running time of an algorithm on an input size x. Then we say that $g(x) = O(f(x))$ if $\exists$ some $c \in \mathbb{R}^+$ such that $g(x) \leq c \cdot f(x)$ for every sufficiently large x".

Example 1.8.2 If $g(x) = 7(\log x)^3 + 8x^2 + 15x^3$, then $g(x) = O(x^3)$.

Now we discuss the computational complexity of some well-known algorithms we use in the later chapters.

Let $P \in E(\mathbb{F}_q)$ be a point. We can compute aP in $O(\log a)$ steps using the *Double-and-Add* method ([18]). First we write

$$a = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_r \cdot 2^r$$

with $a_i \in \{0,1\}$ for $i = 0, 1, 2, \cdots, r$. Then aP can be computed as

$$aP = a_0 + a_1 \cdot 2P + a_2 \cdot 2^2 P + \cdots + a_r \cdot 2^r P$$

where $2^k P = 2 \cdot 2 \cdots 2P$ requires only k doublings. Thus, on average, it takes approximately $\log_2 a$ doublings and $\frac{1}{2}\log_2 a$ additions to compute aP.

Algorithm 1 [18]

Input P
$Q \longleftarrow P$
for i from 1 to r do
    $Q \longleftarrow 2Q$
    if $a_i = 1$ then $Q \longleftarrow Q + P$
Output Q.

The computational cost of point addition and doubling on elliptic curve are **I**+2**M**+**S** and **I**+2**M**+2**S** respectively where **I**, **M**, **S** stand for inverse, multiplication and squaring (see [1]). There are many bilinear pairings that cost logarithmic time (see [34, 44]). The time complexity of matrix multiplication of order $n \times t$ and $t \times 1$ is $O(nt)$ and the inverse of a matrix of order n is $O(n^3)$. This can be seen using basic formulas.

Remark 1.8.3 For the security analysis of our schemes, we need the following basic result (see [49, Theorem 5.3.6]) from linear algebra. For the completeness, we provide its proof.

Proposition 1.8.4 ([49]) *A system of m linear equations over a finite field of order q with n unknowns has either a unique solution, no solution, or q^k solutions for some k with $1 \leq k \leq n$. Each solution is of equal probability for the case of q^k solutions.*

Proof. Consider a system of m equations over $\mathbb{F}_q$

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= c_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= c_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= c_m. \end{aligned}$$

Let the coefficient matrix be A and the augmented matrix be A', where

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \text{ and } A' = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & c_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & c_m. \end{array}\right).$$

We know that the system has a solution if and only if $\text{rank}(A)$ is same as $\text{rank}(A')$. We assume this is the case. After performing elementary row operations, the matrix A' is equivalent to the matrix

$$\left(\begin{array}{ccccccccccccccc|c} 0 & \cdots & 0 & 1 & b_{1(i_1+1)} & \cdots & b_{1(i_2-1)} & 0 & b_{1(i_2+1)} & \cdots & b_{1(i_\ell-1)} & 0 & b_{1(i_\ell+1)} & \cdots & b_{1n} & d_1 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & b_{2(i_2+1)} & \cdots & b_{2(i_\ell-1)} & 0 & b_{2(i_\ell+1)} & \cdots & b_{2n} & d_2 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & b_{\ell(i_\ell+1)} & \cdots & b_{\ell n} & d_\ell \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \end{array}\right)$$

where $1 \leq i_1 < i_2 < \cdots < i_\ell \leq n$ are the column indices and 1's are the pivot element. Thus, $k = n - \ell$ is the number of free variables, and hence the dimension of the solution space is also $k = n - \ell$. For any choice of values of free variables $x_1, \cdots, x_{i_1-1}, x_{i_1+1}, \cdots, x_{i_2-1}, x_{i_2+1}, \cdots, x_{i_\ell-1}, x_{i_\ell+1}, \cdots, x_n$ from $\mathbb{F}_q$, we get a unique solution. Thus, the number of solutions is q^k.

Moreover, as a free variable can assume any of q values (with probability $1/q$), the probability of each solution is $1/q^k$.

Chapter 2

A Blind Signature Scheme

In this chapter, we present our work [17] on a blind signature scheme. This work has been published in the "Proceedings of the Seventh International Conference on Mathematics and Computing, Advances in Intelligent Systems and Computing, vol. 1412, Springer, (2022)".

The blind signature scheme has been the most significant responsibility from the beginning of the era of electronic money (e-money). It is an interdependent agreement that includes two parties, a Bank and a Client. The scheme permits a client to urge a signature on a message from the Bank without disclosing the context of the message. The message-signature pair received by the client is factually uncorrelated to the view acquired by the Bank during the execution of the agreement. D. Chaum [11] in 1983 first proposed the blind signature scheme. Later, many blind digital signature schemes were proposed (see [10, 46, 50, 45, 72]). The main applications of the blind signature scheme are in securing electronic payment systems, electronic voting systems etc.

A blind digital signature scheme should satisfy the following properties:
Blindness: It permits a user to urge a signature on a given message, whereas not revealing the context of the message to the signer.
Untraceability: When the user has disclosed the signature to the general public, the signer cannot trace the signature-message pair.
Unforgeability: Solely, the signer will generate a legitimate signature. For an attacker, executing the signature protocol with the signers private key is the only practical method to obtain a valid message and signature pair. This property is foremost very important and should satisfy all signature schemes.
Unlinkability: Nobody can obtain a link between a legitimate blind signature and

a protocol view except the author of the message.
For detailed security aspects of the blind signature scheme, we refer to [30]. A verifier can verify the blind signature publicly and meet the necessities of security-oriented agreements that have an imbalance between the author of the message and the signer.

In 2014, K. Chakraborty and J. Mehta [10] proposed a stamped blind signature scheme based on ECDLP (see Definition 1.4.1). Later, M. Tian, Y. Zhu and Z. Chen [65] observed that Chakraborty-Mehta's blind signature scheme is insecure by giving two simple but powerful attacks. In [17], we considered an analogue version of Chakraborty-Mehta's scheme, which uses self-pairing (see [17]). The scheme gives more security and avoids the attacks given by Tian, Zhu and Chen [65].

The self-pairing was first proposed by H.-S. Lee [38] in 2004. We note that Lee's self-pairing is anti-symmetric. Several secret sharing schemes were introduced based on self-pairing (see [40, 8]). A slightly modified Lee's pairing is defined in the next section which is used in this chapter.

2.1 Self-Pairings

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with characteristics not equal to 2 and 3. Let r be a prime divisor of $\#E(\mathbb{F}_q)$ and $r \neq p$. Recall that $E[r] \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$. Let S, T be a fixed generating pair of points for the r-torsion group $E[r]$. Consider two points $P = a_1S + b_1T$ and $Q = a_2S + b_2T$ in $E[r]$, where $a_1, a_2, b_1, b_2 \in [0, r-1]$. For some fixed $\alpha, \beta \in [0, r-1]$, we define self-pairing map

$$\mathrm{e}_{\alpha,\beta} : E[r] \times E[r] \longrightarrow E[r]$$

as $\mathrm{e}_{\alpha,\beta}(P, Q) = (a_1a_2 - b_1b_2)(\alpha S + \beta T)$. The trivial case ($\alpha = 0 = \beta$) has been excluded.

The following theorem lists some of the properties satisfied by self-pairing map $\mathrm{e}_{\alpha,\beta}$.

Theorem 2.1.1 *For all P, Q, $R \in E[r]$ and the point at infinity $\mathcal{O}$,*

1. *Bilinearity:* $\mathrm{e}_{\alpha,\beta}(P + Q, R) = \mathrm{e}_{\alpha,\beta}(P, R) + \mathrm{e}_{\alpha,\beta}(Q, R)$ *and* $\mathrm{e}_{\alpha,\beta}(P, Q + R) = \mathrm{e}_{\alpha,\beta}(P, Q) + \mathrm{e}_{\alpha,\beta}(P, R)$.

2. *Non-degeneracy: If* $\mathrm{e}_{\alpha,\beta}(P,Q) = \mathcal{O}$ *for all* $Q \in E[r]$*, then* $P = \mathcal{O}$.

3. *Symmetry:* $\mathrm{e}_{\alpha,\beta}(P,Q) = \mathrm{e}_{\alpha,\beta}(Q,P)$ *for all* $P,\ Q \in E[r]$.

The proof of the theorem is very similar to [38, Proposition 3.1]. For completeness, we provide the proof below.

1. For all $P, Q, R \in E[r]$ with $R = a_3S + b_3T$, we have

$$\begin{aligned}\mathrm{e}_{\alpha,\beta}(P+Q,R) &= \mathrm{e}_{\alpha,\beta}((a_1+a_2)S + (b_1+b_2)T, a_3S + b_3T)\\ &= ((a_1+a_2)a_3 - (b_1+b_2)b_3)(\alpha S + \beta T)\\ &= (a_1a_3 - b_1b_3)(\alpha S + \beta T) + (a_2a_3 - b_2b_3)(\alpha S + \beta T)\\ &= \mathrm{e}_{\alpha,\beta}(P,R) + \mathrm{e}_{\alpha,\beta}(Q,R).\end{aligned}$$

   Similarly $\mathrm{e}_{\alpha,\beta}(P,Q+R) = \mathrm{e}_{\alpha,\beta}(P,Q) + \mathrm{e}_{\alpha,\beta}(P,R)$.

2. For any $Q = a_2S + b_2T \in E[r]$, we have

$$\mathrm{e}_{\alpha,\beta}(P,Q) = (a_1a_2 - b_1b_2)(\alpha S + \beta T) = \mathcal{O}.$$

   Thus, $a_1a_2 - b_1b_2 = 0$. By choosing Q with $a_2 \neq 0$ and $b_2 = 0$, we obtain $a_1 = 0$. Similarly, by choosing Q with $a_2 = 0$ and $b_2 \neq 0$, we obtain $b_1 = 0$. Hence $P = a_1S + b_1T = \mathcal{O}$.

3. For all $P, Q \in E[r]$, $\mathrm{e}_{\alpha,\beta}(P,Q) = (a_1a_2 - b_1b_2)(\alpha S + \beta T) = \mathrm{e}_{\alpha,\beta}(Q,P)$.

The self-pairing map also satisfies the following additional properties:
For all $P,\ Q \in E[r]$, we have

1. $\mathrm{e}_{\alpha,\beta}(P,P) = \mathcal{O}$, if $a_1 = b_1$.

2. $\mathrm{e}_{\alpha,\beta}(P,\mathcal{O}) = \mathrm{e}_{\alpha,\beta}(\mathcal{O},Q) = \mathcal{O}$.

3. $\mathrm{e}_{\alpha,\beta}(aP,bQ) = ab \cdot \mathrm{e}_{\alpha,\beta}(P,Q)$ for all $a, b \in \mathbb{Z}$.

For an illustration, we consider the elliptic curve E, 3-torsion points $E[3]$, S and T as in Example 1.5.8. Choose $a_1 = 2$, $b_1 = 2$, $a_2 = 2$, $b_2 = 1$ in $\mathbb{Z}_3$ and fix $\alpha = 1$, $\beta = 2$ in $\mathbb{Z}_3$. Then $\mathrm{e}_{\alpha,\beta}(P,Q) = \mathrm{e}_{1,2}(2S + 2T, 2S + T) = (2 \times 2 - 2 \times 1)(1S + 2T) = 2(1S + 2T) = 2S + T = (1 + \gamma, 2 + 2\gamma)$.

We will give an overview of the Chakraborty-Mehta's [10] blind signature scheme and the attacks on it as given by M. Tian, Y. Zhu and Z. Chen [65], which proved that the scheme is insecure.

2.2 Overview of Chakraborty-Mehta's Blind Signature Scheme

Let $P \in E(\mathbb{F}_q)$ be a point of large prime order r. Let $G = \langle P \rangle$ such that ECDLP is hard to solve. The scheme uses a collision-resistant hash function $h : \{0,1\}^* \longrightarrow \mathbb{Z}_r^\times$ (see Section 1.6).

The scheme involves an Author (**A**) of the message, a Signer (**S**), and a Verifier (**V**). The signer chooses a secret key $x \in \mathbb{Z}_r^\times$ and computes $Q = xP \in G$. The signer makes Q public.

Signing protocol

The signing protocol involves a blinding algorithm which is executed by **A** and a signing algorithm which is carried out by **S**.

Blinding algorithm:

- **A** computes $h(M) = m$, where M is the message.
- Then **A** calculates $K = mQ = mxP$ and sends it to the signer.

Signing algorithm:

- **S** receives $K = mQ$ and computes $K' = x^{-1}K = mP$.
- Then **S** generates a signature parameter z, called as stamp, and computes $h(z)$.
- Again, **S** computes a point $R = K' + h(z)P$ and $s = x - h(z)$.
- Then **S** sends the generated signature (R, s, z) to the verifier for verification.

Verification protocol

The verifier **V** verifies the signature by checking the correctness of the equation

$$sP - Q + R = h(M)P.$$

If the above equation holds true, only then the signature is valid. This can be observed as follows.

$$\begin{aligned} sP - Q + R &= (x - h(z))P - xP + K' + h(z)P \\ &= xP - h(z)P - xP + mP + h(z)P \\ &= h(M)P. \end{aligned}$$

Now we discuss two attacks on the Chakraborty-Mehta's scheme, which is given by M. Tian, Y. Zhu and Z. Chen [65].

Attack 1. Suppose an attacker **X** wants to get the signer's secret key x, then he perform the following steps.

- **X** queries a blind signature on message M. Then the signer will compute and produce a signature (R, s, z).
- **X** calculates $h(z)$ upon receiving of the signature (R, s, z).
- Finally, **X** gets the signer's secret key $x = s + h(z)$.

We know that $s = x - h(z)$ by signing algorithm. Observe that **X** can find the signer's secret key x by the above process. So **X** having a signer's secret key x will be able to generate valid signatures on any messages.

Attack 2. Suppose an attacker **X** wants to get valid signature on a message M, then he perform the following steps.

- **X** initially produces a stamp z' of the signature.
- Then **X** computes $h(z')$ and $h(M)$.
- **X** chooses an integer $s' \in \mathbb{Z}_r^{\times}$ randomly.
- Finally, **X** computes a point $R' = h(M)P + Q - s'P$, where $Q = xP$ is the signer's public key.

The forged signature on M is (R', s', z'). We can see that

$$s'P - Q + R' = s'P - Q + h(M)P + Q - s'P = h(M)P.$$

As a result, the signature (R', s', z') will pass the verifier's scrutiny. That is, the forged signature (R', s', z') of $\mathbf{X}$ is valid.

To avoid these attacks and to make the scheme more secure, an analogue/modified version of the above scheme is proposed in [17], which is discussed in the next section.

2.3 A Blind Signature Scheme

The scheme involves three parties, namely Author ($\mathbf{A}$), Signer ($\mathbf{S}$), and Verifier ($\mathbf{V}$). The scheme consists of two protocols called *signing protocol* and *verification protocol*. The signing protocol is carried out by both $\mathbf{A}$ and $\mathbf{S}$ while the verification protocol is checked out by $\mathbf{V}$. $\mathbf{A}$ wants to obtain a signature on a message from the signer without revealing the context of the message. This includes blinding the message with the goal that the $\mathbf{S}$ can't read the message. Simultaneously $\mathbf{A}$ needs to ensure that $\mathbf{S}$ is the assigned beneficiary of the blinded message. This can be accomplished by twofold blinding the message (i.e., putting two locks on the message). One lock is put by $\mathbf{S}$, and he is the one in particular who can open it, which guarantees that he is the main individual who is accepting blinded messages from $\mathbf{A}$. Another lock is put by $\mathbf{A}$ to ensure that $\mathbf{S}$ cannot read the actual message.

Setting up domain parameters

Firstly, the signer sets up the domain parameters for the scheme.

- $\mathbf{S}$ chooses an elliptic curve E over $\mathbb{F}_q$, where $q = p^{i_0}$, $i_0 \in \mathbb{N}$, and p is a large prime.
- $\mathbf{S}$ chooses a random generating pair (S, T) in $E[r]$, where r is a large prime divisor of $\#E(\mathbb{F}_q)$ so that ECDLP in $E(\mathbb{F}_q)$ is hard, and some fixed α, $\beta \in \mathbb{Z}_r$ for which the pairing $\mathrm{e}_{\alpha,\beta}$ can be determined.
- Finally, $\mathbf{S}$ makes $\{E, q, r, \alpha, \beta, S, T, \alpha S + \beta T\}$ as public.

It additionally utilizes a cryptographic hash function (see Section 1.6) $h : \{0,1\}^* \longrightarrow \mathbb{Z}_r^\times$ which is collision-resistant.

Signing Protocol

- **S** chooses two secret keys a, $b \in \mathbb{Z}_r$ such that $\gcd(a, b)$=1 and makes $P = aS + bT \in E[r]$ public.

- **A** computes $h(M) = m$ where M is the actual message and m is the hash value.

- Then **A** computes $G = mP = maS + mbT$ and sends G to the signer for signing.

- **S** selects a point $H = cS + dT \in E[r]$ such that $ac - bd = 1$.

Remark 2.3.1 The author wants to send $m(\alpha S + \beta T)$ for signing to the signer. The value $m(\alpha S + \beta T)$ can be computed from G by only the signer, the person who can find c, $d \in \mathbb{Z}_r$ such that $ac - bd = 1$.

Signing Algorithm

1. The signer **S** receives G and calculates $A = \mathrm{e}_{\alpha,\beta}(G, H) = m(ac - bd)(\alpha S + \beta T) = m(\alpha S + \beta T)$, where $H = cS + dT$.

2. **S** generates signature parameter z (say stamp), and calculates $h(z)$.

3. **S** selects a random integer $x \in [1, r - 1]$ such that $h(z)x \neq 1$.

4. **S** calculates a point B on elliptic curve as follows
   $B = m(\alpha S + \beta T) + \mathrm{e}_{\alpha,\beta}(xS + T, h(z)S + T)$ and set $J = h(z)xH$.

5. **S** sends the generated signature parameters (B, J, z) to the verifier for verification.

Verification Protocol

The verifier **V** computes $B - \mathrm{e}_{\alpha,\beta}(J, P) + (\alpha S + \beta T)$ and observes the validity of the following equation

$$B - \mathrm{e}_{\alpha,\beta}(J, P) + (\alpha S + \beta T) = A.$$

The verifier **V** accepts the signature if the above equation holds true. The correctness of the signature is verified as

$$\begin{aligned} B - \mathrm{e}_{\alpha,\beta}(J,P) + (\alpha S + \beta T) &= m(\alpha S + \beta T) + (h(z)x - 1)(\alpha S + \beta T) \\ &\quad -h(z)x(ac - bd)(\alpha S + \beta T) + (\alpha S + \beta T) \\ &= m(\alpha S + \beta T) = A. \end{aligned}$$

2.4 Security Aspects of the Scheme

In this section, we analyze the security aspects of the blindness and non-forgeability of the scheme.

Blindness from Signer's point of view: The author **A** sends $G = mP = maS + mbT$ to the signer **S**. Then **S** can compute $m(\alpha S + \beta T)$ from G using his secret keys $a,\ b$ and finding $c,\ d$ such that $ac - bd = 1$. It is hard to find m from $G = mP$ as it is equivalent to solving ECDLP for large prime r. Hence **S** can not see the message.

Blindness from Adversary's point of view: An adversary can able to find P and mP. Finding m from mP is an instance of solving ECDLP. If the adversary performs a total break of the system, then he can find a, b, and $A = m(\alpha S + \beta T)$, but finding m from A is again an instance of solving ECDLP. Hence the message is blinded to the adversary.

We need the following basic result for discussion on unforgeability condition.

Proposition 2.4.1 *The probability of getting two integers a and b such that $gcd(a,b) = 1$ is $\prod_{p,\ p\ prime} (1 - 1/p^2) = 1/\zeta(2)$ where ζ denotes the Riemann zeta function.*

Proof. We recall the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ for $s > 1$. The function $\zeta(s)$ can be written as an infinite product over primes (due to Euler) and is given as $\zeta(s) = \prod_p (1 - 1/p^s)^{-1}$, where p is prime.

Now let a and b be two positive integers. Suppose that $\gcd(a,b) = 1$. Then we must not have a prime p which divides both a and b. So if we take particular prime p, then the probability that a is divisible by p is $1/p$, and for b, also $1/p$. Then, $1/p^2$ is the probability of p dividing both a and b simultaneously. Therefore, the

probability that p does not divide both a and b is $1-1/p^2$. Thus, the probability that no prime divides both a and b is given by $\prod_p(1-1/p^2) = 1/\zeta(2)$.

Non-Forgeability of the signer's secret keys: The probability of guessing signer's keys a and b from P is negligible. So for an adversary, it is practically infeasible to guess a random signature.

1. The probability of getting two integers a and b such that $\gcd(a,b) = 1$ is $\prod_{p \le n,\ p\ prime}(1-1/p^2) \approx 1/\zeta(2)$ where ζ denotes the Riemann zeta function.
2. The probability of getting x such that $h(z)x \neq 1$ is $1/(r-1)$.

We have the following observations.

Theorem 2.4.2 *Let (B_1, J_1) be the signature corresponding to the message m_1 and stamp z_1. To find a random message $m_2(\neq m_1)$ for an adversary that satisfies (B_1, J_1) for a chosen stamp $z_2(\neq z_1)$ is difficult.*

Proof. Suppose the adversary chooses a stamp z_2 and wants to find a message m_2 which satisfies the signature (B_1, J_1). The equation $m_1(\alpha S+\beta T)+\mathrm{e}_{\alpha,\beta}(xS+T, h(z_1)S+T) = m_2(\alpha S+\beta T)+\mathrm{e}_{\alpha,\beta}(xS+T, h(z_2)S+T)$ implies that $m_1(\alpha S+\beta T)+(h(z_1)x-1)(\alpha S+\beta T) = m_2(\alpha S+\beta T)+(h(z_2)x-1)(\alpha S+\beta T)$ and the equation $h(z_1)xH = h(z_2)xH$ implies that $h(z_1)x(cS+dT) = h(z_2)x(cS+dT)$ which gives $h(z_1) = h(z_2)$. Then $m_1(\alpha S+\beta T) = m_2(\alpha S+\beta T)$. Since the hash function h is collision-resistant, $h(z_1) = h(z_2)$ is not possible. In addition, $m_1(\alpha S+\beta T) = m_2(\alpha S+\beta T)$, hence $m_1 = m_2 \pmod r$.

Theorem 2.4.3 *Let (B_1, J_1) be the signature corresponding to the message m_1 and stamp z_1. To find a random stamp $z_2(\neq z_1)$ for an adversary that satisfies (B_1, J_1) for a chosen message $m_2(\neq m_1)$ is difficult.*

Proof. Suppose the adversary chooses a message m_2 and wants to find a stamp z_2 which satisfies the signature (B_1, j_1). Then the equation $m_1(\alpha S+\beta T)+\mathrm{e}_{\alpha,\beta}(xS+T, h(z_1)S+T) = m_2(\alpha S+\beta T)+\mathrm{e}_{\alpha,\beta}(xS+T, h(z_2)S+T)$ implies that $m_1(\alpha S+\beta T)+(h(z_1)x-1)(\alpha S+\beta T) = m_2(\alpha S+\beta T)+(h(z_2)x-1)(\alpha S+\beta T)$ and the equation $h(z_1)xH = h(z_2)xH$ implies that $h(z_1)x(cS+dT) = h(z_2)x(cS+dT)$. Second equation gives $h(z_1) = h(z_2)$. Since the hash function h is collision-resistant, $h(z_1) = h(z_2)$ is not possible.

We will discuss the following two attacks, which fail for our scheme.

Attack 1. Suppose that an attacker **X** wants to get the signer's secret keys a and b, then he performs the following:

X queries a blind signature on message M. Then the signer can cipher and output a signature (B, J, z) as a response. After receiving the signature (B, J, z), **X** will try to find c and d from J. But finding c and d from J is equivalent to solving an ECDLP. Without the knowledge of c and d, **X** cannot get a and b. Hence it is impractical to find the signer's secret keys.

Attack 2. Suppose an attacker **X** wants to generate a valid signature for a message M_1, then can perform the following steps:

1. **X** generate a stamp z_1.
2. **X** computes $h(z_1)$ and $m_1 = h(M_1)$.
3. **X** chooses a integer $x_1 \in [1, r-1]$ such that $h(z_1)x_1 \neq 1$.
4. Then **X** computes $B_1 = m_1(\alpha S + \beta T) + \mathrm{e}_{\alpha,\beta}(x_1 S + T, h(z_1)S + T)$.

Now **X** cannot set $J_1 = h(z_1)x_1 H$ as H is unknown to **X**. Suppose **X** selects a random $J_2 = (h(z_1)x_1 - 1)(c_1 S + d_1 T)$ and send (B_1, J_2, z) to verifier for verification. Then verifier computes

$$\begin{aligned} B_1 - \mathrm{e}_{\alpha,\beta}(J_2, P) + (\alpha S + \beta T) &= m_1(\alpha S + \beta T) + (h(z_1)x_1 - 1)(\alpha S + \beta T) \\ &\quad -h(z_1)x_1(ac_1 - bd_1)(\alpha S + \beta T) + (\alpha S + \beta T) \\ &= m_1(\alpha S + \beta T), \end{aligned}$$

provided that $(ac_1 - bd_1) = 1$, which is impractical. Hence this is resistant to the attack.

Chapter 3

Compartmented Multi-Secret Sharing Scheme

This chapter contains our work [14] on a multi-secret sharing scheme (compartmented). This work has been accepted for publication in the Journal of Information and Optimization Sciences.

In a multi-secret sharing scheme, many secrets are distributed to the users in such a way that only authorized subsets of users can recover 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 [40]. Accordingly, we have presented a threshold multi-secret sharing scheme. It uses a matrix whose any threshold number of rows forms a Vandermonde matrix [51]. For the scheme in [40], 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.

In 1990, G. Simmons [59] introduced a compartmented secret sharing scheme. In a compartmented secret sharing scheme, users are partitioned into disjoint compartments. If the number of the collaborating participants exceeds a global threshold and the collaborating participants from every compartment exceeds a predetermined compartment threshold, the secret can be recovered. Many compartmented schemes have been proposed using polynomials [29, 54, 69] and Chinese Remainder Theorem [33], and many others [13, 12, 22, 62, 64, 68]. The method is advantageous in synchronizing the information provided to multiple groups from a single server.

In this chapter, we have focused on a multi-secret sharing scheme and a com-

partmented multi-secret sharing scheme based on elliptic curves [58], bilinear pairings [35, 41], and matrices [51]. 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. Our 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 [64]. We have also observed that a secret sharing in compartmented groups proposed by Ghodosi, Pieprzyk and Safavi-Naini [29] does not work properly (the case $t > \sum t_i$). See Remark 3.2.1 for more details.

3.1 Multi-Secret Sharing Scheme

Let $q = p^{i_0}$ with $i_0 \in \mathbb{N}$ and p be a large prime. Consider $P \in E(\mathbb{F}_q)$ and $G_a = \langle P \rangle$ be a subgroup of order r where r is a large prime so that ECDLP is hard to solve. Consider a pairing e as in Definition 1.5.1. Suppose that there are n users, say, $u_1, u_2, \cdots, u_n$, and a trusted Dealer. 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 chooses a matrix of order $n \times t$

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

- Dealer chooses t random integers $a_1, a_2, \cdots, a_t \in [0, r-1]$ 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. Dealer makes matrix B public.

- Each u_i selects a private key $x_i \in [1, r-1]$ and makes x_iP public.
- Then Dealer computes b_ix_iP and sends (publicly) to u_i for $i = 1, 2, \cdots, n$.
- Each u_i will get the share b_iP by computing $x_i^{-1}(b_ix_iP)$.
- Dealer computes $s_\lambda = \mathrm{e}(P, \lambda \cdot a_tP) + K_\lambda$, $1 \leq \lambda \leq g$, and makes them public.
- Also, each u_i computes $z_i = \mathrm{e}(P, b_iP)$.

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

Remark 3.1.1 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 [41]), for any $P, Q \in E[r]$, we have $\mathrm{e}(P, Q) \in \mu_r \subseteq \mathbb{F}_{q^k}^* \subseteq \mathbb{F}_{q^k}$. 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.

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

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 the Vandermonde matrix and the shares matrix gives the value a_tP (for more details, we refer to [51]). 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 [56], for example) use 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 the 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.

3.1.1 Security analysis of the multi-secret sharing scheme

Bilinear pairing behaves like a one-way map, 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. 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 3.1.2 *For an attacker, the probability of choosing a random point*

$a'_tP \in G_a$ such that $K_\lambda = s_\lambda - \mathrm{e}(P, a'_tP)$ for $1 \le \lambda \le g$ is $1/(r-1)$.

Proof. We note that $K_\lambda = s_\lambda - \mathrm{e}(P, a'_tP)$ if and only if $\mathrm{e}(P, a'_tP) = \mathrm{e}(P, \lambda \cdot a_tP)$, which is true if and only if $a'_tP = \lambda a_tP$. Thus, the probability of choosing $a'_tP \in G_a$ with $s_\lambda - \mathrm{e}(P, a'_tP) = K_\lambda$ is $1/(r-1)$ as $a'_tP \neq \mathcal{O}$.

Theorem 3.1.3 *The honesty of at least $n - t + 1$ number of users ensures that any $t - 1$ (or less) number of 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) number of 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_tP. Then a_tP can be any element of G_a and without a_tP they cannot compute $K_\lambda = s_\lambda - \mathrm{e}(P, a_tP)^\lambda$.

Theorem 3.1.4 *There is no loss of information about the secrets 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 $x'_iP \in G_a$ satisfying $\mathrm{e}(x'_iP, b_ix_iP) = \mathrm{e}(P, b_iP)$ must satisfy $x'_i \equiv x_i^{-1} \pmod r$. For

$$\begin{aligned} \mathrm{e}(x'_iP, x_ib_iP) = \mathrm{e}(P, b_iP) &\iff \mathrm{e}(P, b_iP)^{x'_ix_i} = \mathrm{e}(P, b_iP) \\ &\iff x'_ix_i \equiv 1 \pmod r \\ &\iff x'_i \equiv x_i^{-1} \pmod r. \end{aligned}$$

3.1.2 Complexity of the 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"* [18], the time for computing scalar multiplication of a point on an elliptic curve is $O(\log_2 \mathrm{r})$, where

r is the order of the point. The number of scalar multiplications rquired for generating shares and reconstruction of the secret is n and t, respectively. For computing $t+g$ pairings, it takes $O((t+g)\log_2 r)$ (see [34, 44], for example). Additionally, the scheme requires $(t-1)\mathbf{M}+1\mathbf{S}$ operations, where $\mathbf{M}$ and $\mathbf{S}$ denote multiplication and subtraction respectively. For computing y_i, $1 \leq i \leq t$, it takes $t((t-1)\mathbf{M}+1\mathbf{S})$ operations. Hence the required time complexity for the scheme is $O(n^2)$.

An example of our multi-secret sharing scheme using modified Tate pairing [41] is given below. The computations are done using SageMath.

Example 3.1.5 Consider $E: y^2 = x^3+5x+13$ 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 $r = 13$, $p = q = 29$ 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 Dealer chooses 4 integers $5, 2, 8, 10 \in [0, 12]$ and computes

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

Let Dealer 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 any irreducible polynomial of degree 3 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 [41]. The Dealer makes P, s_1, s_2 and s_3 public. Each 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_iP 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_ix_iP and sends (publicly) to u_i, $i = 1, 2, \cdots, 6$, where

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

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

$$\begin{aligned}
b_1P = x_1^{-1}(b_1x_1)P &= 9(b_1x_1)P = (5\gamma^2 + 2\gamma + 7, 15\gamma^2 + 25),\\
b_2P = x_2^{-1}(b_2x_2)P &= 3(b_2x_2)P = (7\gamma^2 + 14\gamma + 25, 4\gamma^2 + 28),\\
b_3P = x_3^{-1}(b_3x_3)P &= 7(b_3x_3)P = (17\gamma^2 + 16\gamma + 17, 14\gamma^2 + 22\gamma + 10),\\
b_4P = x_4^{-1}(b_4x_4)P &= 6(b_4x_4)P = (5\gamma^2 + 2\gamma + 7, 14\gamma^2 + 4),\\
b_5P = x_5^{-1}(b_5x_5)P &= 8(b_5x_5)P = (7\gamma^2 + 14\gamma + 25, 25\gamma^2 + 1) \text{ and}\\
b_6P = x_6^{-1}(b_6x_6)P &= 11(b_6x_6)P = (21\gamma^2 + 28\gamma + 9, 21\gamma^2 + 5\gamma + 6).
\end{aligned}$$

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

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

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

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

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

3.2 Compartmented Multi-Secret Sharing Scheme

Let $q = p^{i_0}$ with $i_0 \in \mathbb{N}$ and p be a large prime. Consider $P \in E(\mathbb{F}_q)$ and $G_a = \langle P \rangle$ be a subgroup of order r where r is a large prime so that ECDLP is hard to solve. Consider the pairing e as defined above (Definition 1.5.1). Suppose that the scheme involves a set U of n number of users divided into m disjoint compartments $C_1, C_2, \cdots, C_m$ and a trusted Dealer. Let $|C_i| = n_i$ and t_i be the threshold for C_i, $i = 1, 2, \cdots, m$. Dealer chooses t_i random integers $a_{i1}, a_{i2}, \cdots, a_{it_i} \in [0, r-1]$, with $a_{it_i} \neq 0$, for each compartment C_i, $1 \leq i \leq m$. Dealer chooses g secret keys $K_1, K_2, \cdots, K_g \in [0, p-1]$ and computes $s_\lambda = \prod_{i=1}^{m} \mathrm{e}(P, \lambda \cdot a_{it_i} P) + K_\lambda$ $\Big($or, equivalently $s_\lambda = \mathrm{e}\Big(P, \sum_{i=1}^{m} \lambda \cdot a_{it_i} P\Big) + K_\lambda\Big)$, $1 \leq \lambda \leq g$. 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 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 $k_{ij} \in [1, r-1]$ and $k_{ij} \neq k_{ij'}$ for $j \neq j'$.

- Dealer 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 u_{ij}, $1 \leq j \leq n_i$, in the compartment C_i, $1 \leq i \leq m$, chooses a secret key $x_{ij} \in [1, r-1]$ randomly and makes $x_{ij}P$ public.

- Then Dealer computes $b_{ij}x_{ij}P$ for each u_{ij} in C_i and sends (publicly) to the respective users in C_i for $1 \leq i \leq m$.

- Each u_{ij} in C_i will get the share $b_{ij}P$ by computing $x_{ij}^{-1}(b_{ij}x_{ij})P$, $1 \leq j \leq n_i$.

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

We have the following access structure

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

Let $t_0 = t - \sum_{i=1}^{m} t_i$. Consider the matrix A_i for compartment C_i, $1 \leq i \leq m$, 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 $\omega_1, \omega_2, \cdots, \omega_{t_0} \in [0, r-1]$. 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, $1 \le i \le m$, as in the Case I.

Reconstruction of the secrets.

Case I. Suppose t_i number of 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 number of users in C_i can compute $r_i = \mathrm{e}(P, a_{it_i}P)$ as in previous multi-secret sharing scheme (Section 3.1). Then they compute the secret $K_\lambda = s_\lambda - \prod_{i=1}^{m} r_i^\lambda$, $1 \le \lambda \le g$.

Case II. Suppose that t (or more) number of 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, assume 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.

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

In matrix form, we have

$$
\begin{pmatrix}
1 & k_{11} & \cdots & k_{11}^{t_1-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & k_{11}^{t_1} & \cdots & k_{11}^{t_1+t_0-1} \\
1 & k_{12} & \cdots & k_{12}^{t_1-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & k_{12}^{t_1} & \cdots & k_{12}^{t_1+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
1 & k_{1\alpha_1} & \cdots & k_{1\alpha_1}^{t_1-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & k_{1\alpha_1}^{t_1} & \cdots & k_{1\alpha_1}^{t_1+t_0-1} \\
0 & 0 & \cdots & 0 & 1 & k_{21} & \cdots & k_{21}^{t_2-1} & \cdots & 0 & 0 & \cdots & 0 & k_{21}^{t_2} & \cdots & k_{21}^{t_2+t_0-1} \\
0 & 0 & \cdots & 0 & 1 & k_{22} & \cdots & k_{22}^{t_2-1} & \cdots & 0 & 0 & \cdots & 0 & k_{22}^{t_2} & \cdots & k_{22}^{t_2+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 1 & k_{2\alpha_2} & \cdots & k_{2\alpha_2}^{t_2-1} & \cdots & 0 & 0 & \cdots & 0 & k_{2\alpha_2}^{t_2} & \cdots & k_{2\alpha_2}^{t_2+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & k_{m1} & \cdots & k_{m1}^{t_m-1} & k_{m1}^{t_m} & \cdots & k_{m1}^{t_m+t_0-1} \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & k_{m2} & \cdots & k_{m2}^{t_m-1} & k_{m2}^{t_m} & \cdots & k_{m2}^{t_m+t_0-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & 1 & k_{m\alpha_m} & \cdots & k_{m\alpha_m}^{t_m-1} & k_{m\alpha_m}^{t_m} & \cdots & k_{m\alpha_m}^{t_m+t_0-1}
\end{pmatrix}
$$

$$
\times \left(a_{11}P \cdots a_{1t_1}P\ a_{21}P \cdots a_{2t_2}P \cdots a_{m1}P \cdots a_{mt_m}P\ \omega_1 P \cdots \omega_{t_0}P\right)^T
$$

$$
= \left(b_{11}P\ b_{12}P \cdots b_{1\alpha_1}P\ b_{21}P\ b_{22}P \cdots b_{2\alpha_2}P \cdots b_{m1}P\ b_{m2}P \cdots b_{m\alpha_m}P\right)^T.
$$

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 $K_\lambda = s_\lambda - \mathrm{e}\left(P, \sum_{i=1}^{m} a_{it_i}P\right)^\lambda$, $1 \le \lambda \le g$.

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

Remark 3.2.1 We note that the scheme proposed by Ghodosi, Pieprzyk and Safavi-Naini [29] has some limitations. For example, in the case $t > \sum_{i=1}^{m} t_i$, their scheme fails. We illustrate this with 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,

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

$$s_{22} = k_2 + a_{21}x_{22} + a_{22}x_{22}^2 + \omega_1 x_{22}^3 + \omega_2 x_{22}^4$$
$$s_{23} = k_2 + a_{21}x_{23} + a_{22}x_{23}^2 + \omega_1 x_{23}^3 + \omega_2 x_{23}^4$$
$$s_{24} = k_2 + a_{21}x_{24} + a_{22}x_{24}^2 + \omega_1 x_{24}^3 + \omega_2 x_{24}^4$$

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.

3.2.1 Security analysis of the compartmented multi-secret sharing scheme

The security analysis of the compartmented multi-secret sharing scheme is similar to the previous scheme (see Section 3.1.1).

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. 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 $K_\lambda = s_\lambda - \mathrm{e}\Big(P, \sum_{i=1}^{m} a'_{it_i}P\Big)^\lambda$, $1 \le \lambda \le g$, is negligible for a large prime order group G_a.

We have the following observation.

Theorem 3.2.2 *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 $\mid V_1 \cap C_i \mid < t_i$. Hence they cannot compute compartment secrets a_{it_i} as observed by Theorem 3.1.3.

- In the case $t > \sum_{i=1}^{m} t_i$, there are two possibilities.

  1. There is a compartment U_i for which $\alpha_i = \mid V_1 \cap C_i \mid < t_i$. This implies that the corresponding value a_{it_i} cannot be computed by Proposition 1.8.4.
  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 3.2.3 (Verification of shares) *The compartmented multi-secret sharing 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 u_{ij}. Assume that in order to reconstruct the secrets, the cooperating u_{ij} works with the share $b'_{ij} P$. If $b'_{ij} P = b_{ij} P$, then the equation $\mathrm{e}(P, b'_{ij} P) = \mathrm{e}(P, b_{ij} P)$ is valid. Additionally, $\mathrm{e}(P, b_{ij} P) = \mathrm{e}(x_{ij}^{-1} P, x_{ij} b_{ij} P)$ may be used to calculate the value of $\mathrm{e}(P, b_{ij} P)$ since $x_{ij} b_{ij} P$ is open to the public. As a result, it is possible to confirm the share of u_{ij} by examining the correctness of the equation $\mathrm{e}(x_{ij}^{-1} P, x_{ij} b_{ij} P) = \mathrm{e}(P, b'_{ij} P)$.

We have given below an example of the compartmented multi-secret sharing scheme using modified Tate pairing [41]. The computations are done using SageMath.

Example 3.2.4 Consider $E : y^2 = x^3 + x + 38$ over $\mathbb{F}_{47}$. The $\#E(\mathbb{F}_{47}) = 61$ and $61 \mid 47^3 - 1$, 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 any irreducible polynomial of degree 3 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 $s_1 = \mathrm{e}\Big(Q, \sum_{i=1}^{3} a_{it_i} Q\Big) + 10 = \mathrm{e}(Q, 95Q) + 10 = \mathrm{e}(Q, 34Q) + 10 = 15\gamma^2 + 29\gamma + 52$, $s_2 = \mathrm{e}(Q, 2 \times 34Q) + 22 = 16\gamma^2 + 11\gamma + 26$, $s_3 = \mathrm{e}(Q, 3 \times 34Q) + 31 = 2\gamma^2 + 32\gamma + 7$ and $s_4 = \mathrm{e}(Q, 4 \times 34Q) + 15 = 45\gamma^2 + 30\gamma + 5$ where the pairing e is the modified Tate pairing as in [41]. 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 4.2.5). 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 $\mathrm{e}(Q, 20Q + 30Q + 45Q) = \mathrm{e}((4\gamma + 21, 4\gamma^2 + 15\gamma + 4), (42\gamma^2 + 33\gamma + 10, 20\gamma^2 + 31\gamma + 18)) = 15\gamma^2 + 29\gamma + 42$. 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 $\mathrm{e}(Q, 20Q + 30Q + 45Q) = \mathrm{e}((4\gamma+21, 4\gamma^2+15\gamma+4), (42\gamma^2+33\gamma+10, 20\gamma^2+31\gamma+18)) = 15\gamma^2+29\gamma+42$. 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 $K_4 = s_4 - (15\gamma^2 + 29\gamma + 42)^4 = 15$.

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 scheme is examined in detail in the next section.

3.2.2 Complexity of the 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 3.1.2. 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"* [18], the time for computing scalar multiplication of a point on an elliptic curve is $O(\log_2 r)$, where r is the order of the point. There are n scalar multiplications required which cost $O(n\log_2 r)$. At the time of reconstruction, the time computation for finding the inverse of a coefficient matrix of order t, as in Example 3.2.4, 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 the addition of two distinct points on the elliptic curve is $\mathbf{I}$+2$\mathbf{M}$+$\mathbf{S}$ and for doubling $\mathbf{I}$+2$\mathbf{M}$+2$\mathbf{S}$ (see [1], for example), where $\mathbf{I}$, $\mathbf{S}$, $\mathbf{M}$ denotes inverse, subtraction 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 [34, 44], for example) and we required $m + g$ pairing computations. We required g more 1$\mathbf{S}$ for reconstruction of the secrets K_λ, $1 \leq \lambda \leq g$. Combining all these, we get that the complexity of the scheme is $O(n^3)$ for Case II.

Comparision with [64]: The paper [64] 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 [64]. Also, our scheme requires $O(mn^2)$ or $O(n^3)$ time computation which is less as compared to [64].

Chapter 4

Conjunctive and Disjunctive Compartmented Secret Sharing Schemes

This chapter contains our work [15] on conjunctive and disjunctive compartmented secret sharing schemes. An extended abstract of this chapter is published in the Proceedings of Central European Conference on Cryptology (CECC '22), (2022). The full length paper has been submitted to the Tatra Mountains Mathematical Publications.

In a compartmented secret sharing scheme, users are divided into distinct compartments. 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 scheme is defined in Section 1.3.2.

Many compartmented secret sharing schemes have been proposed using polynomials [29, 54, 69] and Chinese Remainder Theorem [33], and many others [12, 64, 68]. The scheme [12] is based on locally repairable codes. The paper [29] uses polynomials and requires a secure channel for distributing the shares. A computationally perfect compartmented secret sharing scheme has been proposed using MDS codes in [64]. In the paper [54], the authors introduced a joint compartmented threshold access structure where the compartments are not necessarily disjoint.

In this chapter, we present two schemes; a conjunctive and a disjunctive compartmented schemes. The schemes use elliptic curves [58] and bilinear pairings

[35, 41]. Our schemes are verifiable and efficient. Also, the schemes are computationally secure. We have provided an explicit example of the schemes.

This chapter is motivated by the following.

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 scheme, if a particular (threshold) number of users from every compartment of each company collaborates, they can get the global secret. While in a disjunctive scheme, a particular number of users from every compartment of any single company can collaborate and get the global secret.

4.1 Conjunctive and Disjunctive Compartmented Secret Sharing Schemes

4.1.1 Setting up and distribution of the parameters of the schemes

Let $q = p^{i_0}$ with $i_0 \in \mathbb{N}$ and p be a large prime. Consider $P \in E(\mathbb{F}_q)$ and $G_a = \langle P \rangle$ be a subgroup of $E(\mathbb{F}_q)$ of order r where r is also a prime integer. We choose r to be a large prime so that ECDLP is hard to solve. Let $G_m = \mu_r$ where μ_r is as in Section 1.5.2. Consider a bilinear pairing e as in Definition 1.5.1.

Let $C_1, C_2, \cdots, C_m$ be m companies interested to merge for a project. Each company C_i has τ_i compartments say $C_{i1}, C_{i2}, \cdots, C_{i\tau_i}$ for $1 \leq i \leq m$ (see Figure 4.1). Suppose there is a set U of n users divided disjointly into these compartments in the presence of a *trusted* Dealer. Let n_{ij} be the number of users in the compartment C_{ij} for each i, $1 \leq i \leq m$ and each j, $1 \leq j \leq \tau_i$. Let $t_{ij} \geq 1$ be the threshold number for each C_{ij} and $t_i \geq \sum t_{ij}$ be the company threshold of C_i. We define the *conjunctive compartmented access structure* as

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

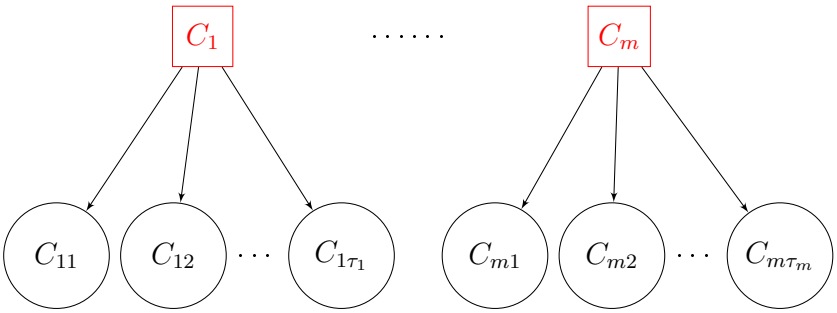


Figure 4.1: Example of conjunctive and disjunctive compartmented schemes

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

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

The Dealer chooses company secret keys $K_1, K_2, \cdots, K_m \in [0, p-1]$ for C_1, C_2, $\cdots, C_m$ respectively and a global secret key $K \in [0, p-1]$. Let $a_{j1}^{(i)}$, $a_{j2}^{(i)}$, $\cdots, a_{jt_{ij}}^{(i)} \in [0, r-1]$ be t_{ij} random integers, with $a_{j1}^{(i)} \neq 0$, for each compartment C_{ij}, $1 \leq i \leq m$ and $1 \leq j \leq \tau_i$.

Let $u_{jk}^{(i)}$ denote k^{th} user in the compartment C_{ij} of company C_i, where $1 \leq i \leq m, 1 \leq j \leq \tau_i$ and $1 \leq k \leq n_{ij}$.

We have two cases according to the definition of the compartmented access structure.

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).

- 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 related to MDS matrices [53].

- Dealer computes $\left(b_{j1}^{(i)}\ b_{j2}^{(i)}\ \cdots\ b_{jn_{ij}}^{(i)}\right)^T = M_{ij} \cdot \left(a_{j1}^{(i)}\ a_{j2}^{(i)}\ \cdots\ a_{jt_{ij}}^{(i)}\right)^T$ 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 $u_{j1}^{(i)}, u_{j2}^{(i)}, \cdots, u_{jn_{ij}}^{(i)}$ in the compartment C_{ij} randomly choose private keys $x_{j1}^{(i)}, x_{j2}^{(i)}, \cdots, x_{jn_{ij}}^{(i)} \in [1, r-1]$, respectively and make $x_{j1}^{(i)}P$, $x_{j2}^{(i)}P$, $\cdots, x_{jn_{ij}}^{(i)}P$ public.

- Then Dealer computes $b_{j1}^{(i)}x_{j1}^{(i)}P$, $b_{j2}^{(i)}x_{j2}^{(i)}P$, $\cdots$, $b_{jn_{ij}}^{(i)}x_{jn_{ij}}^{(i)}P$ for users in each compartment C_{ij} of C_i and sends (publicly) to the respective users in C_{ij}.

- The users $u_{j1}^{(i)}, u_{j2}^{(i)}, \cdots, u_{jn_{ij}}^{(i)}$ in C_{ij} will get their respective shares $b_{j1}^{(i)}P$, $b_{j2}^{(i)}P$, $\cdots$, $b_{jn_{ij}}^{(i)}P$ by computing

$$x_{j1}^{(i)^{-1}}\left(b_{j1}^{(i)}x_{j1}^{(i)}P\right),\ x_{j2}^{(i)^{-1}}\left(b_{j2}^{(i)}x_{j2}^{(i)}P\right),\ \cdots,\ x_{jn_{ij}}^{(i)\ -1}\left(b_{jn_{ij}}^{(i)}x_{jn_{ij}}^{(i)}P\right).$$

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, $1 \le j \le \tau_i$, 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 consider the matrix

$$A_i = \left(\begin{array}{ccccc|c} A_{i1} & 0 & \cdots & 0 & 0 & \\ 0 & A_{i2} & \cdots & 0 & 0 & \\ \vdots & \vdots & \ddots & \vdots & \vdots & B_i \\ 0 & 0 & \cdots & A_{i(\tau_i-1)} & 0 & \\ 0 & 0 & \cdots & 0 & A_{i\tau_i} & \end{array}\right).$$

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. (Such a matrix exists. See Example 4.2.5 below).

Dealer chooses t_i' random values $\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{it_i'} \in [0, r-1]$ 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

$$\begin{aligned}&\left(b_{11}^{(i)}\ b_{12}^{(i)}\ \cdots\ b_{1n_{i1}}^{(i)}\ \cdots\ b_{\tau_i 1}^{(i)}\ b_{\tau_i 2}^{(i)}\ \cdots\ b_{\tau_i n_{i\tau_i}}^{(i)}\right)^T \\ &\qquad = A_i \cdot \left(a_{11}^{(i)}\ \cdots\ a_{1t_{i1}}^{(i)}\ \cdots\ a_{\tau_i 1}^{(i)}\ \cdots\ a_{\tau_i t_{i\tau_i}}^{(i)}\ \alpha_{i1}\ \alpha_{i2}\ \cdots\ \alpha_{it_i'}\right)^T\end{aligned}$$

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.

For Conjunctive Compartmented Secret Sharing Scheme

Dealer computes $s_i = \prod_{j=1}^{\tau_i} \mathrm{e}\left(P, a_{j1}^{(i)}P\right) + K_i$ or equivalently $s_i = \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)}P\right) + K_i$ and computes $S = \mathrm{e}\left(P, \sum_{i=1}^{m} K_i P\right) + K$ (see Remark 3.1.1). Finally, Dealer makes P, M_{ij}, A_i, s_i and S public.

For Disjunctive Compartmented Secret Sharing Scheme

Dealer computes $s_i = \prod_{j=1}^{\tau_i} \mathrm{e}\left(P, a_{j1}^{(i)}P\right) + K_i$ or equivalently $s_i = \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)}P\right) + K_i$ and a polynomial $S(x) = (x-K_1)(x-K_2)\cdots(x-K_m)+K$. Finally, Dealer makes P, M_{ij}, A_i, s_i and $S(x)$ public.

4.1.2 Reconstruction of the secret key

For conjunctive compartmented secret sharing scheme.

For Case I, suppose that t_{ij} (or more) number of 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, suppose the users $u_{j1}^{(i)}, u_{j2}^{(i)}, \cdots, u_{jt_{ij}}^{(i)}$ from each compartment C_{ij} of company C_i, $1 \le i \le m$, collaborates. 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 $\left(a_{j1}^{(i)}P\ a_{j2}^{(i)}P\ \cdots\ a_{jt_{ij}}^{(i)}P\right)^T = M_{ij}'^{-1} \cdot \left(b_{j1}^{(i)}P\ b_{j2}^{(i)}P\ \cdots\ b_{jt_{ij}}^{(i)}P\right)^T$. 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 obtained as $K = S - \mathrm{e}\left(P, \sum_{i=1}^{m} K_i P\right)$.

For Case II, suppose, for each i, t_i number of users from company C_i with at least t_{ij} number of users from each compartment C_{ij} collaborates. Without loss of generality, suppose that the users $u_{j1}^{(i)}, u_{j2}^{(i)}, \cdots, u_{j\beta_{ij}}^{(i)}$ from compartment C_{ij} of company C_i, $1 \le i \le m$, collaborate, where $\beta_{ij} \ge t_{ij}$ $\forall i, j$ and $\sum_{j=1}^{\tau_i} \beta_{ij} = t_i$. The

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

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

Thus, they can compute company secret K_i as $K_i = s_i - \mathrm{e}\left(P, \sum_{j=1}^{\tau_i} a_{j1}^{(i)}P\right)$, $1 \le i \le m$, and hence the global secret key K as $K = S - \mathrm{e}\left(P, \sum_{i=1}^{m} K_i P\right)$.

For disjunctive compartmented secret sharing scheme.

The company secret keys K_i, $1 \le i \le m$, can be computed as in the previous reconstruction of the secret key in the conjunctive compartmented secret sharing scheme. Then the users in any company C_i can reconstruct the global secret key as $K = S(K_i)$.

4.1.3 Verification of the shares

Verification of shares is required to resist two types of problems: The Dealer may send incorrect shares to the users at the time of distribution and the user may send incorrect shares at the time of secret reconstruction. The first problem is not arising in our schemes, as the shares are distributed in an encrypted manner. The verification of the shares in the second problem is given below.

At the time of reconstruction of the secret, each collaborating user $u_{jk}^{(i)}$ sends the share $c_{jk}^{(i)}P$ with an additional information $x_{jk}^{(i)^{-1}}P$ for verification. Other collaborating users can check the originality of the share by checking the validity of the equation $\mathrm{e}\left(x_{jk}^{(i)^{-1}}P,\ b_{jk}^{(i)}x_{jk}^{(i)}P\right) = \mathrm{e}\left(P, c_{jk}^{(i)}P\right)$. The above equation holds if and only if $c_{jk}^{(i)}P = b_{jk}^{(i)}P$ as $\mathrm{e}\left(x_{jk}^{(i)^{-1}}P,\ b_{jk}^{(i)}x_{jk}^{(i)}P\right) = \mathrm{e}\left(P, b_{jk}^{(i)}P\right)$.

4.2 Security Analysis of the Schemes

Bilinear pairing operates as a one-way function, which means 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 ECDLP. For an adversary, the probability of guessing a point Q that satisfies $S - \mathrm{e}(P, Q) = K$ is $1/(r-1)$, and the probability of guessing an integer $K' \in [0, p-1]$ that is equal to K is $1/p$. Therefore the probability of getting the secret is $\max\{1/(r-1), 1/p\}$. Since r and p are very large, the probability is very small.

We have the following results.

Theorem 4.2.1 *Any $t_i - 1$(or fewer) number of users from C_i know nothing about the company secret K_i.*

Proof. Let $\mathcal{A}$ be a set of $t_i - 1$ (or less) users in the company C_i who try to get the company secret K_i.

In the case $t_i = \sum_{j=1}^{\tau_i} t_{ij}$, we have a compartment C_{ij} for which $|\mathcal{A} \cap C_{ij}| < t_{ij}$. Without loss of generality, suppose that the users $u_{j1}^{(i)}, u_{j2}^{(i)}, \cdots, u_{j(t_{ij}-1)}^{(i)}$ from the compartment C_{ij} pool their shares. Then the shares of the users can be written as a system of equations

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

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 1.8.4. 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 1.8.4, users cannot get $a_{j1}^{(i)}P$, $1 \le j \le \tau_i$.

Hence they cannot get the company secret key K_i.

Theorem 4.2.2 *An unauthorized group of users cannot access the secret key K.*

Proof. Assume that there is an unauthorized set $\mathcal{A}$ of users who want to get the secret key K.

For conjunctive compartmented scheme.

As $\mathcal{A} \notin \Gamma_1$, we have either of the following cases.

1. There is some i, $1 \leq i \leq m$, such that $|\mathcal{A} \cap C_i| < t_i$. This implies, by Theorem 4.2.1, that the company secret K_i (and hence the global secret K) cannot be obtained.

2. For all i, $|\mathcal{A} \cap C_i| \geq t_i$, but $\exists$ some i and j such that $|\mathcal{A} \cap C_{ij}| < t_{ij}$. Then for both Case I and Case II, we have a system of equations with more unknowns than equations. Thus, by Proposition 1.8.4, we get r^λ many solutions for some λ. As r is large, the probability of getting K_i is negligible. Hence they cannot get the global secret K.

For the disjunctive compartmented scheme, the proof uses Proposition 1.8.4 and similar arguments as in the case of the conjunctive compartmented scheme above. Hence we omit the proof.

We also have the following observations.

Observation 4.2.3 (For the conjunctive compartmented scheme) *The probability of guessing a random $Q \in E[r]$ with $S - \mathrm{e}(P, Q) = K$ is $1/r$, where $E[r]$ is the set of r-torsion points on the elliptic curve.*

The point $Q \in G_a \subseteq E[r]$ is chosen at random and the order of G_a is r. For a given P, there is only one Q that satisfies $S - \mathrm{e}(P, Q) = K$.

Observation 4.2.4 (For the disjunctive compartmented scheme) *The probability of guessing an integer $K' \in [0, p-1]$ such that $S(K') = K$ is m/p. (Recall that m is the degree of $S(x)$).*

Note that there are only m choices of K_i for which $S(K_i) = K$. Therefore, to find the secret K for an attacker, the required probability is m/p and as p is very large, it is negligible.

We also observe that the constant term of $S(x)$ is $K_1 K_2 \cdots K_m + K$ where K is the global secret. Thus by changing the constant term, it is difficult to get any

information about K.

We have given below an example of the schemes using modified Tate pairing [41]. The computations are done using SageMath.

Example 4.2.5 Consider $E: y^2 = x^3+2x+15$ over $\mathbb{F}_{47}$. 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 size of $E(\mathbb{F}_{47^3})$ is 104188. Let γ be a root of any 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 [41]. Let $P = (15\gamma + 33, 9\gamma^2 + 22\gamma + 23) \in E[61]$ and $G_a = \langle P \rangle$.

Assume that there are two companies C_1 and C_2. Company C_1 has 3 compartments, namely, C_{11}, C_{12}, C_{13} and company C_2 has three compartments, namely, C_{21}, C_{22}, C_{23}. Suppose that $n_{11} = 3, n_{12} = 4, n_{13} = 5, n_{21} = 3, n_{22} = 3, n_{23} = 4$ and $t_{11} = 2, t_{12} = 2, t_{13} = 3, t_{21} = 2, t_{22} = 2, t_{23} = 3$. Let $a_{11}^{(1)} = 32, a_{12}^{(1)} = 23, a_{21}^{(1)} = 14, a_{22}^{(1)} = 19, a_{31}^{(1)} = 37, a_{32}^{(1)} = 52, a_{33}^{(1)} = 43$ $a_{11}^{(2)} = 25, a_{12}^{(2)} = 36, a_{21}^{(2)} = 51, a_{22}^{(2)} = 28, a_{31}^{(2)} = 8, a_{32}^{(2)} = 4, a_{33}^{(2)} = 7$.

We put company secret keys $K_1 = 15, K_2 = 22$ for C_1, C_2 respectively and the global secret key $K = 20$.

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,

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

We compute $\begin{pmatrix} b_{11}^{(1)} & b_{12}^{(1)} & b_{13}^{(1)} \end{pmatrix}^T = M_{11} \cdot \begin{pmatrix} a_{11}^{(1)} & a_{12}^{(1)} \end{pmatrix}^T = (20\ 24\ 36)^T$. The shares of the users in the compartment C_{11} of the company C_1 are

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

We compute $\begin{pmatrix} b_{21}^{(1)} & b_{22}^{(1)} & b_{23}^{(1)} & b_{24}^{(1)} \end{pmatrix}^T = M_{12} \cdot \begin{pmatrix} a_{21}^{(1)} & a_{22}^{(1)} \end{pmatrix}^T = (30\ 32\ 18\ 11)^T$. The

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

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

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

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

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

We 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

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

Then, we 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 $\alpha_{11} = 3, \alpha_{12} = 35$ and $\alpha_{21} = 47$.

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

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

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 users in the company C_2. We compute

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

The shares of the users of the company C_2 are

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

Now we compute $s_1 = \mathrm{e}\left(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\right) + K_1 = \mathrm{e}(P, 22P) + 15 = 28\gamma^2 + 45\gamma + 46$ and $s_2 = \mathrm{e}\left(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\right) + K_2 = \mathrm{e}(P, 23P) + 22 = 45\gamma^2 + 15\gamma + 45$ where e is the modified Tate pairing (see [41]).

For conjunctive compartmented scheme, compute $S = \mathrm{e}(P, K_1P + K_2P) + K = \mathrm{e}(P, 37P) + 20 = 9\gamma^2 + 17\gamma + 38$ and make $P, M_{11}, M_{12}, M_{13}, M_{21}, M_{22}, M_{23}, s_1, s_2$ and S public.

For the disjunctive compartmented scheme, compute $S(x) = (x - K_1)(x - K_2) + K = (x - 15)(x - 22) + 20 = x^2 + 24x + 45$ and make P, A_1, A_2, s_1, s_2 and $S(x)$ 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 $M'_{11} = \begin{pmatrix} 11 & 60 \\ 12 & 22 \end{pmatrix}$ of M_{11} and compute the inverse $M'^{-1}_{11} = \begin{pmatrix} 51 & 55 \\ 11 & 56 \end{pmatrix}$. Then they compute $\left(a_{11}^{(1)}P\ a_{12}^{(1)}P\right)^T = M'^{-1}_{11} \cdot \left(b_{12}^{(1)}P\ b_{13}^{(1)}P\right)^T = \left((14\gamma^2+13\gamma+15, 18\gamma^2+5\gamma+29)\ (16\gamma^2+40\gamma+37, 17\gamma^2+42\gamma+11)\right)^T$. Similarly, the users

- $u_{22}^{(1)}, u_{23}^{(1)}$ can compute the value of $a_{21}^{(1)}P, a_{22}^{(1)}P$.
- $u_{31}^{(1)}, u_{32}^{(1)}, u_{34}^{(1)}$ can compute the value of $a_{31}^{(1)}P, a_{32}^{(1)}P, a_{33}^{(1)}P$.

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

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

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

Then they compute the company secrets $K_1 = s_1 - \mathrm{e}\left(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\right)$ $= 15$ and $K_2 = s_2 - \mathrm{e}\left(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\right) = 22$.

For conjunctive compartmented scheme, compute the global secret key $K = S - \mathrm{e}(P, K_1P + K_2P) = 20$.

For the disjunctive compartmented scheme, the collaborating users in any company C_i, $i = 1, 2$, can compute the global secret key $K = S(K_i) = 20$.

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

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

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

Then the users compute

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

Then they compute the company secrets $K_1 = s_1 - \mathrm{e}\left(P, a_{11}^{(1)}P + a_{21}^{(1)}P + a_{31}^{(1)}P\right)$ $= 15$. 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 $A_2'^{-1} = \begin{pmatrix} 13 & 47 & 0 & 0 & 0 & 0 & 0 & 1 \\ 25 & 15 & 0 & 0 & 0 & 0 & 0 & 9 \\ 16 & 12 & 0 & 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 32 & 48 & 0 & 0 & 0 & 11 \\ 0 & 0 & 17 & 45 & 0 & 0 & 0 & 33 \\ 0 & 0 & 0 & 0 & 28 & 52 & 53 & 20 \\ 0 & 0 & 0 & 0 & 10 & 39 & 24 & 57 \\ 0 & 0 & 0 & 0 & 38 & 41 & 33 & 34 \end{pmatrix}$

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

Then the users compute $\left(a_{11}^{(2)}P\ a_{12}^{(2)}P\ a_{21}^{(2)}P\ a_{22}^{(2)}P\ a_{31}^{(2)}P\ a_{32}^{(2)}P\ a_{33}^{(2)}P\ \alpha_{21}P\right)^T =$

$A_2'^{-1} \cdot \left(b_{11}^{(2)}P\ b_{12}^{(2)}P\ b_{13}^{(2)}P\ b_{22}^{(2)}P\ b_{23}^{(2)}P\ b_{31}^{(2)}P\ b_{32}^{(2)}P\ b_{34}^{(2)}P\right)^T$. Then they compute the company secrets $K_2 = s_2 - \mathrm{e}\left(P, a_{11}^{(2)}P + a_{21}^{(2)}P + a_{31}^{(2)}P\right) = 22$.

For conjunctive compartmented scheme, compute the global secret key $K = S - \mathrm{e}(P, K_1P + K_2P) = 20$.

For the disjunctive compartmented scheme, the collaborating users in any company C_i, $i = 1, 2$, can compute the global secret key $K = S(K_i) = 20$.

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

4.3 Computational Complexity of the Schemes

The matrix multiplication of matrices of order $n \times t$ and $t \times 1$ involves nt operations. The time for computing scalar multiplication of a point on an elliptic curve is $O(\log_2 r)$ using the basic "*Double-and-Add Algorithm*" [18], where r is the order of the point. For computing a pairing takes $O(\log_2 r)$ operations (see [34, 44]). Adding two distinct points takes $\mathbf{I}$+2$\mathbf{M}$+$\mathbf{S}$ operations and for doubling takes $\mathbf{I}$+2$\mathbf{M}$+2$\mathbf{S}$ operations (see [1]) where $\mathbf{I}$, $\mathbf{M}$, $\mathbf{S}$ denotes 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 require $\sum_{i=1}^{m} \tau_i$ matrix multiplications of order $n_{ij} \times t_{ij}$ and $t_{ij} \times 1$ which costs $\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij}t_{ij}$ operations. As $n_{ij} \geq t_{ij}$ and $\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij} = n$, the sum $\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij}t_{ij} \leq n^2$. For Case II, the Dealer require m matrix multiplications of order $\left(\sum_{j=1}^{\tau_i} n_{ij}\right) \times t_i$ and $t_i \times 1$ which costs $\sum_{i=1}^{m}\left(\sum_{j=1}^{\tau_i} n_{ij}\right) t_i$ operations. As $\sum_{j=1}^{\tau_i} n_{ij} \geq t_i$ and $\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} n_{ij} = n$, the sum $\sum_{i=1}^{m}\left(\sum_{j=1}^{\tau_i} n_{ij}\right) t_i \leq n^2$. In addition, Dealer require n scalar multiplications of points to encrypt the shares $b_{jk}^{(i)}x_{jk}^{(i)}P$ and m more scalar multiplications require to compute K_iP, $1 \leq i \leq m$, that

costs $O((m+n)\log_2 r)$. To compute s_i require $\sum_{i=1}^{m} \tau_i$ point additions and m pairings which costs $O(m\log_2 r)$. To compute S in the conjunctive compartmented scheme, the Dealer requires m additions of points and one pairing. In disjunctive compartmented scheme, m multiplications and an addition to compute the polynomial $S(x)$.

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 $\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} t_{ij}^3 \leq n^3$ operations. To find the unknowns $a_{jk}^{(i)}P$, they require $\sum_{i=1}^{m}\sum_{j=1}^{\tau_i} t_{ij}^2 \leq n^2$ 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 require point addition is $\sum_{i=1}^{m} t_i^2 \leq n^2$. In addition, to find K_i required $\sum_{i=1}^{m} m_i$ point additions and m pairing computations. Also, they required $O(m)$ additions of points and one pairing computation to find K.

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 $\sum_{j=1}^{\tau_i} t_{ij}^3 < n^3$ operations. To find the unknowns $a_{jk}^{(i)}P$, they require $\sum_{j=1}^{\tau_i} t_{ij}^2 < n^2$ 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, finding K_i requires m_i point additions and one pairing computation. Also, they require $O(m)$ operations to find K.

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

Chapter 5

Conjunctive Hierarchical Multi-Secret Sharing Scheme

In this chapter, we present our work [16] on a conjunctive hierarchical multi-secret sharing scheme using elliptic curves. This work has been submitted to the Indian Journal of Pure and Applied Mathematics.

Secret sharing with many levels of hierarchy is known as hierarchical secret sharing. In a hierarchical secret sharing scheme (see Definition 1.3.1), 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 [5, 23, 29, 56, 59, 61, 63], 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 [3, 8, 40]).

There are two types of hierarchical schemes, namely conjunctive and disjunctive (see Definition 1.3.1). In this chapter, we have presented a conjunctive hierarchical secret sharing scheme using elliptic curves and bilinear pairings. 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' record.

Our scheme is significant because it overcomes all of the limitations inherent in the majority of existing schemes. The 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. 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 [3] and [66] are verifiable.

5.1 Conjunctive Hierarchical Multi-Secret Sharing Scheme

5.1.1 Setting up and distribution of the parameters of the scheme

Consider an elliptic curve E over a finite field $\mathbb{F}_q$, where $q = p^{i_0}$ for some $i_0 \in \mathbb{N}$ and p is a large prime. Let $P \in E(\mathbb{F}_q)$ be a point of order r, where r is a prime integer and $G_a = \langle P \rangle$, $G_m = \mu_r$. We assume that r is large enough so that ECDLP 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 as 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 [32, Theorem 2.4.3]).

Such matrices are known as MDS matrices. We refer to [32] for more details.

We need the following two propositions to describe the scheme.

Proposition 5.1.1 *Let m_1, m_2 and t be positive integers. Suppose $b_1, b_2, \cdots, b_{m_1} \in \mathbb{F}_r$ 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 $X \in \mathbb{F}_r^t$.*

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 5.1.2 *Let m_1, m_2 and t be positive integers with $t \leq m_1$. Suppose $b_1, b_2, \cdots, b_{m_1} \in \mathbb{F}_r$ 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 $v_1, v_2, \cdots, v_t \in \mathbb{F}_r^{m_1}$ be the column vectors of A. Let W be a subspace of $\mathbb{F}_r^{m_1}$ such that $\mathrm{Span}\{\mathrm{v_1}, \mathrm{v_2}, \cdots, \mathrm{v_t}\} + \mathrm{W} = \mathbb{F}_\mathrm{r}^{\mathrm{m_1}}$ 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 $w_1, w_2, \cdots, w_{t'-t} \in \mathbb{F}_r^{m_1}$ 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 $\mathbb{F}_r^{m_1}$, 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

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

(as in Definition 1.3.1). 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 standard MDS matrices.
- D chooses t_1 random integers $a_{11}, a_{12}, \cdots, a_{1t_1} \in [0, r-1]$ 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 $x_{1j} \in [1, r-1]$ 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 $x_{1j}^{-1}(b_{1j}x_{1j})P$.

Level L_2.

Depending on the size of t_2, we make the following cases.

Case I. For $t_2 > n_1$, consider a matrix M_2 of order $(n_1 + n_2) \times t_2$ such that a submatrix of M_2 consisting of any t_2 rows forms an invertible submatrix. D chooses t_2 values $a_{21}, a_{22}, \cdots, a_{2t_2} \in [0, r-1]$ and computes

$$(b_{11}\ \cdots\ b_{1n_1}\ b_{21}\ \cdots\ b_{2n_2})^T = M_2 \cdot (a_{21}\ a_{22}\ \cdots\ a_{2t_2})^T,$$

in such a way that b_{1j}, $j = 1, 2, \cdots, n_1$, are same as in level L_1. By Proposition 5.1.1, choosing a matrix M_2 and values $a_{21}, \cdots, a_{2t_2}$ satisfying above conditions is possible. Each u_{2j} in level L_2 chooses $x_{2j} \in [1, r-1]$ randomly and makes $x_{2j}P$, $j = 1, 2, \cdots, n_2$, public. Then D computes $b_{2j}x_{2j}P$ for u_{2j} and sends (publicly)

to the respective user. Then each u_{2j} will get their share $b_{2j}P$ by computing $x_{2j}^{-1}(b_{2j}x_{2j})P$.

Case II. For $t_2 \leq n_1$, consider a matrix M_2 of order $(n_1 + n_2) \times t_2'$, where $n_1 < t_2' \leq n_1 + n_2$, such that the first t_2 columns of any t_2 rows forms an invertible submatrix of M_2. D chooses t_2' values $a_{21}, a_{22}, \cdots, a_{2t_2}, \cdots, a_{2t_2'} \in [0, r-1]$ and computes

$$(b_{11} \ \cdots \ b_{1n_1} \ b_{21} \ \cdots \ b_{2n_2})^T = M_2 \cdot (a_{21} \ a_{22} \ \cdots \ a_{2t_2} \ \cdots \ a_{2t_2'})^T,$$

in such a way that b_{1j}, $j = 1, 2, \cdots, n_1$, are same as in level L_1. By Proposition 5.1.2, such a matrix M_2 satisfying the above conditions exists. D keeps the first t_2 values $(a_{21}, \cdots, a_{2t_2})$ as secret and declares rest $t_2' - t_2$ values as public. Each u_{2j} in level L_2 chooses $x_{2j} \in [1, r-1]$ randomly and makes $x_{2j}P$ public. Then D computes $b_{2j}x_{2j}P$ for u_{2j} and sends (publicly) to the respective user. Then each u_{2j} will get their share $b_{2j}P$ by computing $x_{2j}^{-1}(b_{2j}x_{2j})P$.

In general, for $i \geq 3$, the distribution of shares is as 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 $a_{i1}, a_{i2}, \cdots, a_{it_i} \in [0, r-1]$ 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 5.1.1. Each u_{ij} in level L_i, chooses $x_{ij} \in [1, r-1]$ 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 $a_{i1}, a_{i2}, \cdots, a_{it_i}, \cdots, a_{it_i'} \in [0, r-1]$ 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 the same as in the previous levels. This is possible in view of Proposition 5.1.2. 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 $x_{ij} \in [1, r-1]$ 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 $v_i = \mathrm{e}\,(P, \ i \cdot Q) + K_i$ where $Q = \sum_{j=1}^{m} a_{j1}P$ (see Remark 3.1.1). Finally, D makes v_i, $1 \leq i \leq s$, and M_j, $1 \leq j \leq m$, public.

5.1.2 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 $M_1'^{-1} \cdot (b_{11}P \ b_{12}P \ \cdots \ b_{1t_1}P)^T = (a_{11}P \ a_{12}P \ \cdots \ a_{1t_1}P)^T$.

At level L_2, in Case I, the collaborating users from levels L_1 and L_2 can find $(a_{21}P, a_{22}P, \cdots, a_{2t_2}P)$ as above. In Case II, let $M_2 = \begin{pmatrix} A_2 & A_2' \\ B_2 & B_2' \end{pmatrix}$ (see Proposition 5.1.2). 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 $\Big(a_{31}P, a_{32}P, \cdots, a_{3t_3}P\Big)$ and so on. Then, the users compute $Q = \sum_{j=1}^{m} a_{j1}P$. Therefore, the secrets $K_i = v_i - \mathrm{e}\left(P, \ i \cdot Q\right)$ for $1 \leq i \leq s$, are revealed.

5.1.3 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 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 $\mathrm{e}(x_{ij}^{-1}P, b_{ij}x_{ij}P) = \mathrm{e}(P, c_{ij}P)$. The above equation holds true if and only if $c_{ij}P = b_{ij}P$ as $\mathrm{e}(x_{ij}^{-1}P, b_{ij}x_{ij}P) = \mathrm{e}(P, b_{ij}P)$.

5.2 Security Analysis of the Scheme

Bilinear pairing e is a one-way function and can be calculated in two steps. The first is to use Miller's algorithm ([44, 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 [26] 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 $\mathrm{e}(P, Q) = g$ 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 $\mathrm{e}(P, Q) = g$ 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 $\mathrm{e}(P, Q) = g = \mathrm{e}(P, Q')$ implies that $\mathrm{e}(P, Q - Q') = 1$. As

P is a generator for G_a, it follows that $Q = Q'$. Hence, we have the following observation.

Observation 5.2.1 *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 $\mathrm{e}(P, Q) = g$.*

For given points P and aP, $a \in \mathbb{Z}$, on an elliptic curve E, finding the value of a is known as *ECDLP*. It is believed that ECDLP is computationally infeasible to solve for a suitable choice of the elliptic curve E and points on E (see [27]).

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

The probability of guessing level secrets $a_{i1}P$ for $1 \leq i \leq m$ $\left(\text{or } \sum_{i=1}^{m} a_{i1}P\right)$ is $1/r$ and guessing the correct secret K_i is $1/p$. So the probability of getting secrets is $\max\{1/r, 1/p\}$. As r and p are large primes, this probability is very small.

Theorem 5.2.3 *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 1.8.4, the system has r^{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 $1/r$. 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 our scheme and some of the known schemes is shown in Table 5.1.

Table 5.1: Comparison with other schemes

Scheme	Binu [8]	Liu [40]	Tentu [63]	Our scheme
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

5.3 An Example of the Scheme

We give an example of the conjunctive hierarchical scheme using modified Tate pairing ([41]). 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 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 ([41]). 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 $v_1 = \mathrm{e}(P,Q)+K_1 = \mathrm{e}(P,13P)+8 = 37\alpha^2+28\alpha+12$, $v_2 = \mathrm{e}(P,2Q)+K_2 = \mathrm{e}(P,26P)+15 = 28\alpha^2+7\alpha+4$, $v_3 = \mathrm{e}(P,3Q)+K_3 = \mathrm{e}(P,2P)+22 = 36\alpha^2+32\alpha+23$, $v_4 = \mathrm{e}(P,4Q)+K_4 = \mathrm{e}(P,15P)+11 = 42\alpha^2+5\alpha+24$. 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

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

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 $K_1 = v_1 - \mathrm{e}(P, Q) = 8$, $K_2 = v_2 - \mathrm{e}(P, 2Q) = 15$, $K_3 = v_3 - \mathrm{e}(P, 3Q) = 22$, $K_4 = v_4 - \mathrm{e}(P, 4Q) = 11$.

5.4 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 [18] is $O(\log_2 \mathrm{r})$, where r 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 $\mathbf{I}$+2$\mathbf{M}$+$\mathbf{S}$ and for doubling $\mathbf{I}$+2$\mathbf{M}$+2$\mathbf{S}$ (see [1]), where $\mathbf{I}$, $\mathbf{S}$, $\mathbf{M}$ denote inverse, squaring and multiplication, respectively. There are many pairings that cost logarithmic time (see [34, 44], 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 $O(n\log_2 \mathrm{r})$. 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, $1 \leq i \leq m$, which takes $\sum_{i=1}^{m} t_i^3$ operations. For $t_i \leq n_i$ and as $\sum_{i=1}^{m} n_i = n$, the sum $\sum_{i=1}^{m} t_i^3 \leq n^3$. 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, $1 \leq i \leq s$.

Hence, combining all these, the computational complexity of the scheme is $O(n^3)$.

The hierarchical scheme proposed in [71] is based on *linear homogeneous recurrences*. The complexity of their scheme is $O(n^{k_m-1}\text{logn})$ where k_m is the threshold of the last level, which is an improvement over the complexity of the scheme proposed by Tassa [62]. However, the complexity of our scheme is $O(n^3)$.

Conclusion

This thesis contains our work which is published/accepted/submitted in two conferences and two journals. All our work is based on elliptic curves and bilinear pairings. In Chapter 2, we have discussed a blind signature scheme using self-pairings. The scheme is an improved version of Chakraborty-Mehta's scheme [10] where the security was lacking. In Chapter 3, we gave a multi-secret sharing scheme, and based on it, we presented a compartmented multi-secret sharing scheme. Then in Chapter 4, we have introduced conjunctive and disjunctive compartmented secret sharing schemes. In Chapter 5, we have proposed a conjunctive hierarchical multi-secret sharing scheme.

The schemes which we presented in Chapter 3, 4 and 5 are based on elliptic curves and bilinear pairings. The schemes are verifiable and computationally efficient. We have provided security analysis of all the schemes and complexity aspects are also discussed. For the illustrations, we have given an example of each of the schemes. The computations are done using SageMath.

Bibliography

[1] R. K. K. Ajeena, K. Hailiza, *The computational complexity of elliptic curve integer sub-decomposition (ISD) method*, In: AIP Conference Proceedings **1605**, 557-562, (2014). ↑26, ↑54, ↑70, ↑84

[2] M. Backes, A. Kate, A. Patra, *Computational Verifiable Secret Sharing Revisited*. In: Advances in Cryptology - ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science **7073**. Springer, Berlin, Heidelberg, (2011). ↑15

[3] M. Bahramian, K. Eslami, *A new verifiable multi-secret sharing scheme based on elliptic curves and pairings*, Italian Journal of Pure and Applied Mathematics, n-41, 456-468, (2019). ↑73, ↑74

[4] R. Balasubramanian, N. Koblitz, *The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptology **11**, 141-145, (1998). ↑21

[5] M. Belenkiy, *Disjunctive multi-level secret sharing*, IACR Cryptology ePrint Archive 2008, 18, (2008). https://eprint.iacr.org/2008/018.pdf ↑73

[6] P. Barreto, H. Kim, B. Lynn, M. Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology - CRYPTO 2002, Lecture Notes in Computer Science **2442**, 354-368, (2002). ↑22

[7] P. Barreto, B. Lynn, M. Scott, *Efficient implementation of pairing-based cryptosystems*, Journal of Cryptology **17**, 321-334, (2004). ↑22

[8] V. P. Binu, A. Sreekumar, *Threshold Multi Secret Sharing Using Elliptic Curve and Pairing*, International Journal of Information Processing, **9(4)**, 100-112, (2015). ↑30, ↑73, ↑81

[9] G. R. Blakley, *Safeguarding cryptographic keys*, In: AFIPS conference proceedings **48**, 313-317, (1979). ↑15

[10] K. Chakraborty, J. Mehta, *A stamped blind signature scheme based on elliptic curve discrete logarithm problem*, International Journal of Network Security **14**(6), 316-319, (2012). ↑4, ↑29, ↑30, ↑31, ↑87

[11] D. Chaum, *Blind signatures for untraceable payments*, Advances in Cryptology: Proceedings of Crypto 82, Springer-Verlag, 199-203, (1983). ↑29

[12] Q. Chen, C. Tang, Z. Lin, *Compartmented secret sharing schemes and locally repairable codes*, IEEE Transactions on Communications **68**(10), 5976-5987, (2020). ↑39, ↑55

[13] Q. Chen, C. Tang, Z. Lin, *Efficient explicit constructions of compartmented secret sharing schemes*, Designs, Codes and Cryptography, **87**(12), 2913-2940, (2019). ↑39

[14] M. Chintamani, P. Paul, L. Sa, *Compartmented Multi-Secret Sharing Schemes using Elliptic Curves*, Journal of Information and Optimization Sciences (accepted). ↑4, ↑39

[15] M. Chintamani, P. Paul, L. Sa, *Conjunctive and Disjunctive Compartmented Secret Sharing Schemes using Elliptic Curves*, Tatra Mountains Mathematical Publications (submitted). Extended abstract of the paper published in the Proceedings of Central European Conference on Cryptology (CECC '22), 34-37, (2022). https://cecc22.re-search.info/files/cecc22-printed.pdf ↑4, ↑55

[16] M. Chintamani, P. Paul, L. Sa, *Conjunctive Hierarchical Multi-Secret Sharing Scheme using Elliptic Curves*, Indian Journal of Pure and Applied Mathematics (submitted). ↑4, ↑73

[17] M. Chintamani, L. Sa, *A Blind Signature Scheme Based on Bilinear Pairings*, In: Proceedings of the Seventh International Conference

on Mathematics and Computing, Advances in Intelligent Systems and Computing **1412**, Springer, Singapore, (2022). https://doi.org/10.1007/978-981-16-6890-6_1 ↑4, ↑29, ↑30, ↑34

[18] 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 1999), Lecture Notes in Computer Science **1717**, 292-302, Springer, (1999). ↑25, ↑26, ↑43, ↑54, ↑70, ↑84

[19] D. S. Dummit, R. M. Foote, *Abstract Algebra*, Third Edition, John Wiley and Sons, Inc., (2004). ↑7

[20] A. Enge, *Elliptic Curves and Their Applications to Cryptography: An Introduction*, Kluwer Academic Publishers, (1999). ↑4, ↑20

[21] P. Feldman, *A practical scheme for non-interactive verifiable secret sharing*, 28th Annual Symposium on Foundations of Computer Science (SFCS 1987), 427-438, (1987). ↑15

[22] O. Farras, J. Marti-Farre, C. Padro, *Ideal multipartite secret sharing schemes*, Journal of Cryptology **25**(3), 434-463, (2012). ↑39

[23] O. Farras, C. Padro, *Ideal Hierarchical Secret Sharing Schemes*, IEEE Transactions on Information Theory **58**, 3273-3286, (2012). ↑73

[24] G. Frey, M. Müller, H.-G. Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Transactions on Information Theory **45**(5), 1717-1718, (1999).

[25] S. Galbraith, K. Harrison, D. Soldera, *Implementing the Tate pairing*, Algorithmic Number Theory: 5th International Symposium, ANTS-V, Lecture Notes in Computer Science **2369**, 324-337, (2002). ↑22

[26] S. D. Galbraith, F. Hess, F. Vercauteren, *Aspects of Pairing Inversion*, IEEE Transactions on Information Theory **54**(12), 5719-5728, (2008). ↑79

[27] S. D. Galbraith, N. P. Smart, *Evaluation report for CRYPTREC: security level of cryptography—ECDLP mathematical problem*, (2001). https://www.cryptrec.go.jp/exreport/cryptrec-ex-1029-2001.pdf ↑80

[28] J. A. Gallian, *Contemporary Abstract Algebra*, 8th Edition, Brooks/Cole, Cengage Learning, (2012). ↑7

[29] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, *Secret sharing in multilevel and compartmented groups*, In: Proceedings of Australasian Conference on Information Security and Privacy, (ACISP 1998), Lecture Notes in Computer Science **1438**, 367-378, (1998). ↑16, ↑39, ↑40, ↑49, ↑55, ↑73

[30] S. Goldwasser, S. Micali, R. Rivest, *A Digital Signature Scheme Secure Against Adaptative Chosen-Message Attacks*, SIAM Sournal of Computing **17(2)**, 281-308, (1988). ↑30

[31] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, (2010). ↑4, ↑17

[32] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press (2012). ↑74, ↑75

[33] S. Iftene, *General secret sharing based on the Chinese remainder theorem with applications in E-voting*, Electronic Notes in Theoretical Computer Science **186**, 67-84, (2007). ↑15, ↑39, ↑55

[34] S. Ionica, A. Joux, *Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree*, In: Pairing-Based Cryptography - Pairing 2010. Pairing 2010. Lecture Notes in Computer Science **6487**, Springer, Berlin, Heidelberg, (2010). ↑26, ↑44, ↑54, ↑70, ↑84

[35] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science **1838**, 385-393, (2000). Full version: Journal of Cryptology **17**, 263-276 (2004). ↑15, ↑40, ↑56

[36] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics **114**, Springer-Verlag, New York, (1994). ↑8, ↑25

[37] S. C. Kothari, *Generalized Linear Threshold Scheme*, Advances in Cryptology: Proceedings of CRYPTO '84 (Blakely, G.R., Chaum, D., eds.), Lecture Notes in Computer Science **196**, 231-241, (1985). ↑15

[38] H.-S. Lee, *A self-pairing map and its applications to cryptography*, Applied Mathematics and Computation **151**, 671-678, (2004). ↑4, ↑30, ↑31

[39] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, **20**, Cambridge University Press, (2000). ↑7

[40] D. Liu, D. Huang, P. Luo, Y. Dai, *New schemes for sharing points on an elliptic curve*, Computers and Mathematics with Applications **56**, 1556-1561, (2008). ↑30, ↑39, ↑73, ↑81

[41] A. Menezes, *An introduction to pairing-based cryptography*, Recent trends in Cryptography, Contemporary Mathematics, **477** (2009) 47-65 American Mathematical Society, Providence, RI, (2009). ↑4, ↑18, ↑20, ↑21, ↑40, ↑41, ↑44, ↑51, ↑52, ↑56, ↑63, ↑67, ↑81

[42] A. Menezes, P. van Oorschot, S. Vastone, *Handbook of Applied Cryptography*, Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, (1997). ↑23

[43] A. Menezes, D. Stebila, *Challenges in Cryptography*, IEEE Security & Privacy **19(2)**: 70-73 (2021). ↑12

[44] V. Miller, *The Weil Pairing, and Its Efficient Calculation*, Journal of Cryptology **17**, 235-261 (2004). ↑22, ↑26, ↑44, ↑54, ↑70, ↑79, ↑84

[45] Nikolay A. Moldovyan, *Blind signature protocols from digital signature standards*, International Journal of Network Security **13**(1), 22-30, (2011). ↑29

[46] D. Pointcheval, J. Stern, *Provably Secure Blind Signature Schemes*, In: Advances in Cryptology -ASIACRYPT '96, Lecture Notes in Computer Science **1163**, 252-265, (1996). ↑29

[47] J. M. Pollard, *Monte Carlo methods for index computation (mod p)*. Math. Comp., **32**(143), 918-924, (1978). ↑18

[48] B. Preneel, *The state of cryptographic hash functions*, Lecture Notes in Computer Science **1561**, 158-182, (1999). ↑22

[49] A. R. Rao, P. Bhimasankaram, *Linear Algebra, 2nd Ed.*, Texts and Readings in Mathematics (TRIM) **19**, Hindustan Book Agency (2000). ↑26

[50] Mohamed M. Rasslan, *A stamped hidden-signature scheme utilizing the elliptic curve discrete logarithm problem*, International Journal of Network Security **13**(1), 49-57, (2011). ↑29

[51] E. A. Rawashdeh, *A simple method for finding the inverse matrix of Vandermonde matrix*, Matematički Vesnik **71**, 207-213 (2019). ↑39, ↑40, ↑41

[52] R. Rivest, A. Shamir, L. Adelman, *A Method for Obtaining Digital Signature and Public Key Cryptosystems*, Communications of the ACM **21**(2), 120-126, (1978). ↑13

[53] S. Roman, *Coding and information theory*, Springer-Verlag, Berlin, Heidelberg, (1992). ↑57

[54] A. A. Selcuk, R. Yilmaz, *Joint compartmented threshold access structures*, IACR Cryptology ePrint Archive, 2013/054, (2013). https://eprint.iacr.org/2013/054.pdf ↑39, ↑55

[55] B. Schoenmakers, *Lecture Notes on Cryptographic Protocols*, Version **1.7**, February 2, (2022). https://www.win.tue.nl/~berry/CryptographicProtocols/LectureNotes.pdf. ↑12, ↑22

[56] A. Shamir, *How to share a secret*, Communications of the ACM 22, 612-613, (1979) ↑15, ↑42, ↑73

[57] D. Shanks, *Class Number, A Theory of Factorization and Genera*, Proceedings of Symposium of Pure Mathematics, Vol. **20**, pp. 415-440, (1969). ↑18

[58] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, New York, (1986). ↑40, ↑55

[59] G. Simmons, *How to (Really) Share a Secret*, in Advances in Cryptology - Proceedings of CRYPTO '88 (S. Goldwasser, ed.), Lecture Notes in Computer Science **403**, 390-448, (1990). ↑15, ↑16, ↑39, ↑73

[60] D. R. Stinson, M. B. Paterson, *Cryptography : Theory and Practice*, 4th ed., Textbook in Mathematics, CRC Press Taylor & Francis Group, (2019). ↑4, ↑23, ↑24

[61] T. Tassa, *Hierarchical Threshold Secret Sharing*, Journal of Cryptology **20**, 237-264, (2007). ↑73

[62] T. Tassa, N. Dyn, *Multipartite secret sharing by bivariate interpolation*, Journal of Cryptology **22**(2), 227-258, (2009). ↑39, ↑85

[63] A. N. Tentu, P. Paul, V. Ch. Venkaiah, *Ideal and Perfect Hierarchical Secret Sharing Schemes based on MDS codes*, IACR Cryptology, ePrint Arch. 189 (2013). eprint.iacr.org/2013/189.pdf ↑15, ↑73, ↑81

[64] A. N. Tentu, P. Paul, V. Ch. Venkaiah, *Computationally perfect compartmented secret sharing schemes based on MDS codes*, International Journal of Trust Management in Computing and Communications **2**(4), 353-378, (2014). ↑16, ↑39, ↑40, ↑54, ↑55

[65] M. Tian, Y. Zhu, Z. Chen, *Two Simple Attacks on a Blind Signature Scheme*, International Journal of Network Security **16**(6), 498-500, (2014). ↑4, ↑30, ↑31, ↑33

[66] S. J. Wang, Y. R. Tsai, C. C. Shen, *Verifiable threshold scheme in multi-secret sharing distributions upon extensions of ECC*, Wireless Personal communications **56**, 173-182, (2011). ↑74

[67] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Second Edition, Discrete Mathematics and its Applications, Chapman & Hall/CRC (2008). ↑4, ↑11, ↑18, ↑20, ↑21, ↑22

[68] G. Xu, J. Yuan, G. Xu, Z. Dang, *An efficient compartmented secret sharing scheme based on linear homogeneous recurrence relations*, Security and Communication Networks **2021**, Article ID 5566179, (2021). ↑39, ↑55

[69] Y. Yu, M. Wang, *A probabilistic secret sharing scheme for a compartmented access structure*, In: Qing S., Susilo W., Wang G., Liu D. (eds) Information and Communications Security. ICICS 2011. Lecture Notes in Computer Science **7043**, Springer, Berlin, Heidelberg, (2011). ↑39, ↑55

[70] L. Yuan, M. Li, C. Guo, K-KR. Choo, Y. Ren, *Novel Threshold Changeable Secret Sharing Schemes Based on Polynomial Interpolation*, PLoS ONE, (2016). ↑15

[71] J. Yuan, J. Yang, C. Wang, X. Jia, F.-W. Fu, G. Xu, *A New efficient hierarchical multi-secret sharing scheme based on linear homogeneous recurrence relations*, Information Sciences **592**, 36-49, (2022). ↑85

[72] Z. M. Zhao, *ID-based weak blind signature from bilinear pairings*, International Journal of Network Security **7**(2), 265-268, (2008). ↑29

UNIVERSITY OF HYDERABAD
Prof. C R Rao Road, Gachibowli
Hyderabad 500 046 INDIA

Dt. 29 May 2023

Dr. Mohan Chintamani
Assistant Professor
School of Mathematics & Statistics

Plagiarism-free Certificate

This is to certify that the similarity index of this thesis as checked by the Library of University of Hyderabad is 17%.

Out of this, 8% of similarity has been identified with the candidate Mr. Laba Sa's (17MMPP01) own publication. All the publications of Mr. Laba Sa have been explicitly mentioned in this thesis. The remaining 9% of the similarity has been excluded since they are of generic nature, pertaining to standard terminology, definitions and symbols of the subject matter.

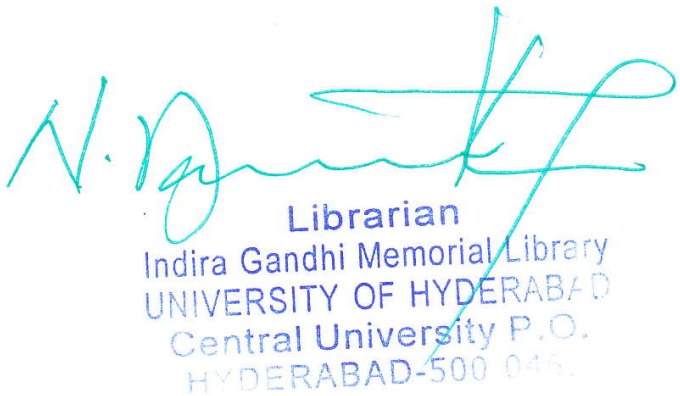
Hence the present thesis may be considered as plagiarism-free.

Dr. Mohan Chintamani

Dr. MOHAN N CHINTAMANI
Assistant Professor
School of Mathematics & Statistics
University of Hyderabad
HYDERABAD-500 046. T.S.

Number Theoretic Cryptography

by Laba Sa



Number Theoretic Cryptography

ORIGINALITY REPORT

17%	7%	17%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Mohan Chintamani, Laba Sa. "Chapter 1 A Blind Signature Scheme Based onBilinear Pairings", Springer Science and Business Media LLC, 2022 Publication This is Candidates own published work. Hence is excluded.	8%
2	Communications in Computer and Information Science, 2014. Publication This are generic terms from area of Cryptography. Hence is excluded.	<1%
3	ijns.jalaxy.com.tw Internet Source Commonly used terms Hence is excluded	<1%
4	"Encyclopedia of Cryptography and Security", Springer Science and Business Media LLC, 2011 Publication This are standard math/cryptological terms Symbols. Hence excluded.	<1%
5	"Information Theoretic Security", Springer Science and Business Media LLC, 2016 Publication Generic terms. Hence excluded.	<1%
6	ebin.pub Internet Source Universal math symbols. Hence excluded	<1%
7	www.docstoc.com Internet Source	

<1%

8	Chan, C.W.. "A scheme for threshold multi-secret sharing", Applied Mathematics and Computation, 20050706 Publication Generic terms from Cryptography - Excluded	<1%
9	Submitted to University of Hyderabad, Hyderabad Student Paper This are standard terminologies & definitions. Hence excluded	<1%
10	"Data Engineering and Communication Technology", Springer Science and Business Media LLC, 2020 Publication Generic Symbols/Terms. Excluded	<1%
11	Robert J. Aumann, Sergiu Hart. "Long Cheap Talk", Econometrica, 2003 Publication Universal terminology - Excluded	<1%
12	Guoai Xu, Jiangtao Yuan, Guosheng Xu, Zhongkai Dang. "An Efficient Compartmented Secret Sharing Scheme Based on Linear Homogeneous Recurrence Relations", Security and Communication Networks, 2021 Publication Commonly used phrase. Hence excluded	<1%
13	Basic Modern Algebra with Applications, 2014. Publication Universal mathematic Symbols Hence excluded	<1%
14	www.win.tue.nl Internet Source	<1%

15	Rolla Subrahmanyam, N. Rukma Rekha, Y. V. Subba Rao. "Authenticated Distributed Group Key Agreement Protocol Using Elliptic Curve Secret Sharing Scheme", IEEE Access, 2023 Publication Commonly used terms. Hence excluded.	<1 %
16	Submitted to University of Birmingham Student Paper This is standard definition & terms. Hence excluded.	<1 %
17	dl.icdst.org Internet Source	<1 %
18	Neal Koblitz. "A Course in Number Theory and Cryptography", Springer Science and Business Media LLC, 1994 Publication	<1 %
19	Advances in Information Security, 2009. Publication	<1 %
20	www.math.uwaterloo.ca Internet Source	<1 %
21	Submitted to Uttar Pradesh Technical University Student Paper	<1 %
22	doras.dcu.ie Internet Source	<1 %
23	Submitted to University of Malaya Student Paper	<1 %
24	www.utupub.fi Internet Source	

		<1 %
25	www.diva-portal.org Internet Source	<1 %
26	"Progress in Cryptology – AFRICACRYPT 2011", Springer Nature, 2011 Publication	<1 %
27	Introduction to Classical Mathematics I, 1991. Publication	<1 %
28	Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. "Chapter 6 Elliptic Curves and Cryptography", Springer Science and Business Media LLC, 2014 Publication	<1 %
29	Hsu, C.F.. "An ideal multi-secret sharing scheme based on MSP", Information Sciences, 20110401 Publication	<1 %
30	www.m-hikari.com Internet Source	<1 %
31	ipfs.io Internet Source	<1 %
32	"Analytic Number Theory", Springer Science and Business Media LLC, 1996 Publication	<1 %

33	Submitted to Georgia Institute of Technology Main Campus Student Paper	<1 %
34	www.math.mcgill.ca Internet Source	<1 %
35	Submitted to UT, Dallas Student Paper	<1 %
36	"Number-Theoretic Methods in Cryptology", Springer Science and Business Media LLC, 2018 Publication	<1 %
37	Ari Ben-Menahem. "Chapter 6 The Clockwork Universe", Springer Science and Business Media LLC, 2009 Publication	<1 %
38	Atsushi Koide, Raylin Tso, Eiji Okamoto. "Convertible Undeniable Partially Blind Signature from Bilinear Pairings", 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008 Publication	<1 %
39	Jiangtao Yuan, Jing Yang, Chenyu Wang, Xingxing Jia, Fang-Wei Fu, Guoai Xu. "A New Efficient Hierarchical Multi-secret Sharing Scheme Based on Linear Homogeneous Recurrence Relations", Information Sciences, 2022	<1 %

	Publication	
40	Lecture Notes in Computer Science, 2014. Publication	<1 %
41	Number Theory for Computing, 2002. Publication	<1 %
42	etheses.bham.ac.uk Internet Source	<1 %
43	thesis.cust.edu.pk Internet Source	<1 %
44	www.math.auckland.ac.nz Internet Source	<1 %
45	Springer Proceedings in Mathematics & Statistics, 2015. Publication	<1 %
46	Appala Naidu Tentu, V.Ch. Venkaiah, V. Kamakshi Prasad. "CRT based multi-secret sharing schemes: revisited", International Journal of Security and Networks, 2018 Publication	<1 %
47	Galbraith, S.. "Algebraic curves and cryptography", Finite Fields and Their Applications, 200508 Publication	<1 %
48	Manik Lal Das. "A Key Escrow-Free Identity-Based Signature Scheme without using Secure Channel", Cryptologia, 2010	<1 %

	Publication	
49	hdl.handle.net Internet Source	<1 %
50	Submitted to Royal Holloway and Bedford New College Student Paper	<1 %
51	Submitted to University of Brighton Student Paper	<1 %
52	Submitted to University of Edinburgh Student Paper	<1 %
53	mafiadoc.com Internet Source	<1 %
54	"Advances in Cryptology — CRYPTO' 99", Springer Science and Business Media LLC, 1999 Publication	<1 %
55	Fabian Schillinger, Christian Schindelhauer. "Crucial and Redundant Shares and Compartments in Secret Sharing", 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA), 2020 Publication	<1 %
56	H. Guo. "Enhanced McCullagh-Barreto identity-based key exchange protocols with	<1 %

	master key forward security", International Journal of Security and Networks, 2010 Publication	
57	Liu, M.. "Linear multi-secret sharing schemes based on multi-party computation", Finite Fields and Their Applications, 200611 Publication	<1 %
58	Yan Lin, Hongliang Zhu, Guoai Xu, Guosheng Xu. "Hierarchical secret sharing scheme for WSN based on linear homogeneous recurrence relations", International Journal of Distributed Sensor Networks, 2022 Publication	<1 %
59	dokumen.pub Internet Source	<1 %
60	www.ijser.org Internet Source	<1 %
61	"Elliptic Curves", Springer Nature, 2004 Publication	<1 %
62	Abdul Basit, N Chaitanya Kumar, V. Ch. Venkaiah, Salman Abdul Moiz, Appala Naidu Tentu, Wilson Naik. "Multi-stage multi-secret sharing scheme for hierarchical access structure", 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017 Publication	<1 %

63	Harald Scheid. "Lineare Gleichungssysteme und Vektorräume", Elemente der Linearen Algebra und der Analysis, 2009 Publication	<1 %
64	Jean-Sébastien Coron. "Resistance Against Differential Power Analysis For Elliptic Curve Cryptosystems", Lecture Notes in Computer Science, 1999 Publication	<1 %
65	L. Zhang, B. Huang. "Robust Model Predictive Control of Singular Systems", IEEE Transactions on Automatic Control, 2004 Publication	<1 %
66	Lecture Notes in Computer Science, 2006. Publication	<1 %
67	Lecture Notes in Computer Science, 2015. Publication	<1 %
68	Lijun Yang, Chao Ding, Meng Wu. "Establishing authenticated pairwise key using Pairing-based Cryptography for sensor networks", 2013 8th International Conference on Communications and Networking in China (CHINACOM), 2013 Publication	<1 %
69	Y J Chen. Journal of Physics Condensed Matter, 03/23/1998 Publication	<1 %

70	cs.stackexchange.com Internet Source	<1 %
71	moam.info Internet Source	<1 %
72	www.freepatentsonline.com Internet Source	<1 %
73	Abhik Ghosh, Ayanendranath Basu. "A Scale-invariant Generalization of the R4enyi Entropy, Associated Divergences and their Optimizations under Tsallis' Nonextensive Framework", IEEE Transactions on Information Theory, 2021 Publication	<1 %
74	Sachin Kumar. "Extending boolean operations-based secret image sharing to compartmented access structure", Multimedia Tools and Applications, 2022 Publication	<1 %
75	Submitted to University of Queensland Student Paper	<1 %
76	Submitted to University of York Student Paper	<1 %
77	Wenbo Mao. "Efficient and practical fair exchange protocols with off-line TTP", Proceedings 1998 IEEE Symposium on	<1 %

Security and Privacy (Cat No 98CB36186)
SECPRI-98, 1998
Publication

78	www.ias.ac.in Internet Source	<1 %
79	www.researchgate.net Internet Source	<1 %
80	"Public-Key Cryptography – PKC 2019", Springer Science and Business Media LLC, 2019 Publication	<1 %
81	Atanu Basu, Indranil Sengupta, Jamuna Kanta Sing. "Secured hierarchical secret sharing using ECC based signcryption", Security and Communication Networks, 2012 Publication	<1 %
82	Carlo Blundo, Antonella Cresti, Alfredo De Santis, Ugo Vaccaro. "Fully dynamic secret sharing schemes", Theoretical Computer Science, 1996 Publication	<1 %
83	Chunqiang Hu, Wei Li, Xiuzhen Cheng, Jiguo Yu, Shengling Wang, Rongfang Bie. "A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds", IEEE Transactions on Big Data, 2018 Publication	<1 %

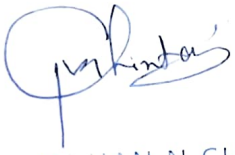
84	Computation Cryptography and Network Security, 2015. Publication	<1 %
85	Handbook of Information and Communication Security, 2010. Publication	<1 %
86	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
87	Yuyin Yu. "A Probabilistic Secret Sharing Scheme for a Compartmented Access Structure", Lecture Notes in Computer Science, 2011 Publication	<1 %
88	Cheng Guo, Chin-Chen Chang, Chuan Qin. "A hierarchical threshold secret image sharing", Pattern Recognition Letters, 2012 Publication	<1 %
89	Submitted to Indian Institute of Technology, Madras Student Paper	<1 %
90	José Luis Gómez Pardo. "Chapter 11 An Introduction to Elliptic Curve Cryptography", Springer Science and Business Media LLC, 2013 Publication	<1 %
91	Submitted to The University of Manchester	

	Student Paper	<1 %
92	midroogcoil.blob.core.windows.net Internet Source	<1 %
93	www.scribd.com Internet Source	<1 %

Exclude quotes On

Exclude bibliography On

Exclude matches < 14 words



Dr. MOHAN N CHINTAMANI
Assistant Professor
School of Mathematics & Statistics
University of Hyderabad
HYDERABAD-500 046. T.S.