DESIGN AND ANALYSIS OF MULTI SECRET SHARING SCHEMES FOR VARIOUS ACCESS STRUCTURES

A thesis submitted during 2021 to the University of Hyderabad in partial fulfillment of the award of a Ph.D. degree in Computer Science

by

ABDUL BASIT

School of Computer and Information Sciences
University of Hyderabad
P.O. Central University, Gachibowli
Hyderabad – 500046, India
Telangana
India

CERTIFICATE

This is to certify that the thesis entitled **Design and Analysis of Multi Secret Sharing Schemes for various Access Structures** submitted by **Abdul Basit** bearing **Reg. No. 14MCPC01** for partial fulfillment of the requirements for the award of **Doctor of Philosophy in Computer Science** is a bonafide work carried out by him under our supervision and guidance.

The thesis is free from plagiarism and 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. The student has the following publications before submission of the thesis for adjudication and has produced the evidence for the same.

1. **New Multi-secret Sharing Scheme based on Superincreasing Sequence for Level-Ordered Access Structure.** *International Journal of Communication Networks and Distributed Systems (IJCNDS), Vol. 24, No. 4*, PP. 357-380, 2020.
2. **Multi Secret Sharing Scheme using modular inverse for Compartmented Access Structure.** *ICDECT 2019, AISC series of Springer* PP. 1-13, 2019.
3. **Multi Stage Multi Secret Sharing Scheme for Hierarchical Access Structure**. *ICCCA 2017, IEEE Xplore*, volume 9, PP. 557-563, 2017.

Further, the student has passed the following courses towards fulfillment of coursework requirement for Ph.D.

Course Code	Name	Credits	Pass/Fail
CS 801	Data Structures and Algorithms	4	Pass
CS 802	Operating Systems and Programming	4	Pass
AI 853	Data Mining	4	Pass
IT 811	Secure Computing	4	Pass

Prof. V. Ch. Venkaiah
Supervisor

Prof. Salman Abdul Moiz
Supervisor

Prof. Chakravarthy Bhagvati
Dean, School of Computer and Information Sciences

DECLARATION

I, **Abdul Basit**, hereby declare that this thesis entitled **Design and Analysis of Multi Secret Sharing Schemes for various Access Structures** submitted by me under the guidance and supervision of **Prof. V. Ch. Venkaiah** and **Prof. Salman Abdul Moiz** 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:

Signature of the Student:

Name: **Abdul Basit**
Reg. No. **14MCPC01**

Acknowledgements

The accomplishment of this doctoral thesis and degree is a result of the collective support and blessings of various people during my journey of Ph.D. I feel overwhelmed and pleased to acknowledge each and everyone for their kind contribution.

The foremost is my supervisor, **Prof. V. Ch. Venkaiah** who has not only taught me science but the facts behind and beyond science. Sir has endowed me with a sacred vision to pursue productive full-time research in computer science. The importance of bearing an optimistic attitude and crystal clear concept of the subject is a boon conferred by sir towards shaping my research questions during my years of Ph.D. I am extremely obliged to sir for making himself always available for rigorous scientific discussions despite his busy schedule. Those insightful inputs by sir are a substantial asset to build the carrier further. I wish to acknowledge sir for being the guiding light in my days of research.

I sincerely gratify my other supervisor, **Prof. Salman Abdul Moiz** for being both amicable and friendly supervisor with whom I was able to share the days of being a research scholar. The periodical scientific counseling and supervision when I was at the initial phase of my Ph.D. carrier are accountably assisted by sir. I genuinely acknowledge sir for taking out his valuable time for undertaking a detailed analysis of the given research problem and giving me precise comments.

I would like to thank my RAC members, **Prof. Vineet Padmanabhan** and **Dr. K Swarupa Rani**, for their valuable suggestions. I extend

admiration to my teachers of Jamia Hamdard, **Prof. Afsar alam** and **Prof. Ranjeet Biswas** for their inspiration to choose computer science as a research field. I would like to honestly praise my colleagues, **Mr. Chaintanya kumar**, **Mrs. Ayang**, **Mr. Abdul salam**, **Mr. GR Anil** and **Mr. Venkat padri** for building an enthusiastic environment and engaging in critical discussions related to research both inside and outside the lab. I thank all my Ph.D. classmates for showering the fun times in hostel day's stay. I am thankful to my best buddies, **Mr. Fiazan Ahmad**, **Mr. Ashrafi iqbal** and **Mr. Ajmal Hussain**, **Mrs. Neetu singh**, **Mr. Gufran**, **Mr. Ajay** for encouraging me whenever some unfavorable situation demands. They have always been appreciating the passion of my profession and unboundedly keeping in touch all times.

I extend the deepest salutation to my whole family members for availing me every needful facility and emotional assistance. Their support imprints me the property to be flexible as water and rigid as rock to balance my twisted research life. I wish to express that I am indebted and owe so much to my mother, **Mrs.Tabassum** and father, **Mr. Abdul Bari** such that my depth of expression acknowledgment will always be small when compared to their contributions of parenting. The unconditional sacrifices and determined motivation are what I have learned from them at every stage of my life and this has enforced me to become a responsible citizen in the first place. With immense pride, this doctoral dissertation is dedicated to my parents for providing me the strong roots to standalone and sustain in such a long journey of life. My deepest thank to my younger brother cum friend **Mr. Abdul Wajid** and **Mr. Abdul Khalid** for believing in me and always makes motivated toward all journey of difficulties.

Finally, I bow to The Almighty for being a source of unknown power and strength in my life.

Abdul Basit

Abstract

Due to advances in technology, automation, and a huge number of electronic communications, the protection of information and its related infrastructure, including the systems and hardware that use, store and transmit has become a big challenge in the computing world. Based on the requirements, various cryptographic algorithms can be used for securing sensitive information. Storing a secret key or sensitive data with one person, server or database reduces the security of the system to the security and credibility of that agent. Besides, not having a backup of the key introduces the problem of losing the key if a software or hardware failure occurs. Secret sharing schemes are designed to address this problem. They are ideal for storing information that is highly sensitive and they achieve arbitrarily high levels of confidentiality and reliability. Secret sharing is a cryptographic primitive, which is used to distribute a secret among a group of participants in such a way that an authorized subset of participants can uniquely reconstruct the secret and an unauthorized subset can get no information about the secret.

In this thesis, we proposed three new secret sharing schemes that realize multipartite as well as multi-stage threshold access structures. The schemes are designed using techniques that employ modular inverse, Lagrange interpolation, superincreasing sequences with special properties and one-way function.

First two of the proposed schemes are based on Polynomial interpolation and the concept of the modular inverse. These schemes realize a hierarchical access structure and compartmented access structure respectively. These two access structures are the special cases of multipartite access structures. The novelty of the first scheme is the secret shares are reusable. If shares are reusable, participants can use the previously distributed shares without

refreshing them for each new secret. And the second scheme can verify whether the reconstructed secret is correct or not.

Next, a new multi secret sharing scheme for Level Ordered Access Structure (LOAS) which differs slightly from the multipartite access structure, is proposed. Further, we have proposed a secret changeable scheme for Level order access structure, wherein the secret can be changed dynamically. This scheme can cater to the dynamic nature of the system.

All the proposed schemes are analyzed for their security as well as for their computational complexity. Comparative analysis with the existing schemes and results are discussed at the end of each chapter in this thesis.

Contents

Chapter 1

Introduction

Information security has become substantially more essential since electronic communications have begun to be used as part of our everyday life. Security is mainly concerned about the secrecy, accessibility, credibility of information stored or communicated. Secret sharing schemes are the methods, which can be used to secure data, in various cryptographic implementations, and to establish other security protocols. Secret sharing is one of the most effective tools to protect highly sensitive information and to keep it secure and confidential, such as encryption and decryption keys, missile launching codes, financial related information, etc. This kind of information must be kept secret because it is vulnerable and the loss of such information may cause heavy damage either to an individual or humanity. Prior to the discovery of secret sharing, multiple copies of crucial information were made and kept in various locations. It was to ensure that the information will be available at least in one of these locations if the information is either lost, harmed physically or damaged by a virus. We are well aware that the more the copies of data, the more vulnerable it is to the security threats. Then the secret sharing scheme evolved to address these issues on a large scale. An illustration of how secret sharing scheme addressed a problem is provided below.

Suppose a group of scientists have come up with a solution to the problem that needs to be kept secret. As a result, the solution is encrypted and the key is stored in a safe place. For the scientists, the solution is so crucial that they can't bear to lose it. That is why they make a few copies of the encryption key and store it in various locations. However, this will increase the risk of the key being stolen. What they actually need to do, is to break the key into bits and store the bits in different

locations. they can also rebuild the key despite the loss of certain bits. If a bit is missing or stolen, they can rebuild a key from the rest of the bits, However, the stolen bits will not be enough to rebuild the key.

1.1 Background and Motivation

In a secret sharing scheme, the secret is divided among all the participants, so that each participant receives a share of the secret. Secret can be reconstructed only when an authorized set of participants pool its shares; with individual shares, the secret will not be recovered. Following are the two primary requirements of a secret sharing scheme.

- **Recoverability:** An authorized subset of participants should be able to get the secret by combining their respective shares.
- **Privacy:** An unauthorized subset of participants should not get any information about the secret.

The first secret sharing schemes were introduced by Shamir [62] and Blakley [11] in 1979, independently. Shamir's scheme is based on the Lagrange interpolation polynomial whereas Blakley's scheme is realised using linear projective geometry. In 1981, Robert and Dilip [52] suggested a secret sharing scheme based on Reed-Solomon code and James L [51] introduced a secret sharing scheme using the linear code. In 1983, a secret sharing scheme proposed by Mignotte [54] defined a sequence and called - the Mignotte sequence. The scheme is based on the Chinese remainder theorem. This has been modified by Charles and Jhon in [3] which leads to another scheme.

Secret sharing scheme is a cryptographic primitive, where a secret is divided into shares. These shares are distributed among the set of participants by a dealer, so that any authorised set of participants can recover the secret by combining their shares, whereas any unauthorised set of participants cannot get any knowledge about the secret. The scheme introduced by Shamir is known as (t, n) threshold secret sharing scheme, where t is the threshold and n is the number of participants. A (t, n) threshold secret sharing scheme allows any t or more than t participants to recover the secret, while it does not allow any less than t participants to recover the secret. Secret reconstruction is based on Lagrange polynomial interpolation of any t or more than t set of private

shares. The following scenario can be solved by a threshold secret sharing scheme which can be illustrated by an example: "To open the vault of a company, multiple people have to work together. The company owner, three managers, and three shift leaders each have a private access code for the vault. As soon as two of the seven people enter their code, the vault can be opened. Each of the n = 7 persons receives a single share, the threshold is t = 2"

The two important characteristics of a secret sharing scheme are ideal and perfect. These concern the efficiency and security of the scheme. Let us suppose that the maximum share length and secret length are the same, then such a secret sharing scheme is known as ideal. In information-theoretic context, the secret sharing scheme is considered as perfect if no knowledge is obtained by unauthorized subset, but an authorized subset acquires complete knowledge about the secret.

The family of all authorized sets, who can recover the secret, is known as an access structure. Γ is the symbol generally used to denote access structures of a secret sharing scheme. The collection of all unauthorized sets, which can not gain any knowledge about the secret, is called adversary structure or forbidden set and it is denoted by $\overline{\Gamma}$. In the literature [31, 44, 69] different types of access structures are proposed based on the context and organizational setup. Examples include generalized access structure, (t, n) threshold access structure, Level ordered access structure and multipartite access structure that includes hierarchical and compartmented access structures. In a (t, n)-threshold access structure, any t or more than t participants constitute an authorized set and any set consisting of less than t participants constitutes an unauthorized set. Symbolically,

$$\Gamma = \{X \in 2^n : |X| \geq t\}$$

$$\overline{\Gamma} = \{X \in 2^n : |X| < t\}$$

where 2^n denotes the power set of the set of participants and $|X|$ denotes the cardinality of the set X. In a threshold access structure, all participants are given equal weightage. An access structure is called monotone, if it satisfies the following:

$$(X \in \Gamma) and (X \subseteq Y) \Rightarrow Y \in \Gamma$$

$$(X \in \overline{\Gamma}) and (Y \subseteq X) \Rightarrow Y \in \overline{\Gamma}$$

If Γ and $\overline{\Gamma}$ are such

$$\Gamma = \{X \in 2^n : |X| = t\} \text{ and}$$

$$\overline{\Gamma} = \{X \in 2^n : |X| = t - 1\}$$

then we say that Γ only contains the minimal authorized sets which can get the secret, $\overline{\Gamma}$ only holds maximal unauthorized sets which can not get the secret.

In a multipartite access structure, the set of participants $\mathcal{P}$ is divided into $m \geq 2$ different sets $L_1, L_2, \ldots, L_m$, which denotes level and all participants in each level plays exactly the same role inside the access structure. The multipartite access structure is further classified into hierarchical (multilevel) and compartmental access structure [29, 40, 41, 70, 74]. Participants across the levels have different weightage and accessibility.

In the multilevel access structure, the set of all participants is partitioned into different levels. These levels create a hierarchical structure, and higher-level participants are more powerful than the lower-level participants. The secret can be reconstructed from the least threshold number of participants at any level. When the number of participating participants at a level is lower than the threshold number of participants, then the remaining participants can be taken from higher levels. For instance, "a bank may require the concurrence of two vice-presidents or three senior tellers to authenticate the National Electronic Fund Transfer (NEFT). If there are only two senior tellers available, the missing one can be substituted by a vice president"

In the compartmented access structure, participants are divided into compartments, so that the cooperation of at least threshold number of participants from all the compartments is required to recover the secret. Consider the example presented by Simmons [64]. "Let two countries agree to control the recovery of the secret (which may initiate a common action) by a secret sharing scheme. The secret can be recreated only if at least two participants from both the compartments pool their shares together".

Another access structure named as a Level-Ordered Access Structure (LOAS) that is different from the existing multipartite access structures was proposed [37, 58, 72]. In Level-Ordered Access Structure (LOAS), a set of participants is divided into different

levels; each level is associated with a threshold, and there is also an ordering imposed upon the levels while reconstructing the secret. This shows that the participants must apply their shares according to the predefined order of the levels to recover the secret. Otherwise, the secret cannot be recovered.

A scheme is known as a one-time use scheme if the shares are not valid after reconstructing the corresponding secret. On the other hand, if shares can be reused for other secrets as well, then the scheme is known as a multi-use scheme. As we know that the distribution of a share must be punctilious, and it is a costly process, therefore multi-use has become an essential property for the secret sharing schemes. We have designed a "multi-secret sharing scheme"with multi-use property in this thesis.

Multi-secret sharing (MSS) scheme is a generalization of a single secret sharing scheme. In an MSS scheme, instead of a single secret, multiple secrets are shared among the participants. The MSS schemes have been studied extensively by the cryptographic community. In these MSS schemes, every participant is required to keep only one share and can be used for as many secrets as desired. In a multi-stage secret sharing scheme, the recovery of the secrets takes place in stage by stage and in a predefined order. Recovery of a secret at an earlier stage does not reveal or weaken the information of the remaining secrets that have not been recovered. In modern days, multi-stage secret sharing scheme plays a vital role; particularly in banking system such as ordering and signing of a cheque, opening bank locker, etc. For example, every bank has a private database. In order to access it, a person is required to pass through different checkpoints specified in a particular order.

1.2 Contributions of the Thesis

Security is a major challenge in the field of digital data storage and transmission. Secret sharing protocols provide solutions to several security problems including secure key management, distributed access control as well as secure multi-party computation. This thesis mainly contributes to the development of secret sharing protocols and also discusses their implementations in typical areas of application.

Major contributions of the thesis are as follows. We have designed three new multi-secret sharing schemes for different access structures based on different mathematical

techniques. In this thesis, we consider the problem of designing multi secret sharing schemes for various application scenarios. Three new multi-secret sharing schemes are proposed that realise different access structures are proposed. They are Hierarchical access structure, Level order access structure and Compartmented access structure.

The first scheme addresses the problem of sharing multiple secrets. It realizes the hierarchical access structure and uses public shift technique and one way function. The resulting scheme is a new hierarchical threshold secret sharing scheme with multi-stage and multi- secret features. In the proposed scheme, multiple secrets are shared in sequential order among the participants. In this multi secret sharing scheme, every participant is required to keep only one share and the share can be used for as many secrets as desired. It has multi-stage feature which means recovery of the secrets is takes place in stages and in a predefined order. Recovery of a secret at an earlier stage does not reveal or weaken the information of remaining secrets that aren't recovered yet. The scheme is computationally perfect, which means that an authorised set can always reconstruct the secret in polynomial time, while this is computationally infeasible for an unauthorised set. The following is a description of the proposed hierarchical scheme:

Let the n participants be partitioned into m levels, $L_j; j \leq 1 \leq m$. Corresponding to each level L_j there is a threshold t_j, $j = 1, 2, \ldots, m$, where L_1 indicates the highest level and L_m indicates the lowest level. A dealer chooses pseudo share $y_i^j, 1 \leq j \leq m$, $1 \leq i \leq n_j$, where n_j, $j = 1, 2, \ldots, m$ denote the number of participants at the j^{th} level L_j. The dealer also chooses the k secrets $S_1, S_2, \ldots, S_k$ and modifies these secrets to become $S_i^{'} = S_i + S_{i+1}$, $1 \leq i \leq k-1$ and $S_k^{'} = S_k$. Shares are then generated corresponding to $S_i^{'}, i = 1, 2, \ldots, k$, using a polynomial function. Public shares are generated by adding these shares to the one-way function of the chosen pseudo shares. These public shares are then published and the pseudo shares are distributed through a secure channel to the participants. While reconstructing the secrets, the participants compute their true shares by subtracting the image of one-way function of their pseudo shares to the corresponding public value. Then Lagrange interpolation is used to reconstruct the modified secret S_i'. Actual secret S_{i-1} is then recovered by subtracting the previously reconstructed secret S_i. These secrets can be recovered stage by stage at any level L_j, only if the number of shares available are greater than or equal to the threshold value

t_j. If the number of shares available at any level L_j is less than the threshold value t_j then participants from a higher level $L_i, (i < j)$, can contribute the remaining shares to recover the secrets.

Next, we have proposed a secret sharing method that realises a special case of the multipartite access structure in the thesis. The proposed scheme realizes a compartmented access structure. The main characteristic of this scheme is that, the reconstructed secret can verify whether the recovered secret is correct or not. This is a multi secret sharing scheme and is based on the concept of modular inverse. No participant in a compartment knows the secrets of the other compartment. The proposed secret sharing scheme applies Shamir's scheme first to recover compartment secrets and combines them into the requested secret. The scheme is ideal as well as perfect. The proposed scheme can be applied in the following situation: Suppose an organisation works on a confidential project. The management divides the project into different modules to make work easier and for on time delivery. Each module is given to different teams, where each team consists of a set of employees. In order to achieve the project's confidentiality, they can use any encryption scheme, but applying an encryption scheme and having the key for each employee is a time consuming and costly process with the risk of key losses. Therefore, instead of using encryption scheme for every employee, it can distribute the key to the employees of each team by using the proposed scheme. The following is a description of the proposed compartmented scheme:

In the beginning, the dealer has a set $\mathcal{P}$ of n number of participants $p_1, p_2, \ldots, p_n$. The participants are divided into m disjoint compartments $C_1, C_2, \ldots, C_m$ and the dealer selects a set of m co-prime integers $c_1, c_2, \ldots, c_m$ as the corresponding compartment secrets. The dealer will compute partial secrets ℓ_i using compartment secrets $c_i, 1 \leq i \leq m$ and adds all the partial secrets ℓ_i to get pseudo secret $s = \sum_{i=1}^{m} \ell_i$. Then calculates shift values Z_j by applying pseudo secret s to actual secret S_j. That is, $Z_j = s + S_j$, $1 \leq j \leq k$ and makes it public. The dealer now applies the Shamir's secret sharing scheme to distribute shares of the compartment secrets c_i to the participants of corresponding compartments C_i. While reconstructing the secret, the participants of the corresponding compartment first apply Lagrange interpolation and recover the corresponding compartment secrets c_i. They compute partial secret ℓ_i at corresponding compartments and add all partial secrets ℓ_i to get pseudo secret s. Then to recover

actual secrets S_j, subtract pseudo secret from the corresponding shift values Z_j, which are public values. That is, $S_j = Z_j - s$.

Another secret sharing scheme proposed that realizes Level order access structure(LOAS). The level order access structure is a sort of multipartite access structure which is required to follow the ordering. In the software industry, an application can be released for delivery only after it has undergone unit testing, followed by integration testing, system testing and finally acceptance testing. It should be noted that integration testing can not be started without completing the unit testing. Likewise, System testing cannot begin before the integration testing is completed, and so on. That is the significance of the ordering. This scenario fails to realise in the existing access structures since it can not execute the required ordering concept. In order to carry out this or similar type of application scenario, there is a need of an access structure which has applied ordering among the levels. The aim of this study is to propose a scheme that addresses these types of scenarios and design a scheme which enforces ordering for the multiple secrets. The proposed scheme is based on the subset sum problem and it uses a superincreasing sequence. Our scheme supports the property of secret changeability without changing the compartment secret shares. which makes our scheme more efficient during the share distributed phase. The proposed scheme is reusable in nature, which means that the participants shares can remain the same and can be reused for a new secret and hence it avoids communication overhead during share distribution phase. The actual secret can be recovered only after recovery of all the compartment secrets along with maintaining the order among the levels.

Security analysis and comparative analysis with the existing scheme of all the schemes proposed in this thesis has been carried out and it is presented at the end of the corresponding scheme. Comparative analysis of the proposed schemes with the existing scheme is also presented.

1.3 Importance of the work

Security of information has proved significantly more important as electronic communication is becoming a part of our day-to-day life. However, irrespective of the algorithms used, security realize on the secrecy of a key that should be known to the owner in any case. The prerequisite of the secret key being secret brings in a lot of issues. Putting a

secret key with one or more servers/databases decreases the security of the system. In case, if a software / hardware malfunction occurs, it presents the issue of losing a key. Subsequently, the keys used as a part of the area that involve critical confidentiality such as large-scale finance applications, specifically in the banking sector and control mechanisms in nuclear systems.

On the basis of the organizational structure/context, many secret sharing schemes are designed that gives conditional and unconditional security. Several secret sharing schemes are proposed for sharing multiple secrets. In this thesis, we consider the problem of designing multi secret sharing schemes for different application scenarios. Three new multi secret sharing schemes that realize different access structures are proposed. They are Hierarchical access structure, Level order access structure and Compartmented access structure. The proposed schemes are evaluated in terms of security parameters like idealness, perfectness, computationally perfectness and probabilistic perfectness.

1.4 Structure of the Thesis

The thesis is organized into seven chapters.

In Chapter 1, brief description of the topic, importance of the work and arrangement of the thesis is presented.

In Chapter 2, review the important mathematical primitives and basic cryptographic preliminaries, related to threshold schemes, that are used for the construction of our schemes.

In Chapter 3, presented a literature survey of the proposed work, motivation behind it, problem identification and methodology of the proposed work.

In Chapter 4, proposed multi stage multi secret sharing schemes that realize hierarchical access structure. Security analysis of the scheme and comparisons with the existing schemes are also presented in this chapter.

In Chapter 5, proposed a multi secret sharing scheme using modular inverse for compartmented access structure. Security analysis of the scheme and comparisons with the existing schemes are also presented in this chapter.

In Chapter 6, presented a scheme which is a new multi secret sharing scheme based on superincreasing sequence for Level-ordered access structure having threshold changeability feature. We analyzed the scheme for its security as well as for its advantages in comparison with the other schemes. We have also discussed applications of multi secret sharing schemes and implementations of the proposed multipartite secret sharing schemes.

In Chapter 7, the concluding remarks of the research work and future work are presented along with the, further extensions and future directions of the proposed scheme.

1.5 Publications

1. **New Multi-secret Sharing Scheme based on Superincreasing Sequence for Level Ordered Access Atructure.** *In International Journal of Communication Networks and Distributed Systems (IJCNDS) pp. 357-380, 24.4 (2020):* (Scopus, ESCI, DBLP Indexed)

2. **Multi-secret Sharing Scheme Using Modular Inverse for Compartmented Access Structure.** *In International Conference on Data Engineering and Communication Technology (ICDECT) pp. 371-385, AISC, Springer, 2019.* (Scopus Indexed)

3. **Multi-stage Multi-secret Sharing Scheme for Hierarchical Access Structure.** *In International Conference on Computing, Communication and Automation (ICCCA), pp. 557-563. IEEE, 2017.* (Scopus Indexed)

Paper Presentations

1. **Multi-secret Sharing Scheme based on Superincreasing Sequence.** *In National Workshop on Cryptology (NWC)- 2018, at "CR RAO Advanced Institute*

of Mathematics, Statistics and Computer Science, Hyderabad".

2. **Multi-secret Sharing Scheme & Various Access Structures.** *In National Instructional Workshop on Cryptology (NIWC)- 2018, at Department of Mathematics, MNIT Allahabad.*

3. **Sequential Multi-secret Sharing Scheme for Multilevel Access Structure.** *In National Workshop on Cryptology (NWC)- 2017, at Department of Computer Science and Engineering, NIT Tiruchirappalli.*

Chapter 2

Preliminaries

This chapter introduces preliminaries required for our proposed schemes. These include Shamir's (t, n) threshold secret sharing scheme, Multi-stage multi-secret sharing scheme and different access structures. We begin by discussing some of the basic concepts from basic number theory, field theory then a complete taxonomy of other fundamental preliminaries of various secret sharing schemes and access structures.

2.1 Mathematical Primitives

Recall that a ring with identity is a set R with two composition laws + and $\cdot$ such that

- $(R, +)$ is a commutative group
- $(R, \cdot)$ is associative, and there exists an element 1_R such that $x \cdot 1_R = 1_R \cdot x = x$, $\forall x \in R$
- The distributive laws holds: for all $x, y, z \in R$,
  $(x + y) \cdot z = x \cdot z + y \cdot z$
  $x \cdot (y + z) = x \cdot y + x \cdot z$

Let I be an ideal for a ring R. Then R/I, together with the operations in coset multiplication and addition, makes a ring. The ring R/I is called a **quotient ring** of R.

To satisfy the following, a field is a finite set F of two binary operation, multiplication modulo (*cdot*) and addition modulo (+).

- $(F, +)$ is an abelian group, with 0 as an identity element.
- $(F^*, \cdot)$ is an abelian group, with 1 as the identity element (F^* denotes $F\backslash\{0\}$)
- For all $x \in F$ then $0 \cdot x = x \cdot 0 = 0$
- For all $x, y, z \in F$, distributive property holds $x \cdot (y + z) = x \cdot y + x \cdot z$

Recall the notion of a vector space under multiplication and addition modulus of binary operations in a field. A $n - dimensional$ vector space over the finite field F_q of q has cardinality q^n (and is finite in particular).

Finite field F_q

Most of our work is based on the simplest finite field Z_q or F_q, where q is a prime number. Take $q \in Z$ as a prime set of integers and $F_q = Z/qZ$ denotes a quotient ring. Explicitly, $F_q = 0, 1, \ldots, q - 1$, and the operations are multiplication and addition of integer modulo q .

2.2 Lagrange Polynomial Interpolation (LPI)

Lagrange polynomial interpolation is one of the simplest mathematical tool used to design a secret-sharing protocol, although there are various other mathematical tools exists in the literature to design a secret-sharing protocol, but among them it is more simple and less computation. In polynomials, two characteristics are very common as follows:

- The polynomial can be used to draw a curve through the polynomial points.
- A fixed-degree polynomial can be determined if we know the values that this polynomial takes on as many points as its degree plus one.

The following observations are made from the below figure 2.1

- Two points determine a single line i.e. a polynomial of degree 1.
- Three points determine a parabola i.e. a polynomial of degree 2.
- Similarly, using $n + 1$ points, a polynomial of degree n can be determined.

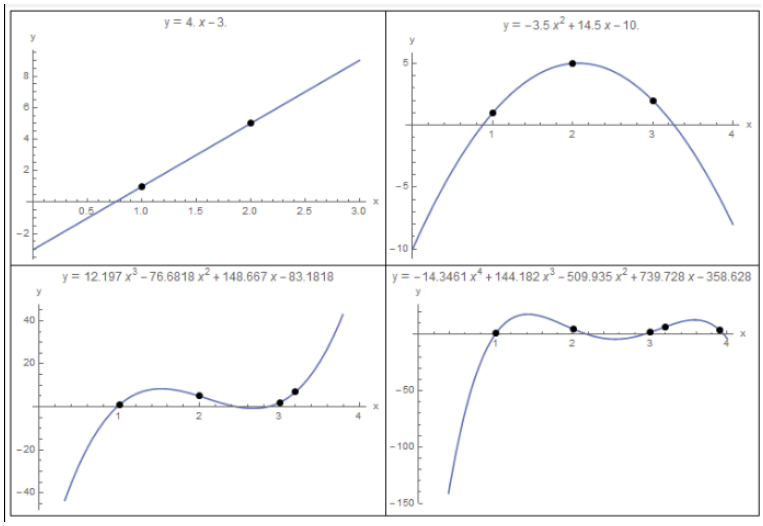

Figure 2.1: Polynomial Interpolation for 2, 3, 4 and 5 data points

There are various techniques of interpolation that exists in the literature. The Interpolation of Lagrange is one of the techniques used in the secret sharing scheme of Shamir. For example, consider to determining the interpolating polynomial of the following data using Lagrange interpolation : $(1,1),(2,5),(3,2)$. The interpolating formula of Lagrange is as follows:

$$f(x) = \sum_{i=1}^{n} L_i y_i \;\; where \;\; L_i = \prod_{j=1, j\neq i}^{n} \frac{x - x_j}{x_i - x_j}$$

and y_i is the function value at x_i. So in our example, we have

$$f(x) = L_1 y_1 + L_2 y_2 + L_3 y_3$$

$$= \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} \times y_1 + \frac{(x-x_2)(x-x_1)}{(x_2-x_1)(x_2-x_3)} \times y_2 + \frac{(x-x_1)(x-x_2)}{(x_3-x_2)(x_3-x_1)} \times y_3$$

$$= \frac{(x-2)(x-3)}{(1-2)(1-3)} \times (1) + \frac{(x-1)(x-3)}{(2-1)(2-3)} \times (5) + \frac{(x-1)(x-2)}{(3-1)(3-2)} \times (2)$$

$$= -3.5 \times x_2 + 14.5 \times x - 10 \qquad (1)$$

Thus, (1) is the interpolating polynomial of the given data.

Theorem: Given t points are in the 2-D plane $(x_1, y_1), \ldots, (x_t, y_t)$ with distinct

$x_i's$, there is only one polynomial $f(x)$ of degree $t-1$, such that $y_i = f(x_i)$, $\forall i$.
$f(x) = a_0 + a_1 \times x + \cdots + a_{t-1} \times x^{t-1}$, where $f(0) = a_0 = secret$

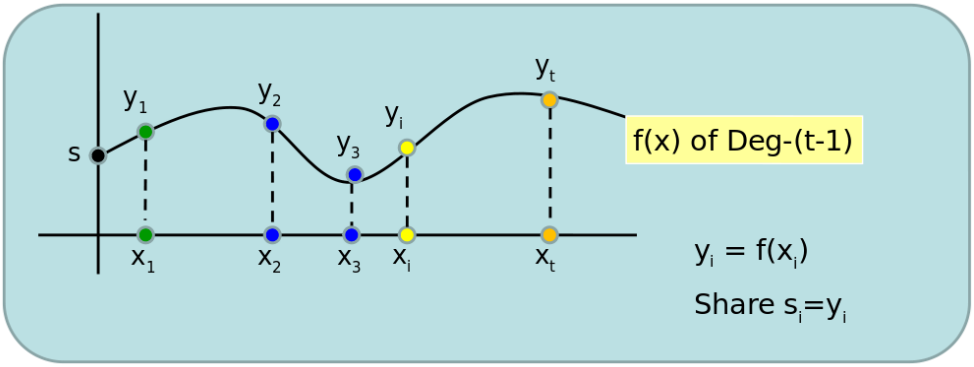

Figure 2.2: Polynomial Interpolation f(x) of deg-(t-1)

- Given t points, the polynomial $f(x)$ can be construct using Lagrange interpolation formula:

$$f(x) = \sum_{i=1}^{t} y_i \times (\prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j})$$

2.3 Preliminaries of Threshold Cryptography

A secret is something that is confidential, sensitive and needs protection against breaches of confidentiality.

A secret sharing scheme is a method, in which a secret is shared among a group of participants as their shares. The secret can be recovered only when, the shares of an authorised group of participants are combined together; unauthorised subset of a group or out of the group absolutely gets no information about the secret. A common (t, n) threshold scheme is the following:

1. If there is t or more than t participants provide their shares, then the secret S can be reconstructed.

2. If $t-1$ or lesser number of participants provide their shares then the secret S remains completely undetermined. Here t is the threshold and n is the number participants of the group with $t \leq n$.

In general, measuring the efficiency of a secret sharing scheme is in terms of information rate and perfectness. The chosen secret key (k) (or secret) belongs to key space which is a finite set K that can consider by a bit-string of length $log_2|K|$. The size of the shares s_i received by a participant is represented by a bit-string of length $log_2|s_i|$. It lies information rate is defined as:

$$InformationRate \quad R_i = \frac{log_2|K|}{max\{log_2|s_i|\}}$$

A secret sharing scheme is known as ideal if the information rate of a scheme is equal to one. It means that the maximal length of the shares are identical to that of the secret. Information entropy $H(S)$, where S is the secret information, is the uncertainty about the secret. This indicates exactly, how much information about the secret can be revealed by the shares of the participants. A secret sharing scheme is referred to be perfect if it is ideal and no information about the secret can be obtained by an unauthorized group or adversary. Formally, for the case of (t, n) threshold scheme.

1. If t or more number of participants can reconstruct the secret and A defines the set of shares of an authorized set, then $H(S|A) = 0 : \forall A \; such \; that \; |A| \geq t$

2. If B denotes the set of shares of an unauthorized set of $t-1$ or less number of participants, then $H(S|B) = S : \forall B, \; such \; that \; |B| \leq t-1$

   A scheme is not ideal means that the length of a longest share is not equal to the length of the secret or information rate is not equal to one. A scheme which is not ideal is referred to as a ramp scheme. There are two types of ramp schemes; strong and weak ramp secret sharing schemes. Strong ramp scheme reveals no information about the secret for an unauthorized group of $t-1$ or less participants, whereas weak ramp schemes may reveal partial information about the secret.

2.4 Knapsack functions:

A well-known problem in Algorithms is the subset sum problem, also known as the 0-1 knapsack problem.

Subset Sum Problem: Let S be a set of numbers and let N be another number. Then the subset sum problem is to find a subset of the set S, whose sum is equal to N.

Superincreasing sequence: A sequence $x_1, x_2, x_3, \ldots x_r$ of the numbers is considered as superincreasing sequence, if each element of the sequence is larger than the sum of the preceding elements. A tuple is called superincreasing, if its members constitute a superincreasing sequence. Thus a tuple $x = [x_1, x_2, x_3, \cdots, x_r]$ is superincreasing if and only if $x_j > x_1 + x_2 + x_3 + \cdots x_{j-1}$ for every j such that $2 \leq j \leq r$. In other words,

$$x_j > \sum_{i=1}^{j-1} x_i$$

In general, the subset sum problem is NP-hard. However, if the elements of the set S form a superincreasing sequence, then the algorithm 2, which is linear time algorithm (in the number of elements of S) can solve the subset sum problem [53].

We now define two functions *bag_sum* and *bag_inverse* which are useful in our scheme. *bag_sum* takes two r-tuples x and s as the input and returns sum as output, where $x = [x_1, x_2, x_3, \cdots x_r], x_i$ is an integer, $s = [s_1, s_2, s_3, \cdots s_r]$ such that $s_i = \{0, 1\}$ for $1 \leq i \leq r$, and $sum = \sum_{i=1}^{r} x_i s_i$. That is,

$sum = bagsum(x, s)$

$$= \sum_{i=1}^{r} x_i s_i = x_1 s_1 + x_2 s_2 + x_3 s_3 + \cdots + x_r s_r$$

bagsum_inverse takes the tuple x and the sum value as input and returns as output Boolean tuple s, i.e., $s = bagsum\_inverse(sum, x)$.

Given x and s, it is easy to find *bagsum*, but given *sum* and x, it is difficult to find s. However, if the elements of x form a superincreasing sequence, it is easy to compute the boolean value vector s using the function *bagsum_inverse* [53].

Following are the *bagsum* and *bagsum_inverse* pseudo codes of superincreasing sequence case:

The running time of *bagsum* is $\mathcal{O}(r)$ and running time of *bagsum_inverse* is also the same as *bagsum*, that is $\mathcal{O}(r)$. In our proposed scheme, both the algorithms are

Algorithm 1: *bagsum* function

function *bagsum* (x, s);
Input : Two r tuples: $x = [x_1, x_2, x_3, \cdots x_r]$ and $s = [s_1, s_2, s_3, \cdots s_r]$.
Output: *sum*: an integer.
$j \leftarrow 1$, $sum \leftarrow 0$;
while $(j \leq r)$ **do**
    $sum \leftarrow sum + x_j \times s_j$;
    $j \leftarrow j + 1$;
return *sum*;

Algorithm 2: *bagsum_inverse* function for superincreasing tuple

function *bagsum_inverse* (sum, x);
Input : An integer *sum* and tuple $x = [x_1, x_2, x_3, \cdots x_r]$.
Output: Boolean Tuple: $s = [s_1, s_2, s_3 \cdots s_r]$.
$j \leftarrow r$;
while $(j > 1)$ **do**
    if $sum \geq x_j$ **then**
        $s_j \leftarrow 1$;
        $sum \leftarrow sum - x_j$;
    else
        $s_j \leftarrow 0$;
    $j \leftarrow j - -$;
return $[s_1, s_2, s_3 \cdots s_r]$;

employed by the compartments during the secret reconstruction phase.

We have used *exor* function to enhance the security of our proposed scheme by keeping the original secret hidden from compartments. The *exor* function takes two binary matrices s and e of equal length as inputs and performs Bitwise *xor* of them, with the resultant binary matrix s' as the output.

2.5 Modular inverse

Consider the m tuples $c_1, c_2, c_3, \ldots, c_m$ such that the elements in the tuple are pairwise co-prime. Then there exists an unique tuple $L = (l_1, l_2, l_3, \ldots, l_m)$ such that $\frac{l_1}{c_1} + \frac{l_2}{c_2} + \frac{l_3}{c_3} + \cdots + \frac{l_m}{c_m} + \frac{1}{c}$ is always an integer, where $c = c_1 \times c_2 \times c_3 \times \cdots \times c_m$. A proof of this statement is as follows:
Let $c_1, c_2, c_3, \ldots, c_m$ be a set of positive pairwise co-primes and $c = c_1 \times c_2 \times c_3 \times \cdots \times c_m$. That is,

$$\Rightarrow gcd(c_i, c_j) = 1 \quad \forall i \neq j$$

$$\Rightarrow gcd(\frac{c}{c_i}, c_i) = 1 \quad \forall i$$

$$\Rightarrow gcd(\frac{-c}{c_i}, c_i) = 1 \quad \forall i$$

$$\Rightarrow \exists l_i | l_i \equiv (\frac{-c}{c_i})^{-1} \ mod \ c_i \quad \forall i$$

$$\Rightarrow l_i(\frac{-c}{c_i}) \equiv 1 \ mod \ c_i \quad \forall i$$

$$\Rightarrow l_i(\frac{c}{c_i}) \equiv -1 \ mod \ c_i \quad \forall i$$

$$\Rightarrow l_i(\frac{c}{c_i}) + 1 \equiv 0 \ mod \ c_i \quad \forall i$$

Let $l_i \equiv (\frac{-c}{c_i})^{-1} \bmod c_i$, $\forall i, 1 \leq i \leq m$ and

$s = l_1(\frac{c}{c_1}) + l_2(\frac{c}{c_2}) + l_3(\frac{c}{c_3}) + \cdots + l_m(\frac{c}{c_m}) + 1$

$\Rightarrow s \equiv l_i(\frac{c}{c_i}) + 1 \equiv 0 \mod c_i, \forall i$

$\Rightarrow s \equiv 0 \mod c$. That is, $l_1(\frac{c}{c_1}) + l_2(\frac{c}{c_2}) + l_3(\frac{c}{c_3}) + \cdots + l_m(\frac{c}{c_m}) + 1 \equiv 0 \mod c$

$\Rightarrow \exists k | l_1(\frac{c}{c_1}) + l_2(\frac{c}{c_2}) + l_3(\frac{c}{c_3}) + \cdots + l_m(\frac{c}{c_m}) + 1 = kc$

$\Rightarrow \exists k|(\frac{l_1}{c_1}) + (\frac{l_2}{c_2}) + (\frac{l_3}{c_3}) + \cdots + (\frac{l_m}{c_m}) + \frac{1}{c} = k$

2.6 One way function

A one-way function is a function in cryptography that can be easily determined on each input, but is difficult to convert given the image of a random input. Formally, a function $f : \{0,1\}^* \implies \{0,1\}^*$ is called one way function when there is an algorithm of polynomial time which can calculate the function f, except for each random algorithm. Such that,

$$Pr[f(A(f(x))) = f(x)] < \frac{1}{p(n)}$$

For sufficiently large integer n and for each polynomial $p(n)$, such that $n = x$, and an adversary function A. Where the probability of choosing x from the uniform distribution in $\{0,1\}^n$ with the randomness of the algorithm. The advantage of One-way functions are easy to calculate, but their reverse functions are very hard to calculate. Therefore with the data x, it is easy to calculate value of $f(x)$ but on the other hand, knowing the $f(x)$ value and calculating the value of x is very hard. One way functions are key components of various tools that are used in modern cryptography. Such "functions are part of a very significant set of cryptographic primitives. A characteristic of the one-way functions is that, any probabilistic polynomial time algorithm tries to invert an one way function, succeeds with only negligible probability, where the probability refers to the elements within the functions" domain. One-way function are used in the proposed scheme to calculate actual shares.

2.7 Two variable One way function

A tuple $F(r, S)$ is a two-variable one-way function, which maps a random value r and S on fixed length. It has the following characteristics:

- If r and S are given, $F(r, S)$ is easily computed, however it is very difficult to calculate r for given S and $F(r, S)$.
- It is difficult to compute $F(r, S)$, when there is no knowledge of S for any r.

- Given S, it is difficult to find two distinct values r_1 and r_2, which satisfy the condition $F(r_1, S) = F(r_2, S)$.
- It is difficult to compute S, for the given r and $F(r, S)$ values.
- It is difficult to find $F(r^{'}, S)$ where $r^{'} \neq r_i$, having pairs of r_i and $F(r_i, S)$.

2.8 Secret sharing scheme

A secret sharing scheme (SSS) is a method in which a secret is divided into shares. These shares are distributed among a set of participants by a dealer, so that any authorised set of participants can recover the secret by combining their shares, whereas any unauthorised set of participants cannot get any knowledge about the secret. The first SS schemes were introduced by Shamir [62] and Blakley [11] in 1979 independently. Shamir's scheme is based on the standard Lagrange polynomial interpolation while Blakley's scheme is realised based on the concept of linear projective geometry. Their schemes are known as (t, n) threshold secret sharing scheme, where t is the threshold and n is the number of participants. A (t, n) threshold secret sharing scheme allows any t or more than t participants to recover the secret, while it does not allow any less than t participants to recover the secret.

2.8.1 Shamir's (t,n) threshold secret sharing scheme

Shamir proposed a (t, n) threshold scheme "based on polynomial interpolation". In Shamir (t, n) secret sharing scheme, a trusted dealer generates n secret shares based on a $(t-1)^{th}$ degree polynomial. Secret reconstruction is based on Lagrange polynomial interpolation of any t or more than t private shares. A secret sharing scheme is ideal if the maximal length of the shares is same as that of the secret. If the set of shares corresponding to an unauthorized set provides no information and the set of shares corresponding to an authorized set gives all the information of a secret, in a information-theoretic context, then the scheme is perfect.

Let there be a dealer D and the participants n. The dealer distribute the shares of secret to all the participants and the secret can be retrieved by collecting the shares from t or more than t participants during reconstruction. The scheme consists of three phases: Initialization phase where the dealer initializes the value, Share distribution

phase where the dealer computes shares from the polynomial and securely distributes them to the corresponding participants, and secret reconstruction phase where at least threshold number of participants is required to collaborate to reach the corresponding interpolation polynomial and get the secret recovered. The following is an overview of the scheme:

Algorithm: Shamir's (t, n) SS scheme [62]

- *I. Initialization Phase:*
  - The dealer chooses a secret S to share among the participants. Let n be the number of participants $\{p_1, p_2, p_3, \ldots, _n\}$ and $\mathsf{Z}_q(q$ prime) denote the finite field. Further, let $t(\leq n)$ be the threshold and i be the participant public identity p_i, where $i \in \{1, 2, 3, \ldots, n\}$.
- *II. Distribution Phase:*
  - Select a secret S from Z_q.
  - Choose $t-1$ coefficients $a_1, a_2, \ldots a_{t-1}$ randomly from Z_q.
  - Construct a $(t-1)^{th}$ degree polynomial as $f(x) = a_0 + a_1 \times x^1 + \cdots + a_{t-1} \times x^{t-1}$, where $f(0) = a_0$ is secret.
  - Calculate the shares (i, y_i), $i \in \{1, 2, 3, \ldots, n\}$.
    where $y_i = f(i) \bmod q$.
  - Distribute y_i as the participants share to the i^{th} participant.
- *III. Reconstruction phase:*

  Given any authorised subset of t or more than t shares, the coefficients of a polynomial $f(x)$ can be determined by using Lagrange interpolation as following:
  - Using any t distinct shares $(x_0, y_0), (x_1, y_1), \cdots, (x_i, y_i), \cdots, (x_t, y_t)$.
  - Calculate

$$f(x) = \sum_{i=0}^{t} y_i \times l_i(x) \bmod q$$

where Lagrange's coefficients are,

$l_i(x) = \prod_{j=0, j\neq i}^{t} \frac{x-x_j}{x_i-x_j}$

– Now, from the above polynomial $f(x)$, the constant term a_0 is the secret S.

Correctness: "If any t participants or more than that combine their shares together, can get the secret uniquely".

Privacy: Any $t-1$ participants or less than that can not learn anything about the secret.

2.8.1.1 Baby Example of Shamir Secret Sharing Scheme

I. Share Distribution Phase:

- Suppose, the number of participants, $n = 5$, threshold, $t = 3$ and choose secret, $S = 3$
- Choose $q = 17$ and $x_i = i, 1 \leq i \leq 5$
- Choose the random coefficients $a_1 = 14, a_2 = 15$
- The coefficient $a_0 = S = 3$ is the secret.
- Choose 2^{nd} degree polynomial such that, $f(x) = a_0 + a_1 \times x + a_2 \times x^2$
- Hence, the polynomial is $f(x) = 3 + 14 \times x + 15 \times x^2$
- Calculate the shares $y_i = f(x_i) \bmod q$ and distribute to the corresponding participants p_i, where $i = 1, 2, \ldots, 5$. $y_1 = f(1) = 15, y_2 = f(2) = 6, y_3 = f(3) = 10, y_4 = f(4) = 10, y_5 = f(5) = 6$

II. Secret Reconstruction Phase:

- Any t participants or more than that can recover the secret by using Lagrange polynomial interpolation.
- Suppose, 3 participants p_1, p_2, p_3, willing to recover the secret with their shares $(1, 15), (2, 6), (3, 10)$ respectively.

- The lagrange interpolation formula yields:

$$f(0) = \sum_{i=1}^{3} y_i \times (\prod_{k=1, k\neq i}^{3} \frac{k}{k-i}) \mod q$$

$f(0) = 15 \times (\frac{2}{2-1})(\frac{3}{3-1}) + 6 \times (\frac{1}{1-2})(\frac{3}{3-2}) + 10 \times (\frac{1}{1-3})(\frac{2}{2-3}) \mod 17$
$= 37 \mod 17 = 3$ (Secret)

2.8.2 Multi secret sharing scheme

Multi secret sharing (MSS) scheme is a generalization of single secret sharing scheme. In MSS scheme, multiple secrets are shared among the participants. Multi secret sharing have been studied extensively by the cryptographic community. In these MSS schemes, every participant requires to keep only one share and it can be used for as many secrets as desired. In a multi-stage SSS,the recovery of the secrets is stage by stage and in a predefined order. Recovery of a secret at an earlier stage does not reveal or weaken the information of remaining secrets that have not been recovered. In modern days, multi-stage secret sharing schemes plays a vital role; particularly in banking systems such as ordering and signing of a cheque, opening bank safes, etc. For example, every bank has a private database. In order to access it, a person is required to pass through different checkpoints specified in a particular order.

2.8.3 Multi-stage Multi-secret sharing scheme

He and Dawson[38] introduced stage by stage reconstruction of secrets in a predetermined order, which is known as multi-stage multi-secret sharing scheme. They used the concept of public shift technique to hide the actual shares and successive applications of a one-way function to reconstruct the secret in stage by stage. The scheme uses the Shamir's secret sharing scheme. The scheme's overview is as follows:

Choose k secrets S_i, $1 \leq i \leq k$, n distinct values x_i as the shareholder public information $1 \leq i \leq n$, f is a one-way function and choose prime as q.

- **I. Distribution Phase:**

  1. Choose randomly n secret shadows $y_1, y_2, \ldots, y_n$ such that $y_i \in \mathsf{F_q}$, $1 \leq i \leq n$.

2. for $i = 1 \rightarrow k$ do
   - Construct a polynomial $F_i(x)$ of order $(t-1)$ and select $F_i(0) = S_i$.
   - for $j = 1 \rightarrow n$ do
     - calculate actual shares $Z_{ij} = F_i(x_j)$
     - calculate shift value $d_{ij} = Z_{ij} - f^{i-1}(y_j)$
3. Deliver y_i to each participant over secure channel and publish all $d_{ij}, \forall j, i$ where $1 \leq j \leq n$, $1 \leq i \leq k$

- **II. Reconstruction phase:**
  - Any t or more than t participants can produce their pseudo shares to recover the secrets using the below steps:
  - for $i = k \rightarrow 1$ do

$$S_i = F_i(0) = \sum_{j=1}^{t} (f^{i-1}(y_j) + d_{ij}) \prod_{a=1, a \neq j}^{t} \frac{x_a}{x_a - x_j}$$

  - The secrets are recovered in the predefined order: $S_k, S_{k-1}, \cdots, S_1$.

2.8.4 CRT based secret sharing scheme

Asmuth Bloom's scheme

Let threshold t and set of participant n be two positive integers and Asmuth-bloom sequence are chosen as a sequence of pairwise co-prime positive integers p_0 and $p_1 < p_2 < \cdots < p_n$. such that

$$\prod_{i=1}^{t} p_i > p_0 \prod_{i=0}^{t-2} p_{n-i}$$

and $gcd(p_0, p_i) = 1 \ \forall i, i = 1$ to n

Sharing a secret S among the set of n participants based on Asmuth-bloom sequence is as follows:

- **Share Generation Phase:**
  - The secret S is chosen as a random integer $S \in Z_{p_0}$.

- Select an arbitrary number γ such that"

$$p_0 \prod_{i=0}^{t-2} p_{n-i} < (S + \gamma \times p_0) < \prod_{i=1}^{t} p_i"$$

- Calculate shares I_i as

$$I_i = X = (S + \gamma \times p_0) \bmod p_i, 1 \leqslant i \leqslant n$$

- Distribute shares $I_i, 1 \leq i \leq n$ to participants.

- **Share Reconstruction Phase:**

  - Given any t or more than t participant's shares $I_1, I_2, \ldots, I_t$. The modified secret X can be calculated using Chinese remainder theorem, as the unique solution modulo $p_1, p_2, \ldots, p_t$.

$$X = I_i \bmod p_i, 1 \leq i \leq t$$

  - The original secret can be calculated as $S = X \bmod p_0$

  Correctness: If any t participants or more than that combine their shares together, can get the secret uniquely.

  Privacy: "Any $t-1$ participants or less than that cannot learn anything about the secret".

- **Example**

  "The scheme is illustrated with the following example:

  - Consider a $(3, 5)$ Asmuth Bloom sequence
  - Let the sequence of pairwise co-prime positive numbers $p_1 = 11, p_2 = 13, p_3 = 17, p_4 = 19, p_5 = 21$ *and* $p_0 = 5$
  - Choose the secret $S = 3$
  - Calculate $= p_0 \times p_5 \times p_4 = 1995$
  - Calculate $= p_1 \times p_2 \times p_3 = 2431$
  - Choose $\gamma = 421$ such that $S + \gamma \times p_0 = 2108 \in (1995, 2431)$

- Shares are calculated as $I_i = (S + \gamma \times p_0) \bmod p_i, 1 \leq i \leq 5$
  $I_1 = (S + \gamma \times p_0) \bmod p_1 = 2108 \bmod 11 = 7$
  $I_2 = (S + \gamma \times p_0) \bmod p_2 = 2108 \bmod 13 = 2$
  $I_3 = (S + \gamma \times p_0) \bmod p_1 = 2108 \bmod 17 = 0$
  $I_4 = (S + \gamma \times p_0) \bmod p_1 = 2108 \bmod 19 = 18$
  $I_5 = (S + \gamma \times p_0) \bmod p_1 = 2108 \bmod 21 = 8$
- Suppose participants $1, 2$ *and* 3 try to recover the secret. Then the system of equations are as follows:
  $X \equiv I_1 \bmod p_1 = 7 \bmod 11$
  $X \equiv I_2 \bmod p_2 = 2 \bmod 13$
  $X \equiv I_3 \bmod p_3 = 0 \bmod 17$
- By applying CRT, the unique solution for the above equation is obtained as $X = 2108$
- The main secret is $S = X \bmod p_0 = 2108 \bmod 5 = 3$"

2.9 Terminology

2.9.1 Access structure

The family of all authorised subsets, who can recover the secret, is known as an access structure of the scheme. Usually Γ is the symbol used to denote access structure of a secret sharing scheme. The set of all unauthorised sets, which can not gain any knowledge about the secret, is called adversary structure or forbidden set. Usually the adversary structure is denoted by $\overline{\Gamma}$. Various access structures are proposed in the literature. Example includes generalized access structures, (t, n) threshold access structures and multipartite access structures.

In a (t, n) threshold access structure any set of t or more participants out of n is an authorised set and any set of less than t participants is an unauthorised set. That is

$$\Gamma = \{X \in 2^n : |X| \geq t\} \text{ and } \overline{\Gamma} = \{X \in 2^n : |X| < t\}$$

where 2^n denotes the power set of the set of participants.

An access structure is called monotone, if it satisfies the following:

$$(X \in \Gamma) \text{ and } (X \subseteq Y) \Rightarrow Y \in \Gamma$$

$$(X \in \overline{\Gamma}) \text{ and } (Y \subseteq X) \Rightarrow Y \in \overline{\Gamma}$$

If Γ and $\overline{\Gamma}$ are such

$$\Gamma = \{X \in 2^n : |X| = t\} \text{ and}$$

$$\overline{\Gamma} = \{X \in 2^n : |X| = t - 1\}$$

then we say that Γ only contains the minimal authorised sets which can get the secret, $\overline{\Gamma}$ only holds maximal unauthorised sets which can not get the secret.

2.9.2 Hierarchical access structure (HAS)

Simmons [64] proposed the first hierarchical threshold secret sharing (HTSS) scheme. In an hierarchical threshold secret sharing scheme, participants play different roles; while in a simple threshold SSS participants play the same role. An hierarchical threshold secret sharing scheme is also known as a multilevel threshold secret sharing (MTSS) scheme.

Let $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ be the set of n participants, partition into m security levels $\mathcal{L} = \{L_1, L_2, \ldots, L_m\}$, such that $\mathcal{P} = \bigcup_{i=1}^{m} L_i$. Let $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$ be a sequence of threshold values $t_1 < t_2 < \cdots < t_m$, such that $1 \leq t_i \leq |L_1| + |L_2| \cdots + |L_i|$, where $1 \leq i \leq m$. Formally, the access structure Γ of $(\mathcal{L}, \mathcal{T})$ hierarchical threshold secret sharing scheme is

$$\Gamma = \{\mathcal{A} \subseteq \mathcal{P} : |\mathcal{A} \cap (\bigcup_{j=1}^{i} L_j)| \geq t_i\}$$

For some i, $1 \leq i \leq m$.

In a hierarchical threshold SSS, all the n participants are divided into m disjoint levels $L_1, L_2, \cdots L_m$. These levels constitute an hierarchical structure. The i^{th} level consists of n_i participants and any t_i or more participants can recover the secret on i^{th} level. At any point when the number of participants in the i^{th} level is less than t_i, say r_i, then the $t_i - r_i$ remaining participants can be taken from higher levels. Note that,

throughout the thesis we have considered the level L_i is higher than the level L_{i+1}, $1 \leq i < m$.

As an example, if the threshold values are $t_1 = 3$ at level L_1 and $t_2 = 4$ at level L_2, then three participants at L_1 or four participants at L_2 can recover the secret. In addition, the secret can be recovered when there is one participant at L_1 and three participants at L_2.

A scheme is known as a one-time use scheme if the shares are not valid after reconstructing the corresponding secret. On the other hand, if shares can be reused for other secrets as well then the scheme is known as a multi-use scheme. It is well known that, distribution of a share must be punctilious, and it is a costly process. For this reason, multi-use has become an essential property for the secret sharing schemes. One of the chapter on multi-secret sharing scheme with multi-use property in the thesis.

2.9.2.1 Secret sharing for hierarchical access structure.

Ghodosi[34] proposed a scheme that is applicable to a hierarchical access structure. He uses a sequence of related Shamir's (t, n) threshold schemes with overlapping shares. He uses $(t_i, N_i)_{T_i}$ which indicates an extension of Shamir's (t_i, N_i) scheme, where the degree of a polynomial is at most $T_i, (T_i > t_i)$ and N_i is the total number of participants from the i^{th} level and higher level i.e. $N_i = \sum_{j=1}^{i} n_j, 1 \leq i \leq m$. Let, the set of all players on the i^{th} and all higher levels be denoted by $\mathcal{P}^i = \bigcup_{j=1}^{i} L_j$. Scheme of Ghodosi, that realizes the hierarchical access structure is as follows:

"First a (t_1, n_1) threshold scheme (scheme A_1) is designed. It corresponds to the first (highest) level of participants from p^1. Then a (t_2, N_2) threshold scheme (scheme A_2) for p^2 is constructed; which is as an extension of A_1. Next a (t_3, N_3) threshold scheme (scheme A_3) for p^3 is constructed. This is as an extension of A_2. The process continues until a (t_m, N_m) threshold scheme (scheme A_m) for p^m is constructed by extending the threshold scheme A_{m-1}". In Ghodosi scheme, each participants has given a single share for sharing a single secret. Overview of the scheme is as follows:

- **I. Distribution Phase:**

    1. Choose a random polynomial of order at most $T_1 = t_1 - 1$ then calculate n_1 shares for n_1 players of P^1. The result is a $(t_1, N_1)_{T_1}$ threshold scheme

$(N_1 = n_1)$.

2. $for\ i = 2 \rightarrow m$ do
   - Construct extension of given initial threshold scheme, i.e. $(t_i, N_i)_{T_i}$
   - Calculate n_i shares for players on the i^{th} level.
3. Distribute the shares to corresponding players via secure channels.

- **II. Reconstruction phase:**
  - Any authorized subset of t_i or more players at level L_i can recover the secret using Lagrange polynomial interpolation.
  - At any point when the number of participants in the i^{th} level is less than t_i remaining participants can be taken from higher levels.

2.9.3 Level ordered access structure (LOAS)

New Level ordered access structure (LOAS) that is not the same as existing multipartite access structure was suggested by Dileep et al. [58]. In LOAS, a set of participants are partitioned into various levels, and every level is associated with the threshold. It introduces an ordering among the levels, which is absent in the existing access structures. In LOAS during the reconstruction, the actual secret should get reconstructed if the shares are submitted by the players adhere to the specified order. Formally, the proposed Level ordered access structure (LOAS) is as follows [58].

Let "$\mathcal{P}$ be the set of n participants $p_1, p_2, \ldots, p_n$ partition into m levels $\mathcal{L} = L_1, L_2, \ldots, L_m$. Let b_i be a boolean variable called the activation index, associated with the i^{th} level L_i, $i \in \{1, 2, \ldots, m\}$ and t be the threshold. Let A_i be an authorised set corresponding to the i^{th} level if

1. $A_i \subseteq L_i$ and $|A_i| \geq t_i$.
2. $\exists$ an authorised set (A_{i-1}) whose activation index(b_{i-1}) is True (T), where $b_0 = T$" and $A_0 = \emptyset$ $(emptyset)$

Overview of the LOAS by Dileep et al. [58]

- **I. Distribution Phase:**

  1. Choose partial secret $s_i, 1 \leq i \leq m$
  2. Set the partial secret of the last level as the master secret $S = s_m$.
  3. *For* $i = m \rightarrow 2$ do
     - Share the secret $s_i - s_{i-1}$ to the participants at level $L_i^{'}$ based on Shamir's (t_i, n_i) scheme and set s_{i-1} as the share of the virtual player v_i at level $L_i^{''}$.
     - Set $i = i - 1$.
  4. Share the secret s_1 to participants at level L_1 using Shamir's (t_1, n_1) scheme.

- **II. Reconstruction phase:**

  - Use Lagrange polynomial interpolation at level L_1 to recover the partial secret s_1 which is the share of the virtual player v_1 in next level L_2.
  - *For* $i = 2 \rightarrow m$ do
    - Use Lagrange polynomial interpolation to recover the secret from $L_i^{'}$, and add it with the share of the virtual player to recover the partial secret of level L_i which then is the share of the virtual player in the next level, i.e., the share of $L_{i+1}^{''}$.
    - If $i < m$, set $i = i + 1$. Else, return the partial secret of level L_m which is the master secret.

2.9.4 Compartmented access structure (CAS)

In compartmented access structure, the group of participants are divided into multiple compartments. Each compartment is assigned a threshold and a global threshold. In compartmented access structure a secret can be reconstructed only when the number of participants is greater than or equal to the threshold from the each compartments and the global threshold is greater than or equal to the total number of participants. In a compartmented access structure, set of n number of participants $\mathcal{P} = p_1, p_2, \ldots, p_n$ are divided into m disjoint compartments $\mathcal{C} = C_1, C_2, \ldots, C_m$. $t_0 = t_1, t_2, \ldots, t_m$ be the

thresholds of the corresponding compartment, such that $1 \leq t_i \leq |C_i|, \forall i = \{1, 2, \ldots m\}$ and t_0 is global threshold.

The access structure consists subsets of participants that contain minimum of t_i participants from compartments C_i, where $i \in \{1, 2, \ldots, m\}$ and a total of t_0 participants. Formal definition of compartmented access structure is follows:

$$\Gamma = \{\mathcal{A} \subseteq \mathcal{P} : |\mathcal{A} \cap C_i| \geq t_i \text{ for all } i \in 1, 2, \ldots, m \text{ and } |\mathcal{A}| \geq t_0\}$$

where $\mathcal{P} = \cup_{i=1}^{m} C_i$, $C_i \cap C_j = \emptyset$ for all $1 \leq i < j \leq m$ and $t_0 \geq \sum_{i=1}^{m} t_i$

2.10 Adversary Model

In the reconstruction phase, it is very important to take care about the authentication of shares, which are exchanged between the shareholders. It is also very important while each shareholders receives his/her share from dealer. Both dealers as well as shareholders can be deceived. Mainly, two types of Adversary model are considered in secret sharing schemes.

2.10.1 Insider Adversary

These are real shareholders who owns a share generated by the dealer. Insider adversaries may work alone or conspire with some other. Any of the participants can be insider adversary including dealer. Insider adversary can learn the secret before the reconstruction or influences the group to recover an invalid secret using fake share.

2.10.2 Outsider Adversary

The outsider attacker is one who does not own any share from the dealer, but he/she may try to learn the secret. She is not authentic to access the secret. These type of adversaries are active when shares are exchanged in an insecure fashion.

2.10.3 Cheating Detection and Identification

A secret sharing scheme divides single secret into multiple shares that are shared between the participants. The secret can be retrieved only by the set of participants

from the authorised access structure. Secret sharing scheme can be used in any situation where the access to a valuable resource has to be restricted. The majority of the secret sharing schemes are handled by a dealer, but a few secret sharing schemes are operated by a combiner (without dealer's help). Combiner will involve into secret sharing scheme when participants integrate their shares to retrieve the secret. If any participant is cheating, then the reconstruction phase may be equipped with one of the following:

- Cheating detection - fake user can be distinguished yet can't recognize the fake user.
- Cheating identification - fake user can be identified.

To manage these cheaters, two principle models have been exhibited in the literature are mentioned below:

- The first model is **CDV (Carpentieri, De Santis and Vaccaro)** model [15]. In this model, cheaters know the main secret and they utilize changed share at the time of recovery to make invalid secret to different users.
- The second model is **OKS (Ogata, Kurosawa and Stinson)** model [49]. In this model, cheaters do not know the main secret beforehand.

Chapter 3

Literature survey

3.1 Secret sharing scheme

Secret sharing schemes have got extensive researchers attention in the last few decades. The first independent development of secret sharing was in 1979 by Adi Shamir [62] and George Blakley [11]. Shamir's scheme uses Lagrange polynomial interpolation, whereas that of Blakley's one uses concepts from Linear projective geometry, i.e. hyperplanes. Later on, many researchers contributed to the domain of secret sharing by proposing various secret sharing schemes. In 1981, McEliece [52] proposed a (t, n) threshold secret sharing on the basis of "Reed Solomon codes" and Massey [51] proposed a secret sharing scheme using a "linear code-based" method for the construction. In 1982, First Mignotte [54] then Asmuth-Bloom *et al.* [3] in 1983, proposed secret sharing schemes using their corresponding sequences and the "Chinese remainder theorem". Secret sharing scheme that uses Mignotte's sequence is discussed in [46] based on the Chinese remainder theorem. Secret sharing schemes based on boolean operations [14], Matroids [19], linear block codes [46, 48, 57], MDS codes [12], computational schemes [8, 80], geometric structures [10], room squares [24], algebraic equations [34], permutations [60], combinatorics and graph theory [40] are discussed. Benaloh [9] proposed a circuit-based approach secret sharing scheme. In 2003, Pieprzyk *et al.* [59] constructed ideal threshold schemes with MDS codes. As we have seen in the literature, many secret sharing schemes have been proposed, but all these schemes have common drawbacks. All of these schemes in the literature allowed only one secret to be shared, and each time a new share has to be generated after the use of the secret.

3.1.1 Multi-secret sharing schemes: Survey

In order to share many secrets, the concept of "multi-secret sharing scheme" and the related terminology comes in secret sharing literature. The "multi secret sharing scheme" is an extension to the Shamir scheme [62]. The literature proposes several "multi secret sharing schemes". In 1994, multi secret sharing was first proposed by Dawson *et al.* [24] in which multiple secrets are able to share with each participant at the same time using a one share.

A multi secret sharing scheme was introduced by He and Dawson [39] which uses one-way function to share multiple secrets. In our proposed scheme, we have also used concepts of one-way function. Karnin et el. [46] introduced a "multi-secret sharing scheme" where several secrets are able to recover simultaneously by a sufficient number of participants. Franklin *et al.* [33] employed a method by which a single secret sharing scheme was modified to a scheme in which several secrets were contained within a single polynomial. A study of the multi-secret scheme based on matroids was conducted by Jackson *et al.* in [45]. Chien *et al.* [22] used systematic block codes and matrices in 2000 to propose a practical threshold multi-secret sharing scheme. In 2004, the new (t, n) threshold "multi-secret sharing scheme" introduced by Yang, Chang, Hwang, (Y.C.H) in [84]. In his scheme, instead of using separate polynomials for each secret, a single polynomial is used for sharing multiple secrets known as the Y.C.H. scheme. The YCH scheme needs less public values, low computation and low storage compared to the Chien *et al.* scheme [22]. In [63], Shao and Cao proposed a efficient verifiable "multi secret sharing scheme" based on the Yang-Hwang-Chang scheme. A practically verifiable multistage secret sharing scheme based on Y.C.H that uses the discrete logarithm has been proposed by Jianjie[87] in 2007. In 2008, Massoud and Samaneh [25] suggested an efficient threshold verifiable "multi-secret sharing" based on the Yang-Hwang-Chang [84] schemes. A new verifiable " "multi-secret sharing scheme" based on bilinear maps proposed by [28] in 2012.

3.1.2 Multi-stage secret sharing schemes: Survey

He and Dawson have made it clear how the participants share a single secret and multiple secrets. Latter Dawson introduced in [38]the idea of multi stage secret sharing (MSS) based on the one way function to share multiple secrets. In this scheme, the

public shift techniques were used to get the actual shares and successive application of the one-way function to recover the secrets stage by stage in a predefined order. In our proposed scheme, we have used some of these concepts. Furthermore, it introduced an alternative multi-stage secret sharing scheme by reducing the number of public values, which realized on the Lagrange interpolating polynomial. Both the schemes suggested by He and Dawson [38] and Harn [35] are known to be multi-use scheme. Such two schemes later proved not to be multi-use by Chang *et al.* in [17] by showing that the dealer fails to recover the secrets in the predefined sequence. In order to eliminate the disadvantages, Chang modified the He and Dawson scheme [38] by using a one-way function. In fact, Chang's [17] scheme also shows that Harn's [35] scheme is not suitable for general multi-secret sharing applications. There are several issues with these schemes [35, 38, 39], for example, each secret sharing process can share only one secret, which is a one-time use scheme. Both Dawson and Harn's scheme, have disadvantages in constructing the schemes to be truly multi use schemes. To overcome those disadvantages Chang [84], Hwang [16] and Yang [42] have introduced a new multi scheme. It is based on the public shift technique and successive applications of a one-way hash function. C. Lien [50] has proposed a new scheme to minimise public values and strictly follow the order in which secrets are revealed. In 2015, a new scheme called multi-stage multi-secret sharing scheme that is CRT based was introduced by Endurthi *et al.* [27]. Several multi-stage multi-secret (MSMS) sharing schemes have been proposed in literature [42, 68, 79].

Since 1979, literature has seen various schemes of secret sharing. Secret sharing schemes can have several properties. In the literature, many "multi secret sharing schemes" were suggested using various mathematical methods and techniques. Secret sharing schemes can be categorized on the basis of the mathematical tools and techniques used, as shown in Table I. A further categorisation of the secret sharing schemes can be in accordance with the number of secrets they share as shown in Table II.

In addition, the presence of "multi secret sharing schemes" in the literature it exists that realises various access structures. The number of access structure have been described using the (t, n) threshold access structures for example, hierarchical(Multi-level) access structures [30, 69], compartmented access structures [34, 40, 55] and level order access structures [39].

Table 3.1: Various Mathematical techniques in secret sharing scheme

Mathematical Approach	Author's Name
Vector space based	Blakley;
Polynomial based	Shamir; Ghodosi; **Basit**; Yang; Franklin; He; ours
CRT based	Mignotte; Asmuth-Bloom; Endurthi; Iftene; Hsu; Singh; Harn;
Matrix projection based	Bai; Wang;
Systematic block codes based	Chien;
superincresing sequence	Harsha; **Basit**;
Finite Geometry	Duari;
Modular inverse	**Basit**;

Table 3.2: Single and Multi secret sharing schemes

Single secret sharing scheme	Multi-secret sharing scheme
Shamir; Brickell; Ghodosi; Asmuth-Bloom; Blakley; Mignotte; Iftene; Farras; Ghodosi; Jackson; Harsha;	Chien; Shao; Singh; Franklin; Tentu; Yang; He; Zhang; Bai; **Ours**

3.2 Access Structure

An access structure is a family of authorized subsets of participants who are allowed to recover the secret. Many access structures were proposed to cater to various application scenarios. The research community contributed by designing various secret sharing scheme which realizes different access structures including multi level (hierarchical) access structure, compartmental access structure and level ordered access structure. The line of work began from Simmon and Gustavus [64], which introduced two types of access structures, a compartmented access structure and the multi-level access structure for ideal secret sharing schemes.

3.2.1 Compartmented access structure : Survey

Simmons and Gustavus [64] introduced the compartmented secret sharing concept. They have considered secret sharing for compartmented access structures. Using geometric techniques, Simmons and Gustavus have developed the concept of compartmented access structures. Herranz *et al.* [40] in 2006 presented the family of ideal multipartite access structure which can be viewed as the variant of a compartmented access structure. The schemes suggested by Ghodosi *et al.* [34] that realize compartmented

access structures. These schemes apply the secret sharing scheme of Shamir's two times, firstly to obtain the secrets and secondly to incorporate them into the required secret. The thesis chapter 2 presents a concise definition of both the cases of global thresholds that correspond when the sum of all local thresholds is equal and when the sum of all local thresholds is higher. In 2007, S. Iftene [43] suggested a compartmented secret sharing scheme mainly based on the "Chinese remainder theorem". In 2009, a new access structure called compartmented access structures with lower limits was introduced by Tassa and Dyn [71]. Brickell [13] suggested a broader family of access structure called a lower-bounded compartmented access structure. For these access structures, Tassa and Dyn also designed a secret sharing scheme with polynomial bivariate interpolation. Farras *et al.*. [31] characterised some new ideal compartmented access structures, such as the upper and lower bounded compartmented access structure. In 2012, Selcuk *et al.* [61] presented the idea of a shared compartmented threshold access structure. Thesis chapter 5 shows that we have proposed new multi-secrete sharing schemes that realise compartmented access structures.

3.2.2 Hierarchical access structure : Survey

Hierarchical threshold access structures have been studied extensively in the literature. The concept of multilevel/hierarchical secret sharing proposed to assigning more shares to players was introduced by a few authors such as Kothari [48], Brickell [13], Simmons [64, 65], Charnes [19] and Ghodosi [34]. Earlier, the secret sharing scheme in a hierarchical structure was proposed under different premises. In 1984, Kothari [48] presented a generalization of existing secret sharing schemes. The scheme proposed by Kothari is a generalized scheme that associates (t, n) hierarchical level threshold schemes. Simmons [64] proposed, in 1988 first "Hierarchical secret sharing scheme known as disjunctive hierarchical secret sharing scheme". He observed that all shareholders play different roles according to their level of authority. The hierarchical scheme proposed by Simmons in [64, 65] was not ideal. It was an open problem to find an optimal, ideal, and linear solution to the disjunctive case of Simmons. In 1989, Brickell [13] proposed an ideal Hierarchical threshold secret scheme (HTSS). In this scheme, the dealer chooses a separate polynomial for every level and sends it to the corresponding participants. Brickell scheme is inefficient since it takes exponential time to ensure the non-singularity of the matrices. Hierarchical secret sharing for threshold access structure based on the

Asmuth Bloom sequence in [3, 77] proposed by using Chinese remainder theorem. Ghodosi *et al.* in [34] proposed a Hierarchical threshold scheme, which only applies to a small number of participants. In 2006, Tamir and Nira [70] proposed a new polynomial time conjunctive secret sharing scheme, that was based on Birkhoff 's bivariate interpolation. It requires a large finite field with certain constraints on participant identity assignment. A variation of this is proposed by Tassa [69], known as conjunctive multilevel secret sharing scheme. Later, Tassa and Dyn [71] have proposed ideal secret sharing scheme for hierarchical access structure, which is ideal and perfect in a probabilistic manner. In 2009, Lien *et al.* [50] proposed an ideal hierarchical threshold SS scheme with a modification to Shamir's secret sharing scheme. In 2014, Harn and Fuyou [36], proposed the hierarchical threshold secret sharing scheme by using the Chinese remainder theorem considering only a single secret.

In 2015, another secret sharing scheme, which is a variation of multi level was proposed by Naidu *et al.* in [74] . The dealer shares the master secret along with a random secret among the participants at the last level. At each level, except at the last level the participants use polynomial distribution to share random secrets. Mehrdad Nojoumian *et al.* [56] suggested a new hierarchical sequential secret sharing scheme, which differs from the existing disjunctive and conjunctive secret sharing schemes. In his scheme, only one secret is distributed among the participants at different levels of authority. T.Appala Naidu *et al.* proposed the conjuctive and disjunctive secret sharing schemes based on error correcting codes in [76] and this scheme is computationally perfect. In 2016, Singh *et al.* [67] proposed a sequential secret sharing scheme for hierarchical access structure with multi-secrets. In sequential secret sharing scheme, along with the master secret, multiple secrets generated from the master secret with thresholds assigned in increasing order are distributed among the participants at different levels of authority.

3.2.3 Level ordered access structure : Survey

Many access structures have been suggested to cater to different application scenarios. In 2016, Dileep *et al.* in [58] proposes a new access structure called "Level ordered access structure" that differs from existing access structures. Level ordered access structure imposes an ordering concept that is absent from the existing access structures. In level

ordered access structure, a set of participants is partitioned into various levels, and every level is associated with the threshold. In 2017, Harsha *et al.* [37] proposed the first secret sharing scheme for the level ordered access structure. However, this scheme is only for one secret.

In chapter 6 of this thesis proposed a new scheme, which is influenced by Harsha *et al.* scheme and can be viewed as a logical extension to the case of multi-secret. There is no multi-secret sharing scheme to date and, to the best of our knowledge, which is based on the level order access structure that uses super increasing sequence. The proposed scheme in this work uses a superincreasing sequence and ensures ordering during the reconstruction corresponding level shares. In other words, the secret bits information can only be obtained at the lower level after all the higher levels have got their secret bit(s). The preliminary chapter in the thesis discusses the detailed description of the super-creasing sequence.

3.3 Motivation and Contribution

3.3.1 Problem Identification and Motivation

In digital data storage and transmission, security is a major challenge. Secret sharing protocols provide solutions to a variety of security concerns. These include secure key management, secure distributed storage and transmissions, distributed access control and secure multi-party computation. The majority of existing secret schemes share only one secret for the different access structure among participants. Once this secret is reconstructed, fresh shares corresponding to a new secret are to be redistributed through a secured channel. It can be considered as an expensive and comprehensive process. Although some of the schemes cater to multiple secrets, no one relies on existing access structures in the literature. The purpose of this study is to design a "new multi secret sharing schemes" for different access structures. This thesis addresses the problem of sharing multiple secrets within a different access structure and also explores their usage in common application areas.

3.3.2 Contributions

This thesis contributes mainly to the design and use of a "Multi secret sharing protocol" in typical areas of application.

3.3.2.1 Contribution 1: Multi Stage Multi Secret Sharing Scheme for Hierarchical Access Structure

In the first contribution, we have addressed the issues of sharing multiple secrets in a hierarchical threshold access structure using the public shift technique. The resulting scheme is a new "multi secret sharing scheme" and is based on polynomial interpolation. The proposed scheme will share many secrets in sequential order among all the participants. In this multi-secret sharing scheme, each participant requires only one share to be kept and can be used as many secrets as desired. The proposed scheme has multi-stage features. It means that recovery of the secrets are stage by stage in a predefined order. The recovery of a secret at an earlier stage does not reveal or weaken the information of remaining secrets which has not been recovered. The shares are reusable in the proposed scheme and secret can be recovered step by step. So, it is both a multi-use and multi-stage secret sharing scheme. The proposed scheme is computationally perfect, which ensures that authorised set can recover the secrets in polynomial time, while it is computationally difficult for an unauthorized set. We have proposed scheme, that satisfies various features and its security is based on the Shamir scheme and the one-way function. The proposed scheme is discussed in detail in Chapter 4.

3.3.2.2 Contribution 2: Multi-secret Sharing Scheme Using Modular Inverse for Compartmented Access Structure

Second contribution to this thesis, we have developed a secret sharing protocol that realises a variation of the "multipartite access structure". We came up with a new scheme that overcomes the limitations that exist in most of the existing schemes in the literature. For the compartmented access structure, we have designed a secret sharing scheme, which uses the concept of the modular inverse. The schemes proposed are able to deal with many secrets. Advantage of this scheme is that the recovered secret can be checked as to whether the retrieved secret is right or not, and also no

compartment participant knows other compartment secrets. In order to retrieve the desired secrets, the proposed multi-secret sharing scheme uses Shamir's scheme first to recover compartment secret, then combines it obtained desired the secrets. The scheme is ideal and computationally perfect. Till date, there is no multi secret sharing scheme in the literature, which realizes the "compartmented access structure by using modular inverse techniques " The proposed scheme can be employed in the situation based application, which is addressed in the details in Chapter 5 of this study.

3.3.2.3 Contribution 3: New multi-secret sharing scheme based on super-increasing sequence for level-ordered access structure

There is no multi-secret sharing in all the existing access structures using ordering concept. We have proposed another secret sharing scheme for level ordered access structure. Level ordered access Structure is different from hierarchical and compartmented access structure. The previous two contributions used both the access structures. The level-order access structure, which imposes ordering for both share distribution and secret reconstruction. The scheme is based on subset sum problem and it uses superincreasing sequence. An important fallout in this access structure is that the actual secret can be recovered only after the reconstruction of all the compartment (level) secrets. All the compartment secrets may be constructed simultaneously. However, constructing the actual secret requires adherence to the hierarchy. For each compartment (level), the Shamir scheme is used for distributing and recovering the compartment secret. In the proposed scheme, there is no ordering among the retrieval of actual secrets, which indicates that the i^{th} secret can be retrieved without the retrieval of $(i-1)^{th}$ or $(i+1)^{th}$ secret, so there is also no relationship between the number of levels and the number of secrets. This ensures that the number of secrets and the number of levels are independent. The proposed scheme holds the property of secret changeability without any changes to the secret shares of the compartment. This implies that the dealer can modify the secret many times without modifying compartment secrets. This feature adds the re-usability to our proposed scheme, hence eliminates the overhead of share distribution to the participants. The proposed scheme can be incorporated in situation-based application and the security of the schemes relies on some computational assumptions. Which are discussed in detail in Chapter 6 of this thesis.on participant identity assignment.

3.4 Summary

In this chapter, we have discussed basic definitions, preliminaries that uses mathematical techniques to understand the various types of secret sharing schemes, functionality and their efficiency. Later, we presented an extensive literature survey on secret sharing schemes, access structures and related work. After that motivation and contribution of work are discussed at the end.

Chapter 4

Multi-stage Multi-secret Sharing Scheme for Hierarchical Access Structure

In the previous chapter, we have discussed various multi secret sharing schemes and their approaches. In this chapter, we elaborate multi secret sharing schemes and propose "Multi-stage multi-secret sharing scheme for hierarchical access structure" by following a polynomial approach.

4.1 Introduction

Secret sharing schemes, that share multiple secrets are known as "multi secret sharing schemes". In the multi secret sharing scheme, participants keep a single share that corresponds to many secrets shared using the scheme. The dealer uses a public information board to publish the necessary public values for the reconstruction of the secrets. The participants use pseudo shares for the reconstruction of multiple secrets. These pseudo shares are calculated using the original share and public information. Reconstruction of a secret does not reveal any information about the remaining secrets that have not been reconstructed. In multistage secret sharing scheme secrets are revealed/retrived stage by stage with each secret is revealed/retrived in one stage. In a single stage secret sharing scheme, all the secrets are revealed in the single stage. Hierarchical threshold secret sharing (HTSS) schemes can be thought as a generalization of classical threshold

secret sharing schemes, and they have been extensively studied in the literature. In an HTSS, participants are classified into different security levels, and the threshold value of a higher level is smaller than that of a lower level. Participants in each level can recover the secrets if the number of shares is equal to or more than the corresponding threshold value. Share of a higher level participant can be used to reconstruct the secret at lower level.

In this chapter, we have described our proposed hierarchical threshold multi-secret sharing scheme based on polynomial interpolation. Proposed scheme is a variation to HTSS schemes based on the CRT suggested by Singh et al. [67] and Harn et al. [36]. Novelty of the proposed scheme is that each participant requires to keep only one secret share and multiple secrets can be shared separately without refreshing the secret share. Also, secrets are recovered stage by stage. Our scheme which is unconditionally secure, is based on Lagrange interpolation polynomial and one-way function.

4.2 Motivation and Contribution

Problem Identification and Motivation

All the existing schemes except the one [67] proposed by Singh et al., share only one secret among the participants, who are in different levels and realizes a hierarchical access structure. When this secret is reconstructed, fresh shares corresponding to a new secret are to be redistributed over a secure channel. This can be seen to be an involved and costly process. Though the scheme in [67] caters to multi secrets, the range of the secrets chosen in this scheme are very limited.

Contribution

This chapter address the problem of sharing multiple secrets in a hierarchical threshold access structure, by using public shift technique and one-way function. The resulting scheme is a new hierarchical threshold secret sharing scheme with multi-stage, multi-secrets and it is based on polynomial interpolation. In our proposed scheme, many secrets are shared among the participants in sequential order. The scheme is unconditionally secure and it is efficient. Proposed scheme can be applied to scenarios wherein an organization consists of different authority levels of the employees for performing

different business functionalities. It may be the case that each functionality requires a set of secrets to be known. In some cases, if the sufficient number of employees are not available for reconstructing a secret then this level employees can take the help of higher level employees for recovering the secret and hence perform the required business functionality.

The proposed scheme satisfies the features listed below, and its security is based on that of the Shamir secret sharing scheme and the one-way function employed. We assume that the participants are partitioned into m disjoint levels with threshold t_i, $1 \leq i \leq m$ and k multiple secrets (S_j, $1 \leq j \leq k$) to be distributed among n participants.

- **Threshold feature:** Any t_i out of n_i participants can collaborate to recover the secrets S_j at i^{th} level, but it is impossible to recover the secrets S_j with the knowledge of less than t_i secret shares where $1 \leq i \leq m$ and $1 \leq j \leq k$.
- **Multilevel feature:** Any t_i, where t_i is the threshold corresponding to the i^{th} level participants can recover the secrets on i^{th} level. At any point when the number of participants from i^{th} level is less than t_i, say q_i, then $t_i - q_i$ remaining participants shares can be taken from higher levels, where $i = 1, 2 \ldots, m$.
- **Determine the values of secrets:** The dealer can randomly choose the values of the secrets S_j, $1 \leq j \leq k$.
- **Multi-stage feature:** The secrets will be reconstructed in specified order as $S_k, S_{k-1}, \ldots, S_1$. Reconstruction of the secrets is such that the secrets constructed at prior stages will not reveal or decrease the secrecy of the remaining secrets.
- **Multiuse feature:** If some particular secrets are reconstructed, it is not necessary that fresh share is distributed again through a secure channel to each shareholder.
- **Efficient:** Each shareholder is required to keep only one secret share.

4.3 Proposed Scheme

4.3.1 Overview of the proposed scheme

The proposed scheme is a threshold "multi secret sharing scheme" where any number of secrets can be shared and threshold number or more number of participants can

reconstruct the multi secrets. The multi secrets can be reconstructed in stage by stage i.e. multi stage secret sharing scheme. The proposed scheme consist of the following three phases :

- Initialization.
- Share Distribution.
- Secret Reconstruction.

Consider the set of n number of participants $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ be partitioned into m disjoint levels, $\mathcal{L} = \{L_1, L_2, \ldots, L_m\}$. Corresponding to each level L_i there is a threshold t_i, $i = 1, 2, \ldots, m$, where L_1 indicates the highest level and L_m indicates the lowest level. Dealer chooses pseudo share y_i^u, $1 \leq u \leq n_i$ and $1 \leq i \leq m$, where n_i denotes the number of participants at the i^{th} level L_i. Dealer also chooses the k secrets $S_1, S_2, \ldots, S_k$ and modifies these secrets to become $S_j^{'} = S_j + S_{j+1}$, $1 \leq j \leq k-1$ and $S_k^{'} = S_k$. Shares are then generated corresponding to $S_j^{'}, j = 1, 2, \ldots, k$, using polynomial function. Public shares are generated by adding these shares to one-way function of the chosen pseudo shares. These public shares are then published and the pseudo shares are distributed through a secure channel to each participants.

While reconstructing the secrets, the participants first compute their true shares by subtracting the image of one-way function of their pseudo shares from the corresponding public value. Then Lagrange interpolation is used to reconstruct the modified secret S_j'. Actual secret S_{j-1} is then recovered by subtracting the previously reconstructed secret S_j, $j = 1, 2, \ldots, k$. The secrets can be recovered stage by stage at any level L_i, $1 \leq i \leq m$ only if the number of shares available is greater than or equal to the threshold value t_i. If the number of shares available at any level L_i is less than the threshold value t_i then participants from the higher level can contribute the remaining shares to recover the secrets.

4.3.2 Algorithm

Following are the proposed scheme algorithm.

Algorithm 3: Initialization

1: Let $\{L_1, L_2, \ldots, L_m\}$ be the m levels.

2: Every level L_i is associated with (t_i, n_i) threshold access structure, where t_i is value of threshold and n_i is the total number of participants at level L_i, $1 \leq i \leq m$.

3: Select large prime q.

4: Choose k secrets i.e $S_1, S_2, S_3, \cdots, S_k$ s.t. $S_j \in Z_q$, $1 \leq j \leq k$.

5: Let f be a one-way function and $f^j(y)$ indicates the j successive applications of f to y, i.e. $f^0(y) = y$ and $f^j(y) = f(f^{j-1}(y))$, for $j \geq 1$.

6: Choose randomly the pseudo shares y_u^i with respect to the participant u at level i, where $1 \leq i \leq m$ and $1 \leq u \leq n_i$.

7: ID_u^i: denote the identifier with respect to the participant u at level i, where $1 \leq i \leq m$ and $1 \leq u \leq n_i$.

Algorithm 4: Share Distribution:

1: Compute $S_j' = S_j + S_{j+1}$, for $j = 1 \rightarrow k-1$

2: $S_k' = S_k$

3: **for** $i = 1 \rightarrow m$ **do**

4: **for** $j = 1 \rightarrow k$ **do**

- Select randomly $t_i - 1$ positive integers from Z_q, $a_{1,j}^i, a_{2,j}^i, \cdots, a_{t_i-1,j}^i$, and let $a_{0,j}^i = S_j^{'}$
- Construct the Polynomial of order $t_i - 1$, $F(x) = a_{t_i-1,j}^i \times x^{(t_i-1)} + \cdots + a_{1,j}^i \times x + a_{0,j}^i$
- **for** $v = i \rightarrow 1$ **do** {
  for $u = 1 \rightarrow n_v$ **do**
  - Compute $d_{u,j}^v = F(ID_u^v) \bmod q$
  - Compute $z_{u,j}^v = d_{u,j}^v + f^j(y_u^v) \bmod q$ }

5: Distribute pseudo shares y_u^i to corresponding participants via secure channel and publish all the $z_{u,j}^i$ values, where $1 \leq i \leq m$, $1 \leq u \leq n_i$ and $1 \leq j \leq k$

Algorithm 5: Share Reconstruction:

1: Participant at any level L_i willing to take part in the reconstruction calculates his actual share by computing $d^i_{u,j} = z^i_{u,j} - f^j(y^i_u) \bmod p$

2: Case 1: At level L_i

- Authorized subset of any t_i or more than t_i participants at level L_i can recover the $S_j{}', 1 \leq j \leq k$ using polynomial interpolation formula.

3: Case 2: At lower level L_i with the help for higher level L_x participants, where $x < i$

- Authorized subset of any t_i or more than t_i participants from level L_i and L_x, can also recover the $S_j{}', 1 \leq j \leq k$ using polynomial interpolation formula.

4: Calculate secrets sequentially $S_k, S_{k-1}, \ldots, S_1$ as $S_k = S'_k$ and $S_j = S'_j - S_{j+1}$, for $j = k-1 \rightarrow 1$

4.3.3 Example

SAGE and Python are used for implementing the scheme. We present a sample example to show our proposed "multi-stage multi-secret sharing scheme" for hierarchical access structure with artificially small parameters. We considered field with smaller prime for easy understanding.

1. *Initialization:*

   - Consider there are 10 participants $p_1, p_2, \ldots, p_{10}$, partitioned into two disjoint levels L_1 and L_2 and suppose the corresponding parameters (t_1, n_1) and (t_2, n_2) are $(2, 4)$ and $(3, 6)$ respectively.
   - Dealer chooses three secrets
     i.e. $S_1 = 5, S_2 = 7$ and $S_3 = 11$.
   - Let prime $q = 19$.
   - Let the chosen one way function be
     $f(y) = 2^y \bmod q$.
   - Let the chosen pseudo shares at the 1^{st} level be
     $y^1_1 = 1, y^1_2 = 2, y^1_3 = 3, y^1_4 = 4$ and

at the 2^{nd} level be
$y_1^2 = 5, y_2^2 = 6, y_3^2 = 7, y_4^2 = 8, y_5^2 = 9, y_6^2 = 10$

- ID's of the 1^{st} level participants be
  $ID_1^1 = 1, ID_2^1 = 2, ID_3^1 = 3, ID_4^1 = 4$ and
  at the 2^{nd} level be
  $ID_1^2 = 5, ID_2^2 = 6, ID_3^2 = 7, ID_4^2 = 8, ID_5^2 = 9, ID_6^2 = 10$

2. *Distribution*

- Compute $S_j' = S_j + S_{j+1}$, for $j = 1, 2$ i.e.,
  $S_1' = 5 + 7 = 12,\ S_2' = 7 + 11 = 18,\ S_3' = 11$
- **At level** $L_1, t_1 = 2$
  - **for** $S_1^{'} = 12$,
    $F(x) = 3 \times x + S_1^{'} = 3 \times x + 12$
    Compute Actual Shares :
    $d_{11}^1 = 15, d_{21}^1 = 18, d_{31}^1 = 2, d_{41}^1 = 5$
    Compute Public shares :
    $z_{11}^1 = 17, z_{21}^1 = 3, z_{31}^1 = 10, z_{41}^1 = 2$
  - **for** $S_2^{'} = 18$,
    $F(x) = 4 \times x + S_2^{'} = 4 \times x + 18$
    Compute Actual Shares :
    $d_{12}^1 = 3, d_{22}^1 = 7, d_{32}^1 = 11, d_{42}^1 = 15$
    Compute Public shares :
    $z_{12}^1 = 7, z_{22}^1 = 4, z_{32}^1 = 1, z_{42}^1 = 1$
  - **for** $S_3^{'} = 11$,
    $F(x) = 5 \times x + S_3^{'} = 5 \times x + 11$
    Compute Actual Shares :
    $d_{13}^1 = 16, d_{23}^1 = 2, d_{33}^1 = 7, d_{43}^1 = 12$
    Compute Public shares :
    $z_{13}^1 = 13, z_{23}^1 = 7, z_{33}^1 = 6, z_{43}^1 = 6$
- **At level** $L_2, t_2 = 4$
  - **for** $S_1^{'} = 12$,
    $F(x) = 4 \times x^2 + 3 \times x + S_1{}' = 4 \times x^2 + 3 \times x + 12$

Compute Actual Shares :

$d_{11}^2 = 13, d_{21}^2 = 3, d_{31}^2 = 1,$

$d_{41}^2 = 7, d_{51}^2 = 2, d_{61}^2 = 5$

Compute Actual Shares for higher level L_1 :

$d_{11}^1 = 0, d_{21}^1 = 15, d_{31}^1 = 0, d_{41}^1 = 12$

Compute Public shares :

$z_{11}^2 = 7, z_{21}^2 = 10, z_{31}^2 = 15,$

$z_{41}^2 = 16, z_{51}^2 = 1, z_{61}^2 = 3$

Compute Public shares for higher level L_1 :

$z_{11}^1 = 2, z_{21}^1 = 0, z_{31}^1 = 8, z_{41}^1 = 9$

- **for** $S_2^{'} = 18,$

  $F(x) = 5 \times x^2 + 4 \times x + S_2{'} = 5x^2 + 4x + 18$

  Compute Actual Shares :

  $d_{12}^2 = 11, d_{22}^2 = 13, d_{32}^2 = 6,$

  $d_{42}^2 = 9, d_{52}^2 = 3, d_{62}^2 = 7$

  Compute Actual Shares for higher level L_1 :

  $d_{12}^1 = 8, d_{22}^1 = 8, d_{32}^1 = 18, d_{42}^1 = 0$

  Compute Public shares :

  $z_{12}^2 = 14, z_{22}^2 = 8, z_{32}^2 = 12,$

  $z_{42}^2 = 8, z_{52}^2 = 4, z_{62}^2 = 17$

  Compute Public shares for higher level L_1 :

  $z_{12}^1 = 12, z_{22}^1 = 5, z_{32}^1 = 8, z_{42}^1 = 5$

- **for** $S_3^{'} = 11,$

  $F(x) = 6 \times x^2 + 5 \times x + S_3{'} = 6x^2 + 5x + 11$

  Compute Actual Shares :

  $d_{13}^2) = 15, d_{23}^2 = 10, d_{33}^2 = 17,$

  $d_{43}^2 = 17, d_{53}^2 = 10, d_{63}^2 = 15$

  Compute Actual Shares for higher level L_1 :

  $d_{13}^1 = 3, d_{23}^1 = 7, d_{33}^1 = 4, d_{43}^1 = 13$

  Compute Public shares :

  $z_{13}^2 = 4, z_{23}^2 = 16, z_{33}^2 = 5,$

  $z_{43}^2 = 18, z_{53}^2 = 12, z_{63}^2 = 13$

Compute Public shares for higher level L_1 :
$z_{13}^1 = 0, z_{23}^1 = 12, z_{33}^1 = 3, z_{43}^1 = 7$

3. *Reconstruction:*
Suppose at level L_2 with the higher level L_1 wants to reconstruct the secret. Since at level L_2 threshold value is 3. Let us assume, two participants from L_2 are p_2^2, p_4^2 and one participant from L_1 is p_1^1 are reconstructing the secrets.

- **for** $S_3^{'}$ calculate actual shares :
  - $d_{23}^2 = z_{23}^2 - f^3(y_2^2) = 10$,
    $d_{43}^2 = z_{43}^2 - f^3(y_4^2) = 17$,
    $d_{13}^1 = z_{13}^1 - f^3(y_1^1) = 3$ and
    ID's of corresponding participant are $6, 8, 1$
  - Apply Lagrange polynomial interpolation on $(6, 10), (8, 17)$ and $(1, 3)$ and get
    $F(x) = \frac{3}{10} \times x^2 - \frac{7}{10} \times x + \frac{17}{5} \bmod 19$
    $= 6 \times x^2 + 5 \times x + 11$
  - $\therefore S_3^{'} = 11$
- **For** $S_2^{'}$ calculate actual shares :
  - $d_{22}^2 = z_{22}^2 - f^2(y_2^2) = 13$,
    $d_{42}^2 = z_{42}^2 - f^2(y_4^2) = 9$,
    $d_{12}^1 = z_{12}^1 - f^2(y_1^1) = 8$ and
    ID's of corresponding participant are $6, 8, 1$
  - Apply Lagrange polynomial interpolation on $(6, 13), (8, 9)$ and $(1, 8)$ and get
    $F(x) = \frac{-3}{7} \times x^2 + 4 \times x + \frac{31}{7} \bmod 19$
    $= 5 \times x^2 + 4 \times x + 18$
  - $\therefore S_2^{'} = 18$
- **For** $S_1^{'}$ calculate actual shares :
  - $d_{21}^2 = z_{21}^2 - f^1(y_2^2) = 3$,
    $d_{41}^2 = z_{41}^2 - f^1(y_4^2) = 7$,
    $d_{11}^1 = d_{11}^1 - f^1(y_1^1) = 0$ and
    ID's of corresponding participant are $6, 8, 1$

- Apply Lagrange polynomial interpolation on $(6,3),(8,7)$ and $(1,0)$ and get
  $F(x) = \frac{1}{5} \times x^2 - \frac{4}{5} \times x + \frac{3}{5} \bmod 19$
  $= 4 \times x^2 + 3 \times x + 12$
- $\therefore S_1' = 12$

- Now calculate secrets S_3, S_2, S_1 sequentially as
  - $S_3 = S_3' = 11$
  - $S_u = S_u' - S_{u+1}$
    $S_2 = S_2' - S_3 = 18 - 11 = 7$
    $S_1 = S_1' - S_2 = 12 - 7 = 5$

4.4 Comparison with existing schemes

In the existing hierarchical access structures, only one secret is distributed among the set of participants which are divided into various levels of authority. Moreover, there is no concept of stage by stage construction of the secrets during the reconstruction. In our scheme, multiple secrets are shared among the group of the participants which are partitioned into various levels of authority. Access structure is such that secret can be recovered in any level with threshold number of participants from that level. If there are less than threshold number of participants available, they can take the higher level participants shares for recovering the secrets. Table 4.1 compares the proposed scheme with the corresponding existing schemes against some of the popular features.

Table 4.1: Comparison with existing schemes

Property	Ghodosi[34]	Harn[36]	Nidhi[67]	Endurthi[27]	Lien[50]	Proposed scheme
Based on	LPI	CRT	CRT	CRT	LPI	LPI
Reusable	No	No	NO	Yes	No	Yes
No. of Private Shares	n	n	kn	n	n	n
Multi-secret	Single	Single	Multi	Multi	No	Multi
Multi-stage	No	No	Yes	Yes	No	Yes
Hierarchical	Yes	Yes	Yes	No	Yes	Yes
Ideal and Perfect	Yes	Yes	Yes	No	Yes	Yes

4.5 Security Analysis:

Security of our proposed scheme depends on the security of one-way function f and Shamir's secret sharing scheme [62]. In this section, we have discussed some possible attacks on our proposed scheme.

Attack 1: Let $t_i - 1$ or fewer players at level L_i try to recover the secret.

`Analysis:` Recovery in the proposed scheme is based on Lagrange interpolation polynomial. So, solving for t_i values, need t_i equations. Therefore, only t_i or more players can get the secret, less than t_i can not get any piece of knowledge about the secret.

Attack 2: Let player p_l^i at same level L_i try to recover other's actual share $d_{u,j}^i$, where $1 \leq i \leq m, 1 \leq j \leq k, 1 \leq u, l \leq n_i, l \neq u$.

`Analysis:` When the secret is being recovered, each player knows other's pseudo shares $f(y_u^i)$. But, no one can get the real share y_u^i from $f(y_u^i)$ because f is a one-way function.

Attack 3: Players p_l^i tries to reveal other players pseudo shares $f^k(y_u^i)$.

`Analysis:` The secrets are recovered as sequence $S_k, S_{k-1}, \cdots, S_1$. To recover the secret S_k, t_i players should combined their pseudo shares $f^k(y_u^i)$. But, no one can get the other players pseudo shares $f^k(y_u^i)$ $(i < k)$. It is protected under hardness of the one-way function.

Attack 4: t_i players try to change the sequence of the secrets to be recovered.

`Analysis:` To get the S_i secret, they should recover the secret S_{i+1} first. So, the change in the order of recovering cannot work in our scheme.

4.6 Conclusions

A hierarchical multi stage multi secret sharing scheme using polynomials and one way function is proposed. The security of proposed scheme is same as that of the Shamir's scheme and hardness of one-way function which is unconditionally secure. In this proposed scheme participants are partitioned into different security levels based on Hierarchical access structure, and each level has different threshold. In our scheme,

each participant will have a single share of multi secret which reduces participant's overhead to keep multiple shares. The proposed scheme has a unique feature where the shares are reusable. So shares need not be refreshed for future sharing of shares. The secrets can be recovered stage by stage when authorized participants combine their shares and lower level participants can use higher level participants share to recover the secrets. Proposed scheme can be thought as a variation of hierarchical threshold secret sharing. The scheme may be improved by using only one polynomial for the construction of many secrets. Verification phase can be added to the proposed scheme to verify participant's share.

Chapter 5

Multi Secret Sharing Scheme using modular inverse for Compartmented Access Structure

In the previous chapters, we have proposed the scheme for sharing multiple secrets which realizes hierarchical access structure. In this chapter, we have proposed a scheme for another variation of access structure, which realizes compartmented access structure for sharing multiple secrets. In this access structure, the group of participants are divided into different compartments. A secret can be obtained only when threshold number of participants from each of the compartments reconstruct their compartment secret, and participate to recover the actual secret. The proposed scheme uses Shamir's scheme first to retrieve partial secrets and combines them to calculate the global secret. The scheme can also verify whether the retrieved secret is valid or not. Security analysis of the scheme is carried out and showed that the scheme resists both the insider as well as outsider attacks. Our proposed scheme is simple and easy to understand as we have used only the modular inverse concept.

5.1 Introduction

In a multi secret sharing scheme, participants keep only a single share that corresponds to many secrets shared using the scheme. The dealer uses a public information board to publish the necessary public values for the recovery of the secrets. The participants use pseudo shares for the reconstruction of multiple secrets. These pseudo shares are calculated using the original share and public information. Reconstruction of a secret does not reveal any information about the remaining secrets that have not been reconstructed. In literature, several access structures have been introduced. In compartmented access structure the group of participants are divided into multiple compartments. Each compartment is assigned a threshold and the global threshold. In compartmented access structure a secret can be reconstructed only when the number of participants is greater than or equal to the threshold from the each compartment and the global threshold is greater than or equal to the total number of participants. In a compartmented access structure, set of n number of participants $\mathcal{P} = p_1, p_2, \ldots, p_n$ are divided into m disjoint compartments $\mathcal{C} = C_1, C_2, \ldots, C_m$. Let $t_0 = t_1, t_2, \ldots, t_m$ be the thresholds of the corresponding compartment, such that $1 \leq t_i \leq |C_i|$ for all $1 \leq i \leq m$ and t_0 is the global threshold.

The access structure consists of subsets of participants containing minimum of t_i participants from compartments C_i, where $i = 1, 2, \ldots, m$ and a total of t_0 participants. Formal definition of compartmented access structure is follows:

$$\Gamma = \{\mathcal{A} \subseteq \mathcal{P} : |\mathcal{A} \cap C_i| \geq t_i \text{ for all } i \in 1, 2, \ldots, m \text{ and } |\mathcal{A}| \geq t_0\}$$

where $\mathcal{P} = \cup_{i=1}^{m} C_i$, $C_i \cap C_j = \emptyset$ for all $1 \leq i < j \leq m$ and $t_0 \geq \sum_{i=1}^{m} t_i$

5.2 Motivation and contribution

Information security has grown much more since electronic communication started. Now it is part of our daily life. The cryptographic secret key, which is used for securing the information, is shared among the group of players by a dealer in the distribution process. Initially, secret sharing schemes are proposed to solve problems that arise

in application such as safeguarding cryptographic keys. Later, several useful applications have been identified in various cryptographic protocols. Nowadays, it is widely used in many interesting applications including multi-party computations, threshold cryptography, generalised oblivious transfer protocol, missile launching, and biometric authentication system. This chapter mainly contributes to the development of a another multi secret sharing protocol and also explores its uses in typical areas of application. We proposed a multi-secret sharing scheme for the compartmented access structure by using modular inverse. The reconstructed secret can be verified whether it is correct or not, and no participant in a compartment knows other compartment secrets. The proposed secret sharing scheme uses Shamir's scheme first to reconstruct the compartment secret then combines them into the requested secret. The scheme is ideal as well as perfect. Our proposed scheme can be applied in the following situation: Suppose an organization has a confidential project. To make work easier and for on time delivery, the management divides the project into different modules. Each module is given to a different team, where each team consists of a set of employees. In order to achieve the project's confidentiality, they can use any encryption scheme but applying an encryption scheme and having the key for each employee is a time consuming and costly process with the risk of key losses. Therefore, distribute the key to any employee in each team by using the proposed scheme instead of other encryption scheme.

5.3 Proposed Scheme

5.3.1 Overview of the proposed scheme

We have introduced a new "multi secret sharing scheme" for the compartment access structure. In this scheme set of n number of participants $\mathcal{P} = p_1, p_2, \ldots, p_n$ is partitioned into m distinct compartments $C_1, C_2, \ldots, C_m$. The dealer choose a set of m co-prime integers $c_1, c_2, \ldots, c_m$ as the compartment secrets for their corresponding compartments. The dealer calculates partial secrets ℓ_i using compartmental secrets $c_i, 1 \leq i \leq m$ and adds all the partial secret to get pseudo secret $s = \sum_{i=1}^{m} \ell_i$. Then dealer computes shift values Z_j by adding pseudo secret s to actual secrets S_j. i.e., $Z_j = s + S_j$, $1 \leq j \leq k$ and make it public. Now dealer applies the Shamir's secret sharing scheme to distribute shares of the compartment secrets c_i to the participants of corresponding compartments C_i. While reconstructing the secret, the participants

of the corresponding compartment first apply Lagrange interpolation and recover the corresponding compartment secrets c_i. They compute partial secret ℓ_i at corresponding compartments and add all partial secrets ℓ_i to get pseudo secret s. Then to recover actual secrets S_j, Subtract pseudo secrets from the corresponding shift values Z_j, which are public values.

5.3.2 Algorithm

Following are the proposed scheme algorithm.

Algorithm 6: Initialization:

1: Let $\mathcal{P} = \{p_1, p_2, p_3, \ldots, p_n\}$ be the group of n participants divided into m different compartments.
2: Let $\{C_1, C_2, \ldots, C_m\}$ be the m compartments.
3: Each compartment C_i is associated with (t_i, n_i) threshold access structure, where n_i represents total number of participants and t_i represents threshold for compartment C_i, $i \in \{1, 2, \ldots, m\}$.
4: Choose k secrets i.e, $S_1, S_2, \ldots, S_k$
5: Choose m pairwise co-prime integers i.e, $c_1, c_2, \ldots, c_m$ s.t. $GCD(c_i, c_j) = 1, \forall i \neq j$ as the compartmented secret.
6: Choose a large prime q.
7: id_u^i: denotes as the identifier of the participants u at the compartment i, where $1 \leq u \leq n_i$ and $1 \leq i \leq m$,

Algorithm 7: Share Distribution:

1: Calculate $c = c_1 \times c_2 \times \cdots c_m$

2: Compute the pseudo secret $s = \sum_{i=1}^{m} \ell_i$, where $\ell_i = (\frac{-c}{c_i})^{-1} \mod c_i$

3: Compute shift value $Z_j = s + S_j$, where $1 \leq j \leq k$

4: **for** $i = 1 \rightarrow m$ **do**

- Choose $t_i - 1$ positive integers randomly from F_q s.t, $a_1^i, a_2^i, \ldots, a_{t_i-1}^i$, and let $a_0^i = c_i$
- Construct the polynomial of degree $t_i - 1$, $F(x) = a_0^i + a_1^i \times x + \cdots + a_{t_i-1}^i \times x^{(t_i-1)}$
- Compute $Shr_u^i = F(id_j^i) \bmod q$, $1 \leq u \leq n_i$

5: Distribute shares Shr_u^i to the respective participants via secure channel and make c and Z_j values public, where $1 \leq j \leq k$, $1 \leq u \leq n_i$ and $1 \leq i \leq m$.

Algorithm 8: Share Reconstruction:

1: Authorised subset of any t_i or more than t_i participants using their ID's id_u^i and shares Shr_u^i from compartment C_i can reconstruct compartmented secret c_i, $1 \leq i \leq m$ and $1 \leq u \leq n_i$ by computing Lagrange interpolation formula as follows:

2: **for** $i = 1 \rightarrow m$ **do**

- Calculate compartmented secrets :

$$c_i = \sum_{u=1}^{t} shr_u^i \prod_{k=1, k \neq u}^{t} \frac{id_k^i}{id_k^i - id_u^i} \mod q$$

- Compute $\ell_i = (\frac{-c}{c_i})^{-1} \mod c_i$

5: Calculates pseudo secret $s = \sum_{i=1}^{m} \ell_i$

6: Computes Actual secrets $S_j = Z_j - s$, $1 \leq j \leq k$

Algorithm 9: Secret Verification:

1: $x = \sum_{i=1}^{m} \{\ell_i \times (\frac{c}{c_i})\} + \frac{1}{c}$

2: if x is any integer.

3: secret may be correct.

4: else secret is wrong.

5.3.3 Example

SAGE and Python are used for implementing the scheme. We hereby explain with a simple example showing our proposed Multi-stage multi-secret sharing scheme for Compartment access structure with artificially small parameters. We considered field with smaller prime for easy understanding.

1. *Initialization:*

   - Suppose total number of participants are $n = 15$. These participants are partitioned into three disjoint compartments C_1, C_2, C_3 such that threshold values and number of participants of the corresponding compartment as (t_1, n_1) is (2, 4), (t_2, n_2) is (3, 6) and (t_3, n_3) is (3, 5).
   - Choose $k = 4$ secrets i.e $S_1 = 11, S_2 = 13, S_3 = 15, S_4 = 17$
   - Choose 3 pairwise co-prime integers be $c_1 = 143, c_2 = 35, c_3 = 6$. These are the compartmented secrets.
   - Let prime $q = 151$.
   - ID's of the 1^{st} compartment participants be
     $id_1^1 = 1, id_2^1 = 2, id_3^1 = 3, id_4^1 = 4,$
     2^{nd} compartment participants ID's be
     $id_1^2 = 5, id_2^2 = 6, id_3^2 = 7, id_4^2 = 8, id_5^2 = 9, id_6^2 = 10$ and
     3^{rd} compartment participants ID's be
     $id_1^3 = 11, id_2^3 = 12, id_3^3 = 13, id_4^3 = 14, id_5^3 = 15,$

2. *Distribution:*

   - Compute $c = c_1 \times c_2 \times c_3 = 143 \times 35 \times 6 = 30030$
   - Calculate pseudo secret
     $s = \sum_{i=1}^{m} (\frac{-c}{c_i})^{-1} \mod c_i = 70$
   - Compute shift values $Z_j = S_j + s$, $1 \leq j \leq k$;
   - $Z_1 = 11 + 70 = 81$, $Z_2 = 13 + 70 = 83$,
     $Z_3 = 15 + 70 = 85$, $Z_4 = 17 + 70 = 87$
   - At compartment $C_1, t_1 = 2, n_1 = 4, c_1 = 143$

- $F(x) = c_1 + 3 \times x = 143 + 3 \times x$
- Compute shares $Shr_1^1 = 146, Shr_2^1 = 149,$
  $Shr_3^1 = 1, Shr_4^1 = 4$

- At compartment $C_2, t_2 = 3, n_2 = 6, c_2 = 35$
  - $F(x) = c_2 + 3 \times x + 4 \times x^2 = 35 + 3 \times x + 4 \times x^2$
  - Compute shares $Shr_1^2 = 150, Shr_2^2 = 46,$
    $Shr_3^2 = 101, Shr_4^2 = 13, Shr_5^2 = 84, Shr_6^2 = 12$

- At compartment $C_3, t_3 = 3, n_3 = 5, c_3 = 6$
  - $F(x) = c_3 + 2 \times x + 3 \times x^2 = 6 + 2 \times x + 3 \times x^2$
  - Compute shares $Shr_1^3 = 89, Shr_2^3 = 9,$
    $Shr_3^3 = 86, Shr_4^3 = 18, Shr_5^3 = 107$

3. *Reconstruction:*

- Any t_i or more than t_i participants from an authorized set can reconstruct the secrets. Using their ID's $id_u^i$and shares Shr_u^i each compartment reconstructs compartmented secret c_i by computing Lagrange interpolation formula.

- **Compartment secret reconstruction at compartment** C_1
  - Suppose participant 2^{nd} and 3^{rd} want to reconstruct the secret by sharing their ID's and shares $Shr_2^1 = 149, Shr_3^1 = 1$ respectively.
  - Apply Lagrange polynomial interpolation on $(2, 149), (3, 1)$ and gets
    $c_1 = \sum_{u=1}^{2} shr_u^1 \prod_{k=1, k\neq j}^{2} \frac{id_k^1}{id_k^i - id_u^1} \mod q$
    $c_1 = 149 \times (\frac{3}{3-2}) + 1 \times (\frac{2}{2-3}) \mod 151$
    $= 445 \mod 151 = 143$
  - $\therefore c_1 = 143$
  - Compute partial secret $\ell_1 = (\frac{-c}{c_1})^{-1} \mod c_1$
  - Compute partial secret
    $\ell_1 = (\frac{-30030}{143})^{-1} \mod 143 = 32$

- **Compartment secret reconstruction at compartment** C_2

- Suppose participant 1^{st}, 2^{nd} and 3^{rd} want to reconstruct the secret by sharing their ID's and shares $Shr_1^2 = 150, Shr_2^2 = 46, Shr_3^2 = 101$ respectively.
- Apply Lagrange polynomial interpolation on $(5, 150), (6, 46), (7, 101)$ and gets
  $c_2 = \sum_{u=1}^{3} shr_u^2 \prod_{k=1,k\neq u}^{3} \frac{id_k^2}{id_k^2 - id_u^2} \mod q$
  $c_2 = 150 \times (\frac{6}{6-5}) \times (\frac{7}{7-5}) + 46 \times (\frac{5}{5-6}) \times (\frac{7}{7-6}) + 101 \times (\frac{5}{5-7}) \times (\frac{6}{6-7}) \mod 151$
  $= 3055 \mod 151 = 35$
- $\therefore c_2 = 35$
- Compute partial secret $\ell_2 = (\frac{-c}{c_2})^{-1} \mod c_2$
- Compute partial secret
  $\ell_2 = (\frac{-30030}{35})^{-1} \mod 35 = 33$

- **Compartment secret reconstruction at compartment** C_3
  - Suppose participant 2^{nd}, 3^{rd} and 4^{th} want to reconstruct the secret by sharing their ID's and shares $Shr_2^3 = 9, Shr_3^3 = 86, Shr_4^3 = 18$ respectively
  - Apply Lagrange polynomial interpolation on $(12, 9), (13, 86), (14, 18)$ and gets
    $c_3 = \sum_{u=1}^{3} shr_u^3 \prod_{k=1,k\neq u}^{3} \frac{id_k^3}{id_k^3 - id_u^3} \mod q$
    $c_3 = 9 \times (\frac{13}{13-12}) \times (\frac{14}{14-12}) + 86 \times (\frac{12}{12-13}) \times (\frac{14}{14-13}) + 18 \times (\frac{12}{12-14}) \times (\frac{13}{13-14}) \mod 151$
    $= -12225 \mod 151 = 6$
  - $\therefore c_3 = 6$
  - Compute partial secret $\ell_3 = (\frac{-c}{c_3})^{-1} \mod c_3$
  - Compute partial secret
    $\ell_3 = (\frac{-30030}{6})^{-1} \mod 6 = 5$

- Calculate pseudo secret $s = \sum_{i=1}^{m} \ell_i = 32 + 33 + 5 = 70$
- Compute Secret $S_1 = Z_1 - S = 81 - 70 = 11$, $S_2 = Z_2 - S = 83 - 70 = 13$, $S_3 = Z_3 - S = 85 - 70 = 15$, $S_4 = Z_4 - S = 87 - 70 = 17$

5.4 Comparison with existing scheme

5.5 Security Analysis

This section discusses the security analysis of the proposed "multi-secret sharing scheme" for compartmented access structure assuming that dealer is honest and the communication channels between two connecting networks are reliable, so that information cannot leak to the non-authenticating network. Subsequently,, we have discussed the security analysis for the outside adversaries and inside adversaries.

Following are the possible attacks:

- Unauthorised group of participants tries to recover the partial secret ℓ_i at i^{th} compartment , $1 \leq i \leq m$.
- Less than m compartments participant tries to recover the j^{th} secret, $1 \leq j \leq k$.
- Outside adversary tries to recover the secrets S_j using the available public values Z_j, $1 \leq j \leq k$.

Lemma1: Unauthorised group of participants tries to get the secret ℓ_i at i^{th} compartment .
Proof: Partial secret ℓ_i can only be gained when c_i is known and it is distributed using Shamir's (t_i, n_i) threshold scheme. Less than t_i participants can not obtain c_i, which is essential to get ℓ_i. Therefore, unauthorised set of participants can not get ℓ_i at i^{th} compartment.

Lemma2: Less than m compartments participant tries to get the j^{th} secret S_j.
Proof: The j^{th} secret S_j can be recovered by subtracting pseudo secret s from available j^{th} public values Z_j. However, pseudo secret s is sum of all the m compartmented secrets. Therefore, less than m compartment participants can not recover the j^{th} secret S_j.

Lemma3: Outside adversary tries to recover the secrets S_j using the available public values Z_j.

Proof: Recovery of any secret S_j requires public value Z_j and pseudo secret s. Pseudo secret s can be computed only by authorised participants of all the compartments. Hence, outside adversary cannot obtain the secret S_j using the public values Z_j only.

Privacy

The secrets can be recovered by an authorised group of participants; while an unauthorised group of participants cannot recover the secrets. In the proposed scheme no one knows other compartment secret. As every compartment uses Shamir's secret sharing to distribute the shares to its participants, at least t or more than t participants must cooperate in order to get the compartment secret. Therefore no outside adversary can cheat to get the compartment secret.

5.6 Conclusions

In this chapter, we presented a new "multi-secret sharing scheme" that realises the compartmented access structure by using the concept of modular inverse. It can check whether the reconstructed secret is correct or not, and no compartment participant knows another compartment secret. The proposed "multi-secret sharing scheme for the compartmented access structure" uses Shamir's scheme in order to recover the partial secrets and combines it into the actual secret. The secret can only be obtained if the threshold number of participants in each compartment reconstructs their compartment secret and participates during the recovery of the secret. Security analysis is carried out on possible attacks by both the inside as well as outside adversaries. The proposed scheme may be improved to use only one polynomial for sharing all the secrets in a compartment.

Chapter 6

New Multi-secret Sharing Scheme based on Superincreasing Sequence for Level-ordered Access Structure

In the previous chapters, we have proposed the scheme for sharing multiple secrets which realizes compartmented access structure. In this chapter, a new multi-secret sharing scheme (MSSS) that uses a superincreasing sequence and realizes Level-Ordered Access Structure (LOAS) is proposed. The novelty of the scheme is that not only a single share for all the secrets is sufficient but also the secrets can be changed without renewing the shares of the participants. The proposed scheme has low communication cost and less overhead.

6.1 Introduction

There are several access structures including the (t, n)-threshold access structures, hierarchical access structures, compartmented access structures and generalized access structures in literature[31, 44, 69], which are discussed and explained in detailed in the chapter 2. A new access structure named as a Level-ordered access structure (LOAS) that is distinct from all the existing multipartite access structures proposed by Dileep et. el [58] in 2016. In Level-ordered access structure(LOAS), a set of participants are

divided into different levels; each level is associated with a threshold, and also there is an ordering imposed on the levels while reconstructing the secret. This shows that the players must apply their shares according to predefined order of level, to recover the secret. Otherwise, the secret cannot be recovered".

6.2 Motivation and contribution

In a software industry, an application can be released to production only after it has gone through unit testing, integration testing, then system testing and final approval testing. It is to be noted here that without the completion of unit testing, integration testing cannot be started and similarly without the completion of integration testing, system testing cannot be started and so on. To realize a similar kind of activity we need a hierarchical access structure that has an inbuilt ordering amid the levels. Existing access structures fail to realize this scenario as they are short of enforcing the required ordering. The purpose of this work is to propose a scheme that caters to this kind of scenarios and come up with schemes that realize this access structure for the multiple secrets".

In this chapter, we have proposed a new multi secret sharing scheme for LOAS. The important fallout of this access structure is that the actual secret can be recovered only after the reconstruction of all the compartment(level) secrets. Compartment secrets can be constructed at the same time. However, constructing the actual secret requires adherence to the hierarchy. The Shamir's secret sharing scheme is used at each level to distribute and recover the compartment secret. In the proposed scheme, there is no ordering among the recovery of actual secrets, which shows that the i^{th} secret can be recovered without recovery of $(i-1)^{th}$ or $(i+1)^{th}$ secret and also there is no relation between the number of levels and the number of secrets. That means the number of secrets and the number of levels are independent.

The proposed scheme has the property of secret changeability without any changes to the compartment secret shares. It can be done as the actual secret is not the only function of compartment shares. This implies that the dealer can modify the secret many times without modifying compartment secrets. This re-usability feature add up to our proposed scheme, hence it avoids the overhead during the communication phase of share distribution to the participants. Whenever the secret changes, public value

is declared by the dealer based on the secret and compartment shares. Then, with the help of current public value along with the same compartment secret shares, the compartments together can obtain the actual secret. For each change in the secret, the compartments have to recover the current secret based on their current public value and the secret compartment shares because the old secret is not valid any more.

6.3 Proposed scheme

Overview of proposed scheme

New multi-secret sharing scheme for level ordered access structure based on superincreasing sequence, consists of two phases:

- Share distribution phase :
- Secret reconstruction phase:

It can be visualize in figure 6.1 and 6.2. Consider the $\mathcal{P} = p_1, p_2, \ldots, p_n$ denotes a group of n participants and k be the number of secrets. Suppose participants are divided into m disjoint levels $L_1, L_2, \ldots, L_m$. Let n_i is the total number of participants and $t_i(\leq n_i)$ is threshold at i^{th} level, where $1 \leq i \leq m$ and global threshold t, is the summation of all the levels threshold in our proposed scheme. Let us denote the i^{th} row of a matrix M by M_i

6.3.1 Share distribution:

Following steps are performed by the dealer:

1. Choose $k \times 1$ secret vector S;

$$S = \begin{pmatrix} s_1 \\ s_2 \\ \cdots \\ s_k \end{pmatrix}$$

where $s_i \in \mathbb{Z}_{2^{m-1}} - \{0\}$, i.e. s_i is a nonzero $m-1$ bit number, $1 \leq i \leq k$;

2. Convert secret vector S into $k \times (m-1)$ secret matrix SM;

$$SM = \begin{pmatrix} s_{1,m-1} & s_{1,m-2} & \cdots & s_{1,1} \\ s_{2,m-1} & s_{2,m-2} & \cdots & s_{2,1} \\ \cdots & \cdots & \cdots & \cdots \\ s_{k,m-1} & s_{k,m-2} & \cdots & s_{k,1} \end{pmatrix}$$

where SM_i is the $m-1$ bit binary representation of s_i, for $i \in \{1, 2, \ldots, k\}$;

3. Generate a random $k \times (m-1)$ temp matrix TM;

$$TM = \begin{pmatrix} e_{1,m-1} & e_{1,m-2} & \cdots & e_{1,1} \\ e_{2,m-1} & e_{2,m-2} & \cdots & e_{2,1} \\ \cdots & \cdots & \cdots & \cdots \\ e_{k,m-1} & e_{k,m-2} & \cdots & e_{k,1} \end{pmatrix}$$

4. Calculate $SM' = exor(SM, TM)$

$$SM' = \begin{pmatrix} s'_{1,m-1} & s'_{1,m-2} & \cdots & s'_{1,1} \\ s'_{2,m-1} & s'_{2,m-2} & \cdots & s'_{2,1} \\ \cdots & \cdots & \cdots & \cdots \\ s'_{k,m-1} & s'_{k,m-2} & \cdots & s'_{k,1} \end{pmatrix}$$

where bits $s'_{i,j} = s_{i,j} \oplus e_{i,j}$ for $i \in \{1, 2, \ldots, k\}, j \in \{1, 2, \ldots, m-1\}$ and $\oplus$ defines the *exor* operation.

5. Generate $(m-1) \times 1$ superincreasing vector XM;

$$XM = \begin{pmatrix} x_{m-1} \\ x_{m-2} \\ \cdots \\ x_1 \end{pmatrix}$$

where $x_{m-1}, x_{m-2}, \cdots, x_1$ is a superincreasing sequence.

6. Calculate public vector $U = bagsum(SM', XM)$;

$$U = \begin{pmatrix} u_1 \\ u_2 \\ \cdots \\ u_k \end{pmatrix} = SM' \times XM$$

7. Select a prime q, and $q > \sum_{i=1}^{m-1} x_i$

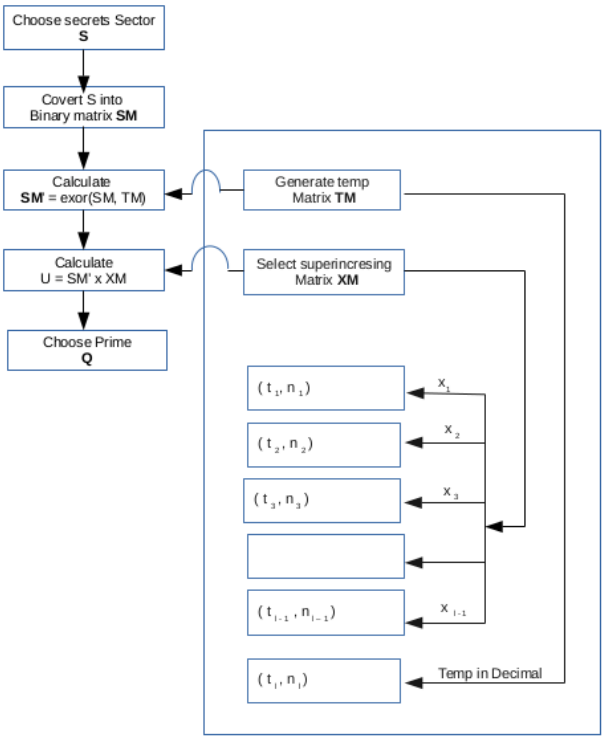

Figure 6.1: Share Distribution.

8. Distribute the shares of x_i to all the corresponding participants in level i by applying Shamir's (t_i, n_i) share distribution, where $i \in \{1, 2, \ldots, m-1\}$;

9. Distribute the shares of decimal equivalents of the rows TM_i, $1 \leq i \leq k$, of the temp matrix TM to level m by applying Shamir's (t_m, n_m) share distribution.

Note:

- q, U is public. S, SM, TM, SM', XM are not public, but known to dealer.
- The share distribution phase can be summarized in simple and informal language as: SM is the binary Matrix for S. $SM' = SM \oplus TM$.
- Level m participants receive k shares each corresponding to the decimal equivalents of the k rows of the temp matrix TM.

6.3.2 Secret reconstruction:

In order to reconstruct secret s_r, where $r \in \{1, 2, 3, \cdots, k\}$, the following operations are carried out. which can be visualize in figure 6.2

1. Any t_i or more than t_i participants of level i perform (t_i, n_i) Shamir's secret reconstruction and get the corresponding level share x_i. where, $i \in \{1, 2, \ldots, m-1\}$;

2. Check whether $u_r \geq x_1$ is at Level 1

   - If true, then bit 1 is the output of level 1 and sends $u'_{r,1,2} = u_r - x_1$ to the level 2.
   - Otherwise, bit 0 is the output and sends $u'_{r,1,2} = u_r$ to the level 2 and
   - Appends its output bit (which is $s'_{r,1}$) to the empty tuple (let say SM''_r);

3. For $i = 2 \rightarrow m-1$, check whether $u'_{r,i-1,i} \geq x_i$ is at Level i

   - If true, bit 1 is the output of level i and sends $u'_{r,i,i+1} = u'_{r,i-1,i} - x_i$ to the next level $i+1$.
   - Otherwise, bit 0 is the output and sends $u'_{r,i,i+1} = u'_{r,i-1,i}$ to the next level $i+1$. and
   - Appends the output bit (which is $s'_{r,i}$) to the starting index of the tuple SM''_r;

4. Level m performs (t_m, n_m) Shamir's secret reconstruction corresponding to the r^{th} shares and converts the result into $m-1$ bit binary tuple, which is $TM_r = [e_{r,m-1}, e_{r,m-2}, e_{r,m-3} \cdots e_{r,3}, e_{r,2}, e_{r,1}]$. Then compute $exor(TM_r, SM''_r)$ which results in binary tuple SM_r;

5. Finally, to obtain the secret s_r, the secret binary tuple SM_r is converted to decimal.

Note: Since TM is distributed in the last level m, even though remaining $m-1$ levels get the associated bit values, they cannot get secret binary tuple SM_r.

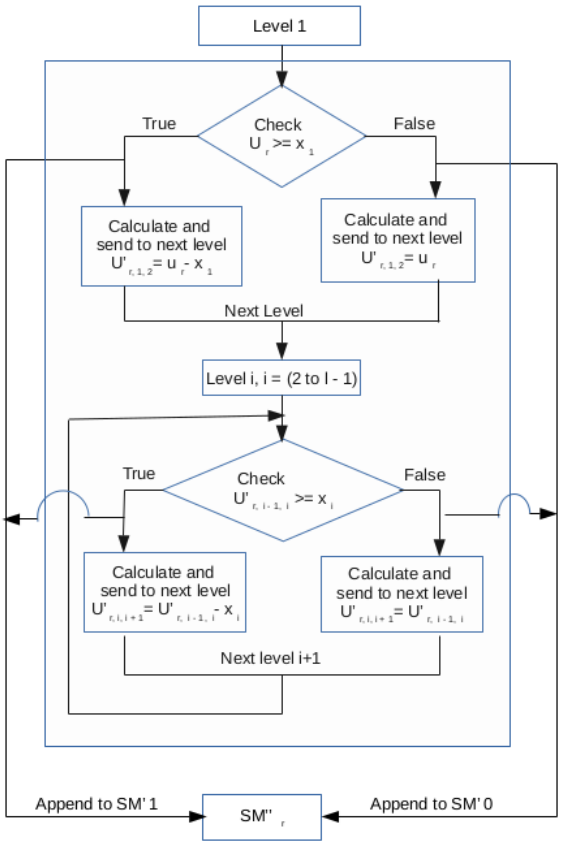

Figure 6.2: Secret Reconstruction.

6.4 Explanation with an example

SAGE and Python are used for implementing the scheme. Following example illustrates our proposed multi-stage multi-secret sharing scheme for Level order Structure with artificially small parameters. We considered field with smaller prime for easy understanding.

6.4.1 Share distribution:

Let the number of levels m be 9 and the number of secrets k be 6. Also, for each level, consider the following threshold values and the total number of participants: $(t_1, n_1) = (4, 6)$, $(t_2, n_2) = (2, 5)$, $(t_3, n_3) = (3, 5)$, $(t_4, n_4) = (4, 5)$, $(t_5, n_5) = (5, 6)$, $(t_6, n_6) = (3, 6)$, $(t_7, n_7) = (5, 7)$, $(t_8, n_8) = (4, 6)$, $(t_9, n_9) = (4, 7)$. Let $1, 2, 3 \cdots n_i$ be the participants public identities for compartment (level) i.

The following steps have to be performed by the dealer:

1. Selects 6×1 secret vector

$$S = \begin{pmatrix} 27 \\ 166 \\ 95 \\ 173 \\ 119 \\ 178 \end{pmatrix}$$

Since $m = 9$, $\mathbb{Z}_{2^{m-1}} - \{0\} = \{1, 2, 3 \cdots 255\}$

2. Convert secret vector S into 6×8 secret matrix SM; [Binary representation of secret]

$$\boldsymbol{SM} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}$$

3. Generate random 6×8 temp matrix

$$\boldsymbol{TM} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \end{pmatrix}$$

4. Calculate $SM' = exor(SM, TM)$

$$\boldsymbol{SM'} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

5. Generate 8×1 superincreasing vector

$$\boldsymbol{XM} = \begin{pmatrix} \mathbf{10} \\ \mathbf{11} \\ \mathbf{24} \\ \mathbf{51} \\ \mathbf{108} \\ \mathbf{206} \\ \mathbf{420} \\ \mathbf{836} \end{pmatrix}$$

6. Calculate public vector $U = bagsum(SM', XM)$;

$$\boldsymbol{U} = \begin{pmatrix} \mathbf{688} \\ \mathbf{183} \\ \mathbf{552} \\ \mathbf{1093} \\ \mathbf{1114} \\ \mathbf{1006} \end{pmatrix}$$

7. Choose a prime q, which should be greater than the sum of superincreasing sequence matrix XM, and make q as public; $\boldsymbol{x_8+x_7+x_6+x_5+x_4+x_3+x_2+x_1 = 10+11+24+51+108+206+420+836 = 1666}$
   Therefore, Let $q = 1669$

8. Distribute shares of x_i to all the corresponding participants in level i using Shamir's (t_i, n_i) share distribution for $1 \leq i \leq 8$. The result is shown in Table 6.1

9. Distribute the shares of decimal equivalents of rows TM_i, $1 \leq i \leq 6$, of the temp matrix TM to last level $m = 9$, using Shamir's (t_m, n_m) share distribution. The result is shown in Table 6.2

6.4.2 Secret reconstruction of s_r

Let r be 5. In order to reconstruct fifth secret s_5, the following steps are followed

1. Any t_i or more than t_i participants of level i perform (t_i, n_i) Shamir's secret reconstruction and get the corresponding level share x_i, for $1 \leq i \leq 8$. The results are shown in Table 6.3

2. Check whether $u_5 \geq x_1$ is at Level 1.

   - If it is true, then bit 1 is the output of level 1 and it sends $u'_{5,1,2} = u_5 - x_1$ to the level 2

6. MULTI SSS USING SUPERINCREASING SEQUENCE FOR LOAS

Table 6.1: Shamir's share distribution at compartments(level), $m = 1$ to 8

Level number	$(\mathbf{t_i}, \mathbf{n_i})$	**Polynomial**	**Share list (Public identity, Share value)**
1	(4,6)	$836 + 3x + 4x^2 + 8x^3$	$(1, 851), (2, 922), (3, 1097), (4, 1424), (5, 282), (6, 1057)$
2	(2,5)	$420 + 5x$	$(1, 425), (2, 430), (3, 435), (4, 440), (5, 445)$
3	(3,5)	$206 + 4x + 2x^2$	$(1, 212), (2, 222), (3, 236), (4, 254), (5, 276)$
4	(4,5)	$108 + 6x + 2x^3$	$(1, 116), (2, 136), (3, 180), (4, 260), (5, 388)$
5	(5,6)	$51 + 4x + 2x^3 + 2x^4$	$(1, 59), (2, 107), (3, 276), (4, 707), (5, 1571), (6, 1430)$
6	(3,6)	$24 + 3x + 2x^2$	$(1, 29), (2, 38), (3, 51), (4, 68), (5, 89), (6, 114)$
7	(5,7)	$11 + 3x + 2x^4$	$(1, 16), (2, 49), (3, 182), (4, 535), (5, 1276), (6, 952), (7, 1496)$
8	(4,6)	$10 + 4x + 2x^3$	$(1, 16), (2, 34), (3, 76), (4, 154), (5, 280), (6, 466)$

Table 6.2: Shamir's share distribution at last compartment(level), m =9

$(\mathbf{t_m}, \mathbf{n_m})$	TM_r $1 \leq r \leq k$	**Polynomial**	**Share list (Public identity, Share value)**
(4,7)	1	$77 + 2x + 3x^2 + 5x^3$	$(1, 87), (2, 133), (3, 245), (4, 453), (5, 787), (6, 1277), (7, 284)$
	2	$158 + 2x + 3x^2 + 5x^3$	$(1, 168), (2, 214), (3, 326), (4, 534), (5, 868), (6, 1358), (7, 365)$
	3	$117 + 2x + 3x^2 + 5x^3$	$(1, 127), (2, 173), (3, 285), (4, 493), (5, 827), (6, 1317), (7, 324)$
	4	$184 + 2x + 3x^2 + 5x^3$	$(1, 194), (2, 240), (3, 352), (4, 560), (5, 894), (6, 1384), (7, 391)$
	5	$162 + 2x + 3x^2 + 5x^3$	$(1, 172), (2, 218), (3, 330), (4, 538), (5, 872), (6, 1362), (7, 369)$
	6	$107 + 2x + 3x^2 + 5x^3$	$(1, 117), (2, 163), (3, 275), (4, 483), (5, 817), (6, 1307), (7, 314)$

- Otherwise, bit 0 is the output of level 1 and sends $u'_{5,1,2} = u_5$ to the level 2 and
- Appends its output bit to an empty tuple (let say SM''_5).

The result of this step is shown in Table 6.4

3. For $i = 2 \rightarrow m-1$, check whether $u'_{5,i-1,i} \geq x_i$ is at Level i
   - If it is true, bit 1 is the output of level i and sends $u'_{5,i,i+1} = u'_{5,i-1,i} - x_i$ to the next level $i+1$.
   - Otherwise, bit 0 is the output of level i and sends $u'_{5,i,i+1} = u'_{5,i-1,i}$ to the next level $i+1$. and
   - Appends the output bit (which is $s'_{r,i}$) to the starting index of the tuple SM''_5;

   The result of this step is shown in Table 6.5

4. Last level $m = 9$ performs (t_m, n_m) Shamir's secret reconstruction. The result of this step is shown in Table 6.6

   These results are then converted into $m-1$ bit tuple, i.e.

$$TM_5 = [e_{5,m-1}, e_{5,m-2}, e_{5,m-5} \cdots e_{5,3}, e_{5,2}, e_{5,1}]$$

   Note: It is enough to reconstruct TM_5 in order to reconstruct s_5, but in table 6.6, the total TM matrix is reconstructed(in decimal) for completeness. Level m performs $exor(TM_5, SM''_5)$ which results in SM_5.

$$\boldsymbol{TM_5 = 162 = (10100010)_2, \therefore TM_5 \oplus SM''_5 \implies SM_5}$$
$$\boldsymbol{[1,0,1,0,0,0,1,0] \oplus [1,1,0,1,0,1,0,1] = [0,1,1,1,0,1,1,1]}$$

5. Finally, the secret binary tuple SM_5 is converted to decimal to get the secret s_5.

$$\boldsymbol{s_5 = (01110111)_2 = 119}$$

Table 6.3: Shamir's secret reconstruction at compartments(level), $m = 1$ to 8

Level number	$(\mathbf{t_i}, \mathbf{n_i})$	**Interested participants with shares**	**Compartmental share (Lagrange interpolation)**
1	(4,6)	(1,851), (3,1097), (5,282), (6,1057)	$\frac{9}{4}(851) + \frac{-5}{2}(1097) + \frac{9}{4}(282) - 1057 \equiv \mathbf{836} \mod 1669$
2	(2,5)	$(1, 131), (3, 133)$	$\frac{3}{2}(131) + \frac{-1}{2}(133) \equiv \mathbf{420} \mod 1669$
3	(3,5)	(1,65), (3,93), (5,145)	$\frac{15}{8}(65) + \frac{-5}{4}(93) + \frac{3}{8}(145) \equiv \mathbf{206} \mod 1669$
4	(4,5)	(1,35), (3,69), (4,110), (5,175)	$\frac{5}{2}(35) + (-5)(69) + 5(110) + \frac{-3}{2}(175) \equiv \mathbf{108} \mod 1669$
5	(5,6)	(1,20), (2,95), (3,368), (4,402), (5,473)	$5(20) + (-10)(95) + 10(368) +$ $(-5)(402) + 1(473) = 1293 \equiv \mathbf{51} \mod 1669$
6	(3,6)	(1,11), (3,19), (6,46)	$\frac{9}{5}(11) + (-1)(19) + \frac{1}{5}(46) \equiv \mathbf{24} \mod 1669$
7	(5,7)	(1,16), (2,49), (3,182), (4,535), (5,1276)	$5(16) + (-10)(49) + 10(182) +$ $(-5)(535) + 1(1276) \equiv \mathbf{11} \mod 1669$
8	(4,6)	(1,16), (3,76), (5,280),(6,466)	$\frac{9}{4}(16) + \frac{-5}{2}(76) + \frac{9}{4}(280) - 466 \equiv \mathbf{10} \mod 1669$

Table 6.4: Output bit from level 1

Level number	$\mathbf{u_5}$	$\mathbf{x_1}$	$\mathbf{u_5 \geq x_1}$	**Output bit**	$\mathbf{u'_{5,1,2}}$	$\mathbf{SM''_5}$
1	1114	836	True	1	$1114 - 836 = 278$	[1]

Table 6.5: Output bits from level 2 to level 8

Level number	$\mathbf{u'_{5,i-1,i}}$	$\mathbf{x_i}$	$\mathbf{u'_{5,i-1,i} \geq x_i}$	**Output bit**	$\mathbf{u'_{5,i,i+1}}$	$\mathbf{SM''_5}$
2	278	420	False	0	278	[0,1]
3	278	206	True	1	$278 - 206 = 72$	[1,0,1]
4	72	108	False	0	72	[0,1,0,1]
5	72	51	True	1	$72 - 51 = 21$	[1,0,1,0,1]
6	21	24	False	0	21	[0,1,0,1,0,1]
7	21	11	True	1	$21 - 11 = 10$	[1,0,1,0,1,0,1]
8	10	10	True	1	10-10=0	[1,1,0,1,0,1,0,1]

Table 6.6: Shamir's share reconstruction at last level ($m = 9$) compartment

$(\mathbf{t_l}, \mathbf{n_l})$	TM_r	**Interested participants with shares**	**Compartmental share (Lagrange interpolation)**
(4,7)	1	(1,87), (2,133), (3,245), (4,453)	$4(87) - 6(133) + 4(245) - 1(453) \equiv 77 \mod 1669$
	2	(2,214), (3,326), (4,534), (6,1358)	$9(214) - 16(326) + 9(534) - 1(1358) \equiv 158 \mod 1669$
	3	(3,285), (4,493), (6,1317), (7,324)	$14(285) - 21(493) + 14(1317) - 6(324) \equiv 117 \mod 1669$
	4	(1,194), (3,352), (6,1384), (7,391)	$\frac{21}{10}(194) - \frac{7}{4}(352) + \frac{7}{5}(1384) - \frac{3}{4}(391) \equiv 184 \mod 1669$
	5	(1,172), (2,218), (3,330), (7,369)	$\frac{7}{2}(172) - \frac{21}{5}(218) + \frac{7}{4}(330) - \frac{1}{20}(369) \equiv 162 \mod 1669$
	6	(1,117), (2,163), (3,275), (4,483)	$4(117) - 6(163) + 4(275) - 1(483) \equiv 107 \mod 1669$

6.5 Secret changeability with an illustration

6.5.1 Secret changeability

In our proposed scheme, the shares are reusable, which means that the participants shares can remain the same and can be reused for a new secret. The following is the dealer secret renewal algorithm.

6.5.1.1 Secret renewal:

The following steps have to be performed by dealer:

1. Select $k \times 1$ new secret vector

$$nS = \begin{bmatrix} ns_1 \\ ns_2 \\ \cdots \\ ns_k \end{bmatrix}$$

   where $ns_i \in \mathbb{Z}_{2^{m-1}} - \{0\}$, for $1 \leq i \leq k$;

2. Compute $nSM = k \times (m-1)$ matrix, binary representation of s_i for $1 \leq i \leq k$;

3. Calculate $nSM' = nSM \oplus TM$

4. Calculate public matrix $nU = nSM' \times XM$

Table 6.7: Shows the parameter values change

Parameter	**Previous value**	**New value**	**Change in parameter**
Secret vector	S	NS	Yes
Secret Matrix	SM	nSM	Yes
exor Matrix	SM'	nSM'	Yes
Temp matrix	TM	TM	No
Super increasing vector	XM	XM	No
Public vector	U	nU	Yes
Prime number	q	q	No

There are changes only in the secret, secret matrix, *exor* matrix and public value and remaining parameters will be the same. Since superincreasing vector XM holds the compartment secret shares for levels from 1 to $m-1$ and decimal equivalent rows of the Temp matrix TM is the compartment secret share for last level m, the compartment shares remain the same after dealer changes the secret. As the compartment shares remain the same, the distribution phase is not required after the secret update. There is no change in the secret reconstruction phase. Based on the new public value nU, the actual secret can be recovered using corresponding level secrets. The changes in the parameter's values after applying the secret renewal algorithm are listed in Table 6.7

6.5.2 Secret changeability example

The same example used in section 5 is being used here to illustrate secret renewal algorithm. So, the total number of levels are (m)=9. Threshold values and total participants number for each level are as follows: $(t_1, n_1) = (4, 6)$, $(t_2, n_2) = (2, 5)$, $(t_3, n_3) = (3, 5)$, $(t_4, n_4) = (4, 5)$, $(t_5, n_5) = (5, 6)$, $(t_6, n_6) = (3, 6)$, $(t_7, n_7) = (5, 7)$, $(t_8, n_8) = (4, 6)$, $(t_9, n_9) = (4, 7)$.

Now, to change the secret value from S to nS, dealer executes the algorithm given below.

6.5.2.1 Secret renewal:

The following steps are performed by dealer:

1. Select a $k \times 1$ new secret $nS \in \mathbb{Z}_{2^{m-1}} - \{0\}$;

$$\boldsymbol{nS} = \begin{pmatrix} \mathbf{125} \\ \mathbf{143} \\ \mathbf{132} \\ \mathbf{245} \\ \mathbf{250} \\ \mathbf{159} \end{pmatrix}$$

Since $m = 9$, $\mathbb{Z}_{2^{m-1}} - \{0\} = \{1, 2, 3, 4 \ldots 255\}$

2. Convert the secret nS_i into $m-1$ bit binary number and form new secret matrix $nSM, for 1 \leq i \leq k$;

$$\boldsymbol{nSM} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{pmatrix}$$

3. Calculate $nSM' = exor(nSM, TM)$

$$\boldsymbol{nSM'} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix}$$

4. Calculate public matrix

$nU = bagsum(nSM', XM);$

$$\boldsymbol{nU} = \begin{pmatrix} \mathbf{75} \\ \mathbf{887} \\ \mathbf{932} \\ \mathbf{325} \\ \mathbf{170} \\ \mathbf{302} \end{pmatrix}$$

Here, with the new values, we illustrate the secret reconstruction phase. There is no need to repeat compartment share reconstruction. It is rather, an assumption that all compartment participants are applied to Lagrange interpolation and their shares are obtained as we have illustrated in share reconstruction of section 6.4

6.5.2.2 Secret reconstruction of S_r

Let r be 3. In order to reconstruct third secret nS_3, the following steps are realized.

1. Any t_i or more than t_i participants of level i perform (t_i, n_i) Shamir's secret reconstruction and get the compartment share x_i. where, $i \in \{1, 2, \ldots, m-1\}$. The result is shown in Table 6.8

2. Check whether $nu_3 \geq x_1$ is at Level 1

   - If it is true, then bit 1 is the output of level 1 and it sends $nu'_{3,1,2} = nu_3 - x_1$ to the level 2
   - Otherwise, bit 0 is the output of level 1 and sends $nu'_{3,1,2} = nu_3$ to the level 2 and
   - Appends the output bit to an empty tuple (let say nSM''_3).

   The result of this step is shown in Table 6.9

3. For $i = 2 \rightarrow m-1$, Check whether $nu'_{3,i-1,i} \geq x_i$ is at Level i

   - If it is true, then bit 1 is the output of level i and it sends $nu'_{3,i,i+1} = u'_{3,i-1,i} - x_i$ to the next level $i+1$.
   - Otherwise, bit 0 is the output of level i and sends $nu'_{3,i,i+1} = nu'_{3,i-1,i}$ and to the next level $i+1$.

- Appends the output bit to the starting index of the tuple nSM_3''.

The result of this step is shown in Table 6.10

4. Level $m = 9$ performs (t_m, n_m) Shamir's secret reconstruction to reconstruct TM_3 in order to reconstruct nS_3 and the result is converted into $m-1$ bit tuple. Level m performs $exor(TM_3, nSM_3'')$ which results in SM_3.

$$\boldsymbol{TM_3 = (117)_{10} = (01110101)_2 \implies [0,1,1,1,0,1,0,1]}$$
$$\boldsymbol{nSM_3 = exor(TM_3, nSM_3'')}$$
$$\boldsymbol{\implies exor([0,1,1,1,0,1,0,1],[1,1,1,1,0,0,0,1]) = [1,0,0,0,0,1,0,0]}$$

5. Lastly, converting the obtained secret binary tuple nSM_3 to the decimal to obtain the secret nS_3.

$$\boldsymbol{nSM_3 = [1,0,0,0,0,1,0,0] \implies (10000100)_2 = nS_3 = 132.}$$

Consequently, using the same shares by the compartments, the new secret is reconstructed. Here, even though it is not required, as the compartments shares have been calculated in section 6.4.2, we in the section 6.5.2.2, repeated the steps 1 to 4, for the completeness.

Table 6.8: Compartment secrets

Level number	**Compartmental share (Using Lagrange interpolation)**
1	**836** mod 1669
2	**420** mod 1669
3	**206** mod 1669
4	**108** mod 1669
5	**51** mod 1669
6	**24** mod 1669
7	**11** mod 1669
8	**10** mod 1669

Table 6.9: Output bit from level 1

Level number	$\mathbf{nu_3}$	$\mathbf{x_1}$	$\mathbf{nu_3 \geq x_1}$	**Output bit**	$\mathbf{nu'_{3,1,2}}$	$\mathbf{nSM''_3}$
1	932	836	True	1	$932 - 836 = 96$	[1]

Table 6.10: Levels 2 to 8 Output bits

Level number	$\mathbf{nu'_{3,i-1,i}}$	$\mathbf{x_i}$	$\mathbf{nu'_{3,i-1,i} \geq x_i}$	**Output bit**	$\mathbf{nu'_{3,i,i+1}}$	$\mathbf{nSM''_3}$
2	96	420	False	0	96	[0,1]
3	96	206	False	0	96	[0,0,1]
4	96	108	False	0	96	[0,0,0,1]
5	96	51	True	1	$96 - 51 = 45$	[1,0,0,0,1]
6	45	24	True	1	$45 - 24 = 21$	[1,1,0,0,0,1]
7	21	11	True	1	$21 - 11 = 10$	[1,1,1,0,0,0,1]
8	10	10	True	1	$10 - 10 = 45$	[1,1,1,1,0,0,0,1]

6.6 Security analysis and observations

Security analysis and some observations of the proposed scheme are carried out in this section.

Brief security note :

- *Public parameters*: U, q, m;
- *Private to participant at compartment* i: Participant share of the compartment secret x_i.
- *Private to dealer*: S, SM, TM, SM', XM, polynomials (used to generate shares);

It is not possible for an intruder (neither inside nor outside participant $\mathcal{P}$) to get secret vector SM_i and secret s_i with public values U, q, because s_i, SM_i are private to dealer only and superincreasing vector XM is required to compute along with the public value U_i to get s_i, for $1 \leq i \leq k$.

All the levels have to participate in order to get the secret because XM and TM are available only after the reconstruction of compartment secrets from every compartment. Therefore, it is not possible to get the actual secret s by some of the compartments. Without higher level passing their value, the lower levels can not get the bit information because compartment with the lower level number has highest priority (where level m_j indicates lower level and m_1 indicates higher level.) Obtaining s from U, q, is infeasible assuming an honest dealer and with less than m levels. Hence, assuming the presence of a trustworthy dealer, our scheme is secure.

Observations - I

The proposed multi-secret sharing scheme deals with the $m-1$ bit secret, i.e., $1 \leq s \leq 2^{m-1}-1$. Hence, dealer chooses secret $s \in \mathbb{Z}_{2^{m-1}} - \{0\}$ in step 1 of share distribution phase. The range of chosen secret can be increased by assuming the secret is of $m'(> m-1)$ bits. The following two trivial methods can be used to solve this problem:

Method 1: As compartment share, the additional bits can be shared to a compartment (maybe after *exor* with TM) and once the reconstruction phase is done, prepends of these bits to the tuple ST'' takes place.

Method 2: As multiple compartment shares may be given to each level, multiple compartment secrets can be constructed at each level and hence multiple bits can be related to the secret.

Observations - II

The essential step of share distribution running time by a dealer for all the participants using interpolation technique is $\mathcal{O}(\sum_{i=1}^{m}(n_i t_i))$. During the secret reconstruction phase, when the compartments can get their shares at the same time, the running time is $\mathcal{O}((max(n_i))^2 + m)$. Here, to obtain the secret, $m-1$ comparisons and one *exor* is required.

6.7 Conclusions

In this chapter, a new multi-secret sharing scheme is proposed. The scheme is based on the subset sum problem and it uses superincreasing sequence to reconstruct the

secret for level order access structure. In our scheme, after the recovery of all the compartment secrets with honoring order among the levels, then only actual secret can be recovered. The secret changeability property is illustrated with an example. Also, the security analysis of the proposed scheme is discussed briefly assuming the presence of a trustworthy dealer. With the above stated ideas, the work can be extended with similar schemes considering other access structures and also can be extended to the multistage multi-secret sharing scheme. Furthermore, our scheme can be thought of without the dealer to arrive at more secure scheme.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

In this thesis, we focused on the design of techniques for sharing multiple secrets for different access structures, This is one of the important research areas in the domain of information security. We show that the problems in sharing single secret and need for the different access structures for various applications scenario. We proposed three multi secret sharing schemes that realize compartmented, hierarchical and level ordered access structures.

First, in Chapter 4, we proposed secret sharing scheme for hierarchical access structures. The proposed multi-secret sharing scheme uses Lagrange polynomial interpolation and one-way function. In this scheme, participants are classified into different levels based on the authority of the participants, and each level has a different threshold. The novelty of the proposed scheme is that, all participants will have a single share of multiple secrets, which reduces the overhead of the participants in order to keep multiple shares. Participants at each level can recover the secrets stage by stage only if the number of shares is equal to or more than the corresponding threshold value. Share of a higher level participant can be used to recover the secret at the lower level. The recovery of a secret at the earlier stage does not reveal or weaken the information of remaining secrets that have not been recovered. A unique feature of the proposed scheme is that shares are reusable. So shares need not be refreshed for future communication. The scheme is ideal and perfect. The security of the proposed scheme is the same as that of the Shamir's scheme and hardness of the one-way function, which is

unconditionally secure.

Next, in Chapter 5, we proposed a multi-secret sharing scheme that realizes compartmented access structures and uses the concept of the modular inverse. The set of participants in this access structure is divided into different compartments. The secret can be obtained if the threshold number of participants from each of the compartments reconstruct their compartment secret, and participate in recovering the actual secret. The proposed scheme uses Shamir's scheme first to retrieve partial secrets and combines them to form the actual secret. The scheme can also verify whether the actual secret is valid or not. Our proposed scheme is simple and easy to understand as we used only the modular inverse concept. Security analysis of the scheme is carried out and it is shown that the scheme resists both the insider as well as outsider attacks. The scheme is ideal and is computationally perfect, which relies on a hardness assumption. By computationally perfect, we mean that an authorized set can always reconstruct the secret in polynomial time, while this is computationally difficult for an unauthorized set.

Another scheme, in Chapter 6, we proposed for Level ordered Access structure (LOAS), This slightly differs from the two access structures presented in Chapter 4 and Chapter 5. To the best of our knowledge, no scheme is proposed in the literature till date, which shares multiple secret with honouring the order among the levels, The scheme is based on the subset sum problem, and it uses a superincreasing sequence to reconstruct the secrets. In this scheme, actual secret can be recovered only after the recovery of all the compartment secrets. And the recovery of the compartment secrets should honor the order among the levels. The novelty of the scheme is that not only a single share for all the secrets is sufficient but also the secrets can be changed without renewing the shares of the participants.

The secret changeability property is illustrated with an example. The proposed scheme has low communication cost and less overhead for the participant. Also, the security analysis of the proposed scheme is discussed briefly, assuming that the dealer is trustworthy. All the proposed schemes are analyzed for their security as well as discussed their computational complexity, and the results are compared with respective existing schemes.

7.2 Future Scope

There are many interesting directions in which the research work presented in this thesis can be carried out in the future. The schemes may be improved by using only one polynomial to design a scheme for multiple secrets , which will decrease the computational overhead. The verification phase can be added to the proposed schemes to verify the participants share; thereby improve the security of the scheme The schemes proposed in Chapter 5 and Chapter 6 can be extended to have multistage feature. Further, schemes can be thought of (i) without the presence of a dealer and (ii) having a change of threshold feature to provide complete protection for both the passive as well as the active adversary models.

References

[1] Noura Al Ebri, Joonsang Baek, and Chan Yeob Yeun. **Study on Secret Sharing Schemes (SSS) and their applications**. In *2011 International Conference for Internet Technology and Secured Transactions*, pages 40–45. IEEE, 2011. ()

[2] Fahad Alsolami and Terrance E Boult. **CloudStash: using secret-sharing scheme to secure data, not keys, in multi-clouds**. In *2014 11th International Conference on Information Technology: New Generations*, pages 315–320. IEEE, 2014. ()

[3] Charles Asmuth and John Bloom. **A modular approach to key safeguarding**. *IEEE transactions on information theory*, **29**(2):208–210, 1983. (2, 34, 39)

[4] Li Bai and XuKai Zou. **A proactive secret sharing scheme in matrix projection method**. *International Journal of Security and Networks*, **4**(4):201–209, 2009. ()

[5] Edoardo Ballico, Giulia Boato, Claudio Fontanari, and Fabrizio Granelli. **Hierarchical secret sharing in ad hoc networks through birkhoff interpolation**. In *Advances in Computer, Information, and Systems Sciences, and Engineering*, pages 157–164. Springer, 2007. ()

[6] Abdul Basit, N Chaitanya Kumar, V Ch Venkaiah, Salman Abdul Moiz, Appala Naidu Tentu, and Wilson Naik. **Multi-stage multi-secret sharing scheme for hierarchical access structure**. In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pages 557–563. IEEE, 2017. ()

[7] Amos Beimel, Tamir Tassa, and Enav Weinreb. **Characterizing ideal weighted threshold secret sharing**. *SIAM Journal on Discrete Mathematics*, **22**(1):360–397, 2008. ()

[8] Mihir Bellare and Phillip Rogaway. **Robust computational secret sharing and a unified account of classical secret-sharing goals**. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 172–184, 2007. (34)

[9] Josh Cohen Benaloh. **Secret sharing homomorphisms: Keeping shares of a secret secret**. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 251–260. Springer, 1986. (34)

[10] Albrecht Beutelspacher. **Geometric structures as threshold schemes**. *IMA Cryptography and Coding*, pages 255–268, 1986. (34)

[11] George Robert Blakley. **Safeguarding cryptographic keys**. *Proc. of the National Computer Conference1979*, **48**:313–317, 1979. (2, 21, 34)

[12] GR Blakley and GA Kabatianski. **Ideal perfect threshold schemes and MDS codes**. In *Proceedings of 1995 IEEE International Symposium on Information Theory*, page 488. IEEE, 1995. (34)

[13] Ernest F Brickell. **Some ideal secret sharing schemes**. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 468–475. Springer, 1989. (38)

[14] Christian Cachin. **On-line secret sharing**. In *IMA International Conference on Cryptography and Coding*, pages 190–198. Springer, 1995. (34)

[15] Marco Carpentieri, Alfredo De Santis, and Ugo Vaccaro. **Size of shares and probability of cheating in threshold schemes**. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 118–125. Springer, 1993. (33)

[16] Chao-Wen Chan and Chin-Chen Chang. **A scheme for threshold multi-secret sharing**. *Applied Mathematics and Computation*, **166**(1):1–14, 2005. (36)

[17] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang. **A new multi-stage secret sharing scheme using one-way function**. *ACM SIGOPS Operating Systems Review*, **39**(1):48–55, 2005. (36)

[18] Oinam Bidyapati Chanu, Appala Naidu Tentu, and V Ch Venkaiah. **Multi-Stage Multi-Secret Sharing Schemes Based on Chinese Remainder Theorem**. In *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015)*, page 17. ACM, 2015. ()

[19] Chris Charnes, Keith Martin, Josef Pieprzyk, and Rei Safavi-Nainil. **Secret sharing in hierarchical groups**. In *International Conference on Information and Communications Security*, pages 81–86. Springer, 1997. (34, 38)

[20] Sumanta Chatterjee and Shashidhar G Koolagudi. **Hierarchical secret sharing scheme using parts of speech of English grammar**. *International Journal of Security and Networks*, **12**(4):241–254, 2017. ()

[21] Hongtao Chen, Heng Zhao, Liaojun Pang, Jimin Liang, and Jie Tian. **Multi fuzzy vault based on secret sharing for deadlock restoration**. *International Journal of Information Technology and Management*, **11**(1-2):50–60, 2012. ()

[22] Hung-Yu Chien, JAN Jinn-Ke, and Yuh-Min Tseng. **A practical (t, n) multi-secret sharing scheme**. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, **83**(12):2762–2765, 2000. (35)

[23] Wu Chunying, Li Shundonga, and Zhang Yiying. **Key management scheme based on secret sharing for wireless sensor network**. In *2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*, pages 574–578. IEEE, 2013. ()

[24] Ed Dawson and Diane Donovan. **The breadth of Shamir's secret-sharing scheme**. *Computers & Security*, **13**(1):69–78, 1994. (34, 35)

[25] Massoud Hadian Dehkordi and Samaneh Mashhadi. **An efficient threshold verifiable multi-secret sharing**. *Computer Standards & Interfaces*, **30**(3):187–190, 2008. (35)

[26] Barun Duari and Debasis Giri. **An ideal and perfect (t, n) Multi-secret sharing scheme based on finite geometry**. In *Information Technology and Applied Mathematics*, pages 85–94. Springer, 2019. ()

[27] Anjaneyulu Endurthi, Oinam B Chanu, Appala Naidu Tentu, and V Ch Venkaiah. **Reusable multi-stage multi-secret sharing schemes based on CRT**. *Journal of Communications Software and Systems (JCOMSS)*, **11**(1):15–24, 2015. (36, 53)

[28] Ziba Eslami and Saideh Kabiri Rad. **A new verifiable multi-secret sharing scheme based on bilinear maps**. *Wireless Personal Communications*, **63**(2):459–467, 2012. (35)

[29] Oriol Farràs, Jaume Martí-Farré, and Carles Padró. **Ideal multipartite secret sharing schemes**. *Journal of cryptology*, **25**(3):434–463, 2012. (4)

[30] Oriol Farras and Carles Padró. **Ideal hierarchical secret sharing schemes**. *IEEE transactions on information theory*, **58**(5):3273–3286, 2012. (36)

[31] Oriol Farras, Carles Padró, Chaoping Xing, and An Yang. **Natural generalizations of threshold secret sharing**. *IEEE transactions on information theory*, **60**(3):1652–1664, 2014. (3, 38, 66)

[32] P Mohamed Fathimal and P Rani. **Threshold Secret Sharing Scheme for Compartmented Access Structures**. *International Journal of Information Security and Privacy*, **10**(3):1–9, 2016. ()

[33] Matthew Franklin and Moti Yung. **Communication complexity of secure computation**. In *Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 699–710, 1992. (35)

[34] Hossein Ghodosi, Josef Pieprzyk, and Rei Safavi-Naini. **Secret sharing in multilevel and compartmented groups**. In *Australasian Conference on Information Security and Privacy*, pages 367–378. Springer, 1998. (29, 34, 36, 37, 38, 39, 53)

[35] L Harn. **Comment on" Multistage secret sharing based on one-way function"**. *Electronics Letters*, **31**(4):262, 1995. (36)

[36] Lein Harn and Miao Fuyou. **Multilevel threshold secret sharing based on the Chinese Remainder Theorem**. *Information processing letters*, **114**(9):504–509, 2014. (39, 45, 53)

[37] Putla Harsha, Patibandla Chanakya, and China Venkaiah Vadlamudi. **A Reusable Multipartite Secret Sharing Scheme Based on Superincreasing Sequence.** *IJ Network Security*, **20**(3):527–535, 2018. (4, 40)

[38] Jingmin He and Edward Dawson. **Multistage secret sharing based on one-way function**. *Electronics Letters*, **30**(19):1591–1592, 1994. (24, 35, 36)

[39] Jingrui He and Ed Dawson. **Multisecret-sharing scheme based on one-way function**. *Electronics Letters*, **31**(2):93–95, 1995. (35, 36)

[40] Javier Herranz and Germán Sáez. **New results on multipartite access structures**. *IEE Proceedings-Information Security*, **153**(4):153–162, 2006. (4, 34, 36, 37)

[41] Ching-Fang Hsu and Lein Harn. **Multipartite secret sharing based on CRT**. *Wireless personal communications*, **78**(1):271–282, 2014. (4)

[42] Ren-Junn Hwang and Chin-Chen Chang. **An on-line secret sharing scheme for multi-secrets**. *Computer Communications*, **21**(13):1170–1176, 1998. (36)

[43] Sorin 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. (38)

[44] Mitsuru Ito, Akira Saito, and Takao Nishizeki. **Secret sharing scheme realizing general access structure**. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, **72**(9):56–64, 1989. (3, 66)

[45] Wen-Ai Jackson, Keith M Martin, and Christine M O'keefe. **Ideal secret sharing schemes with multiple secrets**. *Journal of Cryptology*, **9**(4):233–250, 1996. (35)

[46] Ehud Karnin, Jonathan Greene, and Martin Hellman. **On secret sharing systems**. *IEEE Transactions on Information Theory*, **29**(1):35–41, 1983. (34, 35)

[47] Emilia Käsper, Ventzislav Nikov, and Svetla Nikova. **Strongly multiplicative hierarchical threshold secret sharing**. In *International Conference on Information Theoretic Security*, pages 148–168. Springer, 2007. ()

[48] Suresh C Kothari. **Generalized linear threshold scheme**. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 231–241. Springer, 1984. (34, 38)

[49] Kaoru Kurosawa, Satoshi Obana, and Wakaha Ogata. **t-Cheater identifiable (k, n) threshold secret sharing schemes**. In *Annual International Cryptology Conference*, pages 410–423. Springer, 1995. (33)

[50] Changlu Lin, L Harn, and Dingfeng Yea. **Ideal Hierarchical (t, n) Secret Sharing Schemes**. In *Proceedings of the Fifth International Conference on Information Assurance and Security (IAS 09), Xian, China*. Citeseer, 2009. (36, 39, 53)

[51] James L Massey. **Minimal codewords and secret sharing**. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279. Citeseer, 1993. (2, 34)

[52] Robert J. McEliece and Dilip V. Sarwate. **On sharing secrets and Reed-Solomon codes**. *Communications of the ACM*, **24**(9):583–584, 1981. (2, 34)

[53] Ralph Merkle and Martin Hellman. **Hiding information and signatures in trapdoor knapsacks**. *IEEE transactions on Information Theory*, **24**(5):525–530, 1978. (17)

[54] Maurice Mignotte. **How to share a secret**. In *Workshop on Cryptography*, pages 371–375. Springer, 1982. (2, 34)

[55] S-L Ng. **Ideal secret sharing schemes with multipartite access structures**. *IEE Proceedings-Communications*, **153**(2):165–168, 2006. (36)

[56] Mehrdad Nojoumian and Douglas R Stinson. **Sequential Secret Sharing as a New Hierarchical Access Structure.** *J. Internet Serv. Inf. Secur.*, **5**(2):24–32, 2015. (39)

[57] Hakan Ozadam, Ferruh Ozbudak, and Zülfükar Saygi. **Secret sharing schemes and linear codes**. In *Information Security Cryptology Conference with International Participation, Proceedings*, pages 101–106, 2007. (34)

[58] Dileep Kumar Pattipati, Appala Naidu Tentu, V Ch Venkaiah, and Allam Appa Rao. **Sequential Secret Sharing Scheme Based on Level Ordered Access Structure.** *IJ Network Security*, **18**(5):874–881, 2016. (4, 30, 31, 39, 66)

[59] Josef Pieprzyk and Xian-Mo Zhang. **Ideal threshold schemes from MDS codes**. In *International Conference on Information Security and Cryptology*, pages 253–263. Springer, 2002. (34)

[60] Josef Pieprzyk and Xian-Mo Zhang. **Ideal secret sharing schemes from permutations**. *International Journal of Network Security*, **2**(3):238–244, 2006. (34)

[61] Ali Aydin Selçuk and Ramazan Yilmaz. **Joint compartmented threshold access structures**. *iacr*, 2012. (38)

[62] Adi Shamir. **How to share a secret**. *Communications of the ACM*, **22**(11):612–613, 1979. (2, 21, 22, 34, 35, 54)

[63] Jun Shao and Zhenfu Cao. **A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme**. *Applied Mathematics and Computation*, **168**(1):135–140, 2005. (35)

[64] Gustavus J Simmons. **How to (really) share a secret**. In *Conference on the Theory and Application of Cryptography*, pages 390–448. Springer, 1988. (4, 28, 37, 38)

[65] Gustavus J Simmons. **Prepositioned shared secret and/or shared control schemes**. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 436–467. Springer, 1989. (38)

[66] Gustavus J Simmons. **An Introduction to Shared Secret and/or Shared Control Schemes and Their Application**. *Wiley-IEEE Press*, 1992. ()

[67] Nidhi Singh, Appala Naidu Tentu, Abdul Basit, and V Ch Venkaiah. **Sequential secret sharing scheme based on Chinese remainder theorem**. In *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, pages 1–6. IEEE, 2016. (39, 45, 53)

[68] Douglas R. Stinson. **An explication of secret sharing schemes**. *Designs, Codes and Cryptography*, **2**(4):357–390, 1992. (36)

[69] Tamir Tassa. **Hierarchical threshold secret sharing**. *Journal of Cryptology*, **20**(2):237–264, 2007. (3, 36, 39, 66)

[70] Tamir Tassa and Nira Dyn. **Multipartite secret sharing by bivariate interpolation**. In *International Colloquium on Automata, Languages, and Programming*, pages 288–299. Springer, 2006. (4, 39)

[71] Tamir Tassa and Nira Dyn. **Multipartite secret sharing by bivariate interpolation**. *Journal of Cryptology*, **22**(2):227–258, 2009. (38, 39)

[72] Appala Naidu Tentu, Abdul Basit, K Bhavani, and V Ch Venkaiah. **Multi-secret sharing scheme for level-ordered access structures**. In *International Conference on Number-Theoretic Methods in Cryptology*, pages 267–278. Springer, 2017. (4)

[73] Appala Naidu Tentu, K Bhavani, Abdul Basit, and V Ch Venkaiah. **Sequential (t, n) multi secret sharing scheme for level-ordered access structure**. *International Journal of Information Technology*, pages 1–11, 2018. ()

[74] Appala Naidu Tentu, Banita Mahapatra, V Ch Venkaiah, and V Kamakshi Prasad. **New secret sharing scheme for multipartite access structures with threshold changeability**. In *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 1910–1916. IEEE, 2015. (4, 39)

[75] Appala Naidu Tentu, Prabal Paul, and 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. ()

[76] Appala Naidu Tentu, Prabal Paul, and V Ch Venkaiah. **Computationally perfect secret sharing scheme based on error-correcting codes**. In *International Conference on Security in Computer Networks and Distributed Systems*, pages 251–262. Springer, 2014. (39)

[77] Appala Naidu Tentu, V Kamakshi Prasad, and V Ch Venkaiah. **Multi-Stage Secret Sharing Schemes Based on Asmuths Bloom Sequence**. *Networking and Communication Engineering*, **8**:75–79, 2016. (39)

[78] Appala Naidu Tentu, V Ch Venkaiah, and V Kamakshi Prasad. **CRT based multi-secret sharing schemes: revisited**. *International Journal of Security and Networks*, **13**(1):1–9, 2018. ()

[79] Martin Tompa and Heather Woll. **How to share a secret with cheaters**. *journal of Cryptology*, **1**(3):133–138, 1989. (36)

[80] V Vinod, Arvind Narayanan, K Srinathan, C Pandu Rangan, and Kwangjo Kim. **On the power of computational secret sharing**. In *International Conference on Cryptology in India*, pages 162–176. Springer, 2003. (34)

[81] Kai Wang, Xukai Zou, and Yan Sui. **A multiple secret sharing scheme based on matrix projection**. In *2009 33rd Annual IEEE International Computer Software and Applications Conference*, **1**, pages 400–405. IEEE, 2009. ()

[82] Xianfang Wang, Can Xiang, and Fang-Wei Fu. **Secret sharing schemes for compartmented access structures**. *Cryptography and Communications*, **9**(5):625–635, 2017. ()

[83] Yongge Wang and Yvo Desmedt. **Efficient secret sharing schemes achieving optimal information rate**. In *2014 IEEE Information Theory Workshop (ITW 2014)*, pages 516–520. IEEE, 2014. ()

[84] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang. **A (t, n) multi-secret sharing scheme**. *Applied Mathematics and Computation*, **151**(2):483–490, 2004. (35, 36)

[85] Geng Yong-Jun, Fan Xiao-Hong, and Hong Fan. **A new multi-secret sharing scheme with multi-policy**. In *The 9th International Conference on Advanced Communication Technology*, 2007. ()

[86] Tong Zhang, Xizheng Ke, and Yanxiao Liu. **(t, n) multi-secret sharing scheme extended from Harn-Hsus scheme**. *EURASIP Journal on Wireless Communications and Networking*, **2018**(1):71, 2018. ()

[87] Jianjie Zhao, Jianzhong Zhang, and Rong Zhao. **A practical verifiable multi-secret sharing scheme**. *Computer Standards & Interfaces*, **29**(1):138–141, 2007. (35)

List of Publication and Presentation

1. **New Multi-secret Sharing Scheme based on Superincreasing Sequence for Level-Ordered Access Structure.** *In International Journal of Communication Networks and Distributed Systems (IJCNDS) pp. 357-380, 24.4 (2020):* (Scopus, ESCI, DBLP Indexed)

2. **Multi Secret Sharing Scheme using modular inverse for Compartmented Access Structure.** *In International Conference on Data Engineering and Communication Technology (ICDECT) pp. 371-385, AISC, Springer, 2019.* (Scopus Indexed)

3. **Multi Stage Multi Secret Sharing Scheme for Hierarchical Access Structure**. *In International Conference on Computing, Communication and Automation (ICCCA), pp. 557-563. IEEE, 2017.* (Scopus Indexed)

4. **Sequential Secret Shraing Scheme based on Chinese Remainder Theorem.** *In IEEE International Conference on Computational Intelligence and Computing Research 2016, at Agni college of Technology Chennai.*(Scopus Indexed)

5. **Sequential Multi-secret Sharing Scheme for Multilevel Access Structure.** *In National Workshop on Cryptology (NWC)- 2017, at Department of Computer Science and Engineering, NIT Tiruchirappalli.*

6. **Multi-secret Sharing Scheme & Various Access Structures.** *In National Instructional Workshop on Cryptology (NIWC)- 2018, at Department of Mathematics, MNIT Allahabad.*

7. **Multi-secret Sharing Scheme based on Superincreasing Sequence.** *In National Workshop on Cryptology (NWC)- 2018, at CR RAO Advanced Institute of Mathematics, Statistics and Computer Science, Hyderabad.*

New Multi-secret Sharing Scheme based on Superincreasing Sequence for Level-ordered Access Structure

Abdul Basit*, Patibandla Chanakya, V. Ch. Venkaiah, Salman Abdul Moiz

School of Computer and Information Sciences
University of Hyderabad, Hyderabad-500046, India
E-mail: abdulmcajh@gmail.com
*Corresponding author

Abstract: A new multi-secret sharing scheme (MSSS) that uses a superincreasing sequence and realizes Level-Ordered Access Structure (LOAS) is proposed. The novelty of the scheme is that not only a single share for all the secrets is sufficient but also the secrets can be changed without renewing the shares of the participants. The proposed scheme has low communication cost and less overhead for the participant.

Keywords: Level-Ordered Access Structure, Multi-secret, Multi-stage, super increasing sequence, Secret Sharing

Reference to this paper should be made as follows: Abdul Basit, Patibandla Chanakya, V. Ch. Venkaiah, and Salman Abdul Moiz (2018) 'New Multi-secret Sharing Scheme based on Superincreasing Sequence for Level-Ordered Access Structure', *International Journal of Communication Networks and Distributed Systems*, Vol. x, No. x, pp.xxxx–xxx.

Biographical notes: Abdul Basit received Master of computer application from Jamia Hamdard University, New Delhi. He did Bachelor of Science in Information Technology from SMU Gangtok. Currently, he is pursuing his PhD in Computer Science from the University of Hyderabad. His research interests include Information security, Cryptography, Cyber security, and Algorithms.

Patibandla Chanakya received M.Tech from University of Hyderabad. Currently he is pursuing his PhD in Computer Science from IIIT Allahabad. His research interests include Computational number theory, Algorithms, and Cryptography.

V.Ch. Venkaiah is currently serving in School of Computer and Information Sciences University of Hyderabad. He obtained his PhD in 1988 from the Indian Institute of Science (IISc), Bangalore in the area of Scientific Computing. He worked for several organisations including the Central Research Laboratory of Bharat Electronics, Tata Elxsi India Pvt. Ltd., Motorola India Electronics Limited, all in Bangalore. He then moved onto academics and served IIT, Delhi, IIIT, Hyderabad, and CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science. He is a vivid researcher. During his tenure at IIIT, Hyderabad, he had set up the Center for Security and Algorithmic Research (C-STAR),

Multi-secret Sharing Scheme Using Modular Inverse for Compartmented Access Structure

Abdul Basit, V. Ch. Venkaiah and Salman Abdul Moiz

Abstract Secret sharing scheme is a cryptographic primitive or a method for increasing the security of crucial information or data. It is used to share a secret among a set of participants, such that specific sets of participants can uniquely reconstruct the secret by pooling their shares. In this paper, we have proposed a new multi-secret sharing scheme for compartment access structure. In this access structure, the set of participants is partitioned into different compartments. The secret can be obtained only if the threshold number of participants from each of the compartments reconstruct their compartment secret, and participate in recovering the actual secret. The proposed scheme uses Shamir's scheme first to retrieve partial secrets and combines them to form the requested secret. The scheme can also verify whether the retrieved secret is valid or not. Security analysis of the scheme is carried out and showed that the scheme resists both the insider as well as outsider attacks. Our proposed scheme is simple and easy to understand as we have used only the modular inverse concept.

Keywords Secret sharing · Multi-secret · Compartmented access structure · Modular inverse

1 Introduction

Information security has grown much more since electronic communication is used in our daily life. The cryptographic secret key, which is used for securing the information, is shared among a set of players by a dealer in the distribution process. The sharing is done in such a way that by pooling specific sets of shares, the secret can be reconstructed. Initially, secret sharing schemes are proposed to solve

A. Basit (✉) · V. Ch. Venkaiah · S. A. Moiz
School of Computer & Information Sciences, University of Hyderabad,
500046 Hyderabad, India
e-mail: abdulmcajh@gmail.com

K. S. Raju et al. (eds.), *Data Engineering and Communication Technology*,
Advances in Intelligent Systems and Computing 1079,
https://doi.org/10.1007/978-981-15-1097-7_31

Multi-stage Multi-secret Sharing Scheme for Hierarchical Access Structure

Abdul Basit[†]✉, N Chaitanya Kumar[†], V. Ch. Venkaiah[†], Salman Abdul Moiz[†], Appala Naidu Tentu[‡], Wilson Naik[†]

[†]*School of Computer & Information Sciences, University of Hyderabad, Hyderabad-500046, India*
[‡]*CR Rao AIMSCS, University of Hyderabad, Hyderabad-500046, India*
Email: abdulmcajh@gmail.com✉

***Abstract*—Hierarchical threshold secret sharing (HTSS) schemes can be thought as a generalization of classical threshold secret sharing schemes, and they have been extensively in the literature. In an HTSS, participants are classified into different security levels, and the threshold value of a higher level is smaller than that of a lower level. Participants in each level can recover the secrets, if the number of shares is equal to or more than the corresponding threshold value. Share of a higher level participant can be used to reconstruct the secret at lower level. In this paper, we proposed first hierarchical threshold multi-secret sharing scheme based on polynomial interpolation. Proposed scheme is a variation to HTSS schemes based on the CRT suggested by Singh et al. and Harn et al. Novelty of the proposed scheme is that each participant requires to keep only one secret share and multiple secrets can be shared separately without refreshing the secret share. Also, secrets are recovered in stage by stage. Our scheme which is unconditionally secure, is based on Lagrange interpolation polynomial and one-way function.**

keywords: Hierarchical, Multi-secret, Multi-stage, Polynomial, Secret Sharing,

1. Introduction

A secret sharing scheme (SSS) is a method in which a secret is divided into shares. These shares are distributed among the set of participants by a dealer in such way that any authorized set of participants can recover the secret by combining their shares, whereas any unauthorised set of participants cannot get any knowledge about the secret. The first SS schemes were introduced by Shamir [1] and Blakley [2] in 1979 independently. Shamir's scheme is based on the Lagrange interpolation polynomial while Blakley's scheme is realised using linear projective geometry. Their schemes are known as (t, n) threshold SSS, where t is the threshold and n is the number of participants. A (t, n) threshold SSS allows any t or more than t participants to recover the secret, while it does not allow any less than t participants to recover the secret.

In Shamir's (t, n) threshold secret sharing scheme, a trusted dealer generates n secret shares based on a $(t-1)^{th}$ degree polynomial. Secret reconstruction is based on lagrange polynomial interpolation of any t or more than t set of private shares. A SSS is ideal if the maximal length of the shares is same as that of the secret. If the set of shares corresponding to an unauthorized set provide no any information and the set of shares corresponding to an authorized set gives all the information of the secret, in the information- theoretic sense, then the scheme is perfect.

The family of all authorized sets, who can recover the secret, is known as an access structure. Γ is the symbol generally used to denote access structure of a SSS. The set of all unauthorized sets, which can not gain any knowledge about the secret, is called adversary structure or forbidden set and it is denoted by $\overline{\Gamma}$. Several access structures are proposed in the literature. Example include generalized access structure, (t, n) threshold access structure and multipartite access structure.

In a (t, n) threshold access structure any set of t or more participants out of n is an authorized set and any set of less than t participants is an unauthorized set. That is

$$\Gamma = \{X \in 2^q : |X| \geq t\}$$
$$\overline{\Gamma} = \{X \in 2^q : |X| < t\}$$

where 2^q denotes the power set of the set of participants.

An access structure is called monotone, if it satisfies the following:

$$(X \in \Gamma)\Lambda(X \subseteq Y) \Rightarrow Y \in \Gamma$$
$$(X \in \overline{\Gamma})\Lambda(Y \subseteq X) \Rightarrow Y \in \overline{\Gamma}$$

If Γ and $\overline{\Gamma}$ are such

$$\Gamma = \{X \in 2^q : |X| = t\} \text{ and}$$
$$\overline{\Gamma} = \{X \in 2^q : |X| = t-1\}$$

then we say that Γ only contains the minimal authorised sets which can get the secret, $\overline{\Gamma}$ only holds maximal unauthorised sets which can not get the secret.

Let $\mathcal{P}$ denote the set of all n participants. Let these participants be divided into $m \geq 2$ disjoint levels $L_1, L_2, \cdots, L_m$ so that each level L_i has n_i participants with a threshold value t_i, where $n = \sum_{i=1}^{m} n_i$. All participants in level L_i play

ISBN: 978-1-5090-6471-7/17/ $31.00 ©2017 IEEE

IEEE PODHIGAI

2016 IEEE INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND COMPUTING RESEARCH

Venue : Agni College of Technology

Chennai - 600 130, Tamil Nadu, India

BEST PAPER AWARD CERTIFICATE

2016 DEC 15-17

This is to certify that the paper entitled Sequential Secret Sharing Scheme Based on Chinese Remainder Theorem

with authors Nidhi Singh, Appala Naidu Tentu, Abdul Basit, V. ch. Venkaiah

presented by Abdul Basit

is the **BEST PAPER** of the Track No. 5, on 2016 December ~~15~~/16 ~~AN~~ / FN Session.

IEEE-SIPCICOM

Session Chair

Dr. M.KARTHIKEYAN
2016 IEEE ICCIC - Organizing Secretary
Secretary - IEEE Podhigai

Dr. KRISHNAN NALLAPERUMAL
2016 IEEE ICCIC - General Chair
Chair IEEE Podhigai / SIPCICOM

IEEE

International Conference on Computing Communication and Automation (ICCCA2017) 05th-06th MAY, 2017

GALGOTIAS UNIVERSITY

(IEEE Conference Record No #41372)

School of Computing Science and Engineering, Galgotias University
Uttar Pradesh, India

Certificate Of Participation

This is to certify that Prof. /Dr. / Mr./ Ms. Abdul Basit

of University of Hyderabad, Hyderabad has presented a paper titled

Multi-stage Multi-secret Sharing Scheme for Hierarchical Access Structure

in IEEE International Conference on Computing Communication and Automation (Technically Co -Sponsored by IEEE UP Section) organized by School of Computing Science and Engineering, Galgotias University during 05th – 06th MAY, 2017.

Prof. Parma Nand
General Chair

Prof. Abhishek Swaroop
TPC

NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

and

CRYPTOLOGY RESEARCH SOCIETY OF INDIA

17th National Workshop on

Cryptology

Organized by

Department of Computer Science and Engineering

This is to certify that Dr/Mr/Ms. Abdul Basit, University of Hyderabad has participated and presented a paper on *"Sequential Multi-secret Sharing Scheme for Multilevel Access Structure"* in the National Workshop on Cryptology (NWC-2017) held at Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli from 28th to 30th August, 2017.

Convener
NWC-2017

Director
NIT-T

National Instructional Workshop on Cryptology
(NIWC - 2018)

June 6-10, 2018

Organized by

Department of Mathematics

Motilal Nehru National Institute of Technology Allahabad

&

Cryptology Research Society of India

Certificate

This is to certify that Abdul Basit of University Of Hyderabad delivered a lightning talk on Multi Secret Sharing Schemes & Various Access Structures in the **National Instructional workshop on Cryptology** held at Department of Mathematics, Motilal Nehru National Institute of Technology Allahabad during **June 6-10, 2018**.

Prof. Shiv Datt Kumar	**Dr. Pitam Singh**	**Dr. Sahadeo Padhye**
Chairman	Co-ordinator	Convener

NATIONAL WORKSHOP ON CRYPTOLOGY
(5-7, September 2018)

CERTIFICATE OF PAPER/POSTER PRESENTATION

This is to certify that Mr/Mrs/Ms /Dr Abdul Basit

of University Of Hyderabad *has successfully presented paper/~~poster~~*

titled Multi-Secret Sharing Scheme based on Superincreasing Sequence *in the three day* ***'National Workshop on Cryptology (NWC-2018)'*** *organized by CR Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS) in association with Cryptology Research Society of India (CRSI), from 5th to 7th September 2018 at CR Rao AIMSCS, University of Hyderabad Campus, Hyderabad.*

Dr. Appala Naidu Tentu
Convenor
NWC-2018

Prof. D. N. Reddy
Chairman
NWC-2018

Springer

NBA ALL UG COURSES

NAAC A' GRADE STANLEY

COMPUTER SOCIETY OF INDIA ESTD. 1965

3rd INTERNATIONAL CONFERENCE ON DATA ENGINEERING AND COMMUNICATION TECHNOLOGY (ICDECT- 2019)

On 14th, 15th & 16th March 2019

at

STANLEY COLLEGE OF ENGINEERING & TECHNOLOGY FOR WOMEN

(Affiliated to Osmania University)

Abids , Hyderabad - 500 001

Certificate of Presentation

This is to certify that Dr./Mr./Ms. Abdul Basit *has*

presented a paper entitled " **Multi Secret Sharing Scheme using modular inverse for Compartmented Access Structure** *" in the*

3rd International Conference on Data Engineering and Communication Technology (ICDECT- 2019) held during 14th, 15th & 16th March 2019.

Dr. A. Vinaya Babu
Conference Chair
ICDECT - 2019

Dr. Satya Prasad Lanka
Principal
SCETW

Design and Analysis of Multi Secret Sharing Schemes for Various Access Structures

by Abdul Basit

Design and Analysis of Multi Secret Sharing Schemes for Various Access Structures

ORIGINALITY REPORT

54%	23%	51%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES Overall Similarity Index: 54 - (18+15+9+2+2) = 8%

Professor
School of CIS
Prof. C.R. Rao Road,
Central University
Hyderabad-46. (India)

1	Abdul Basit, Patibandla Chanakya, V. Ch. Venkaiah, Salman Abdul Moiz. "New multi-secret sharing scheme based on superincreasing sequence for level-ordered access structure", International Journal of Communication Networks and Distributed Systems, 2020 This publication is by the Student Publication	18%
2	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 This publication is by the Student Publication	15%
3	link.springer.com Internet Source	9%
4	Abdul Basit, V. Ch. Venkaiah, Salman Abdul Moiz. "Chapter 31 Multi-secret Sharing	2%

This publication is by the Student

Similarity Screening Done @ IGM Library
15 63 46 0 33
19/4/2021
Librarian / DLIC

Professor
School of CIS
Prof. C.R. Rao Road,
Central University
Hyderabad-46. (India)

Scheme Using Modular Inverse for Compartmented Access Structure", Springer Science and Business Media LLC, 2020
Publication

5	www.coursehero.com Internet Source	2%
6	Submitted to University of Hyderabad, Hyderabad Student Paper	2%
7	Submitted to Jawaharlal Nehru Technological University Student Paper	1%
8	ijns.jalaxy.com.tw Internet Source	1%
9	arxiv.org Internet Source	<1%
10	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%
11	"Number-Theoretic Methods in Cryptology", Springer Science and Business Media LLC, 2018 Publication	<1%
12	www.inderscience.com Internet Source	<1%

This publication is by the Student's Professor

Professor
School of CIS
Prof. C.R. Rao Road,
Central University
Hyderabad-46. (India)

Schemes", IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 08/01/2008
Publication

49	Submitted to Indian Institute of Technology Guwahati Student Paper	<1 %
50	Submitted to University of Alabama Student Paper	<1 %
51	www.hindawi.com Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 14 words
Exclude bibliography	On		