Dynamic Multi-Secret Sharing Scheme With Cheater Detection

A Thesis submitted in the partial fulfillment for the award of

Degree of Master of Technology

in

Software Engineering

by

Sunil Dalal

(2K15/SWE/19)

Under the Guidance of

Dr. Kapil Sharma

DEPARTMENT OF COMPUTER ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

Bawana Road, Delhi

CERTIFICATE

DEPARTMENT OF COMPUTER ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

Bawana Road, Delhi

It is certified that the work contained in this thesis entitled **"Dynamic Multi-secret Sharing Scheme with Cheater Detection"** by "Sunil Dalal" is an authentic work which has been carried out under my supervision. The content embodied in this thesis has not been submitted elsewhere for the award of any degree to the best of my knowledge and belief.

Dr. Kapil Sharma

Head of Department

Department of Information Technology

Delhi Technological University

Declaration

I hereby want to declare that the thesis entitled **"Dynamic Multi-secret Sharing Scheme with Cheater Detection"** which is being submitted to the Delhi Technological University, in the partial fulfillment of the requirements for the award of degree in Master of Technology in Software Engineering is an authentic work carried out by me. The material contained in the thesis has not been submitted to any institution or university for the award of any degree.

Sunil Dalal

2K15/SWE/19

Software Engineering

Department of Computer Engineering

Delhi Technological University

Bawana Road, Delhi

Acknowledgement

I take this opportunity to thank my supervisor, **Dr. Kapil Sharma**, for guiding me and providing me with all the facilities, which paved way to the successful completion of this work. This thesis work was enabled and sustained by his vision and ideas.

I would like to thank the faculty and staff of the Department of Computer Science and Engineering, DTU Delhi, for providing the necessary infrastructure and testing facilities and environment which allowed us to work without any obstructions.

I would also like to thanks to the Almighty God with his blessings I had an opportunity and strength to do this wonderful project and studies, as well as to my parents who always support me and guide me in the right direct direction with their incredible experiences of life..

Sunil Dalal
2K15/SWE/19

Abstract

Secret sharing scheme are used are primarily used in cryptosystem for distributing shares of a secret among a set of entities in such a way that the secret can be reconstructed only with certain combination of shares. These schemes are mainly used in applications where there is no single trusted entity. In this thesis we propose a Dynamic Multi-Secret Sharing Scheme with cheater detection mechanism. The proposed scheme has advantage of Lin –Yen's scheme in which each participant has only one secret share for reconstructed multiple secrets. In addition, proposed scheme does not require any secure channel between any participant and the dealer during secret share distribution phase. Analysis shows that the proposed scheme is as secure as the scheme which uses secure channel for distribution of share.

List of figures

List of Table

Contents

Chapter 1

Introduction

1.1 Overview of Need of Cryptography

Data communication is one of the essential and most often used communication methods in present days. Computer network [20] plays an important role in data communication. Private correspondence is one of the necessities of the social life. In this specific situation, a few inquiries that need consideration are:-

i. *How can one transmit the message secretly, so that no unauthorised person gets knowledge of the message?*
ii. *How can the sender ensure himself that the message arrives at the receiver exactly as it was transmitted?*
iii. *How can the receiver ensure himself that the message is coming exactly as it was transmitted and from the identified user?*

Customarily, there are two approaches to take care of such issues. One can camouflage the very presence of message, by compositions with undetectable ink or attempt to transmit the message by reliable secure channel. An alternate logical way to deal with take care of such issues is cryptography. Cryptography comprises of two words Crypt intends to disguise and Graphy intends to think about. So cryptography is the investigation of covering up and opening of the information thought to be delicate. The essentialness of cryptography can be considered from the accompanying illustration:

At the point when Julius Caesar sent messages to his commanders, he didn't put stock in his emissaries. So he supplanted each in his messages with a D, each B with an E, et cetera through the letter set. Just somebody who knew the "move by 3"rule could disentangle his messages.

It can be further illustrated by Figure 1.1, where Aman want to send secret information about bank account to Mohan but if he send it directly to Mohan then any one can know about secret information and misuse it. Therefore Aman encrypts this secret information about bank account

M utilizing an encryption work E and a key k, bringing about a figure content $C = E_{k(M)}$. Mohan utilizes a similar key for decoding the figure message keeping in mind the end goal to recuperate Aman's unique data utilizing decryption D_k and gets $M = D_{k(C)}$. An unapproved individual, called Chandu, can't recoup the first data from the figure content without knowing the secret key k. He is permitted, be that as it may, to have full learning of the encryption and unscrambling plans E and D.

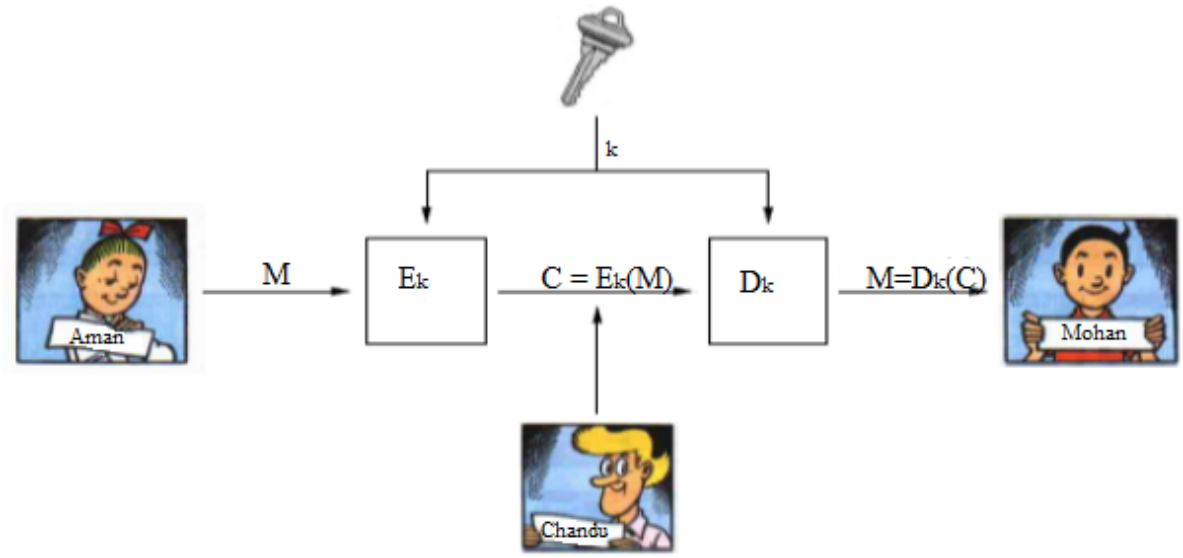

Figure 1.1 General Model for Cryptography.

The above illustration demonstrates that a cryptosystem ought to be secure, regardless of the possibility that an enemy knows everything about the framework, aside from the key.

1.1.1 Fields of Cryptography

Different properties in the field of cryptography require by Aman and Mohan for solid correspondence can be compressed as take after**.** [1]

Confidentiality

Confidentiality implies that lone sender and approved beneficiary ought to have the capacity to get to the message substance. For instance if Aman might want to guarantee that nobody with the exception of Mohan gets his subtle elements of cash, account number and so forth and if someone else gets the transmitted signal, he does not come to know about the details of the transaction.

Authentication [17]

Authentication is assurance of the communication between the authorized persons. Prior to the procedure of exchange Aman and Mohan must be guarantee that they are talking just to each other, and no other individual is disguise in the middle of them.

Data Integrity

Assume that Aman needs to offer his 40% of offers, however an interloper in the middle of changes to 45%, this implies the respectability of the sent message is lost. Information trustworthiness is the system which is utilized for remediation of above issue.

Non-Repudiation

Non-revocation gives security against the refusal of the message sent. For instance, if Aman needed to contribute rupee 10,000 and he confronts misfortune in the market, at that point he may deny that he had not contributed such sum through Mohan. At that point non-denial is the procedure which can help Mohan that message was surely sent by Aman to him.

1.2 Motivation of Secret Sharing

In any kind of network [22] whether wired or wireless, communication reliability and security are two important issues, especially when networks are used in national security and safety critical applications. The secure and reliable way to send information on network is to encrypt the information with the help of encryption algorithm and a secret key. So in this case we have to mainly protect the cryptographic key in order to protect the encrypted data from disclosure as encryption algorithm is publically known due to limited in number and follow a definite pattern to encrypt data, so cryptanalysist can easily know about encryption algorithm. The secure scheme keeps the key safe by putting it in single location but such a scheme is unreliable in case of a single misfortune occurs. To keep multiple copies of a key is also unsecure from theft point of view. Here we need more robust secure way to protect the key and this can be done by sharing of the secret key/ Password using various schemes.

Secret sharing depends on a framework with the end goal that the individuals in the gathering can reproduce the secret, while people not in amass can't recover any piece of data about the

secret. In, 1979 Adi Shamir [2] created edge technique for secret sharing, which is considered to be perfect method. G. Blakely [3] developed method of secret sharing based on isoplane. Many other methods have been developed since the Adi Shamir methods, but most of methods use threshold method secret sharing [4]. In (k, n) limit technique for secret sharing, k is the quantities of any members whose offers are required for secret recreation and n is the quantity of members among whom the secret is shared.

There are situations, where a military troop has many missiles but all do not have the same launch code. To launch missiles in war by sharing the launch codes one can use single secret sharing method n-times. Alternatively Multiple-Secrets sharing method can be used. In, 2006 Li Bai [6] developed multiple-secret sharing scheme based on matrix projection. Li Bai method of multiple-secret sharing is also threshold method of secret sharing.

But if military troop have to change the launch code at regular intervals to keep it safe without changing the secret shares values or new codes have to be assigned to new missiles without changing the secret share values then in such cases dynamic multi-secret secret plan can be utilized. In, 2008 Lin and Yeh [4] developed dynamic multi-secret sharing scheme based on one way hash function. These secret sharing schemes will be discussed in detail in chapter 4 and 5.

In the digital world of transmission any kind of data is treated as packets. It doesn't matter that it is a text data, an image data or video data. All formats are treated in same manner for the case of transmission. So secret sharing scheme is suitable method. Many times this scheme is also not enough for giving the reliability such as we need to keep up a secret on-line. We can store the secret on server. Be that as it may, in the event that we do as such, the secret would be revealed if the server is bargained. In the event that the server is undermined, at that point the secret might be ruined or lost So a (n, k) threshold scheme is developed by Shamir that is ok with the intruders but this scheme is only useful for one secret at a time so for multiple secret Li-Bai developed a multiple secret sharing scheme which generate secret shares for number of secret simultaneously but this scheme is also one time use scheme. Therefore Lin-Yeh developed a dynamic multi secret sharing scheme that can be used, when we have to change the secret without need to change secret shares. Therefore this scheme is more capable to stop intruders. The cheaters are those who are shareholder in scheme or the dealer itself who is distributing wrong secret shares to users. In such cases, There should be a method for detect the cheater from good shareholders and also a method so that dealer not able to know about secret shares. Lin-

Yeh scheme does not provide such kind of solution. We can apply here a verification process to detect the cheater and also the problem regarding dealer. Dynamic multi- secret sharing schemes includes secret shares selection by users themselves using modular arithmetic and verification can be done by calculating W matrix and publish it publically. Now the verification and cheater detection process take place. We can implement it with some programming in any language like C, C++, MATLAB etc. and we can use any operating system which support of those languages for implementation of this scheme.

1.3 Thesis Organisation

This thesis is organize as follows. In chapter 2, different cryptographic systems are described with discussions about Symmetric stream cipher and asymmetric stream cipher used in mobile communication. Chapter 3 describes details of basic requirement for evaluating a polynomial and modular arithmetic operations. Hash function and working of hash function used in our scheme are also presented in the chapter. In chapter 4, there is a detailed explanation about various secret sharing schemes for sharing data showing development in this field. Chapter 5 has details about proposed scheme, its working and its implementation by taking an example. The thesis is concluded in chapter 6, with scope for future work.

1.4 Programming Tool Used

Programming device utilized here to run our plan is MATLAB which remains for MATRIX LABORATORY. It is a product bundle created by Math Works, (written in c, java) Inc. to encourage numerical calculations, network control, plotting charts, making GUI apparatuses and so forth. MATLAB is particularly intended for framework calculations: illuminating frameworks of straight conditions, figuring Eigen esteems and Eigen vectors, considering networks, et cetera. Moreover, it has an assortment of graphical capacities, and can be stretched out through projects written in its own particular programming dialect. MATLAB program and script records dependably have filenames finishing with ".m". The programming dialect is straight forward as practically every information protest is thought to be an exhibit. Graphical yield is accessible to supplement numerical outcomes. MATLAB was presented in 1984; and is a specialized figuring

and application advancement condition utilized today by more than 500,000 architects and researchers.

Add on libraries tool stash permit the fundamental MATLAB library to supplement with .m records critical to particular application zones. It is simple for the MATLAB client to produce new m records for client subordinate applications. MATLAB code is exceptionally brief, making it conceivable to express complex flag preparing (reenactment) calculations utilizing a not very many lines of code.

Chapter-2

Classification of Cryptographic Systems

2.1 Introduction

Cryptography is scientific procedure to encode and decipher data. Cryptography engages you to store delicate information or transmit it transversely over unverifiable frameworks (like the Internet) [23] so it can't be examined by anyone except for the normal recipient. Data that can be scrutinized and fathomed with no extraordinary measures is called as plaintext or clear substance. The strategy for covering plaintext in order to cover the data is called encryption. Encoding plaintext achieves confused "foolishness" called as Figure 2.1 content. Encryption ensures that information is dodged anyone for whom it is not proposed, but anyone can read the mixed data. The route toward returning figure substance to its novel plaintext is called unscrambling.

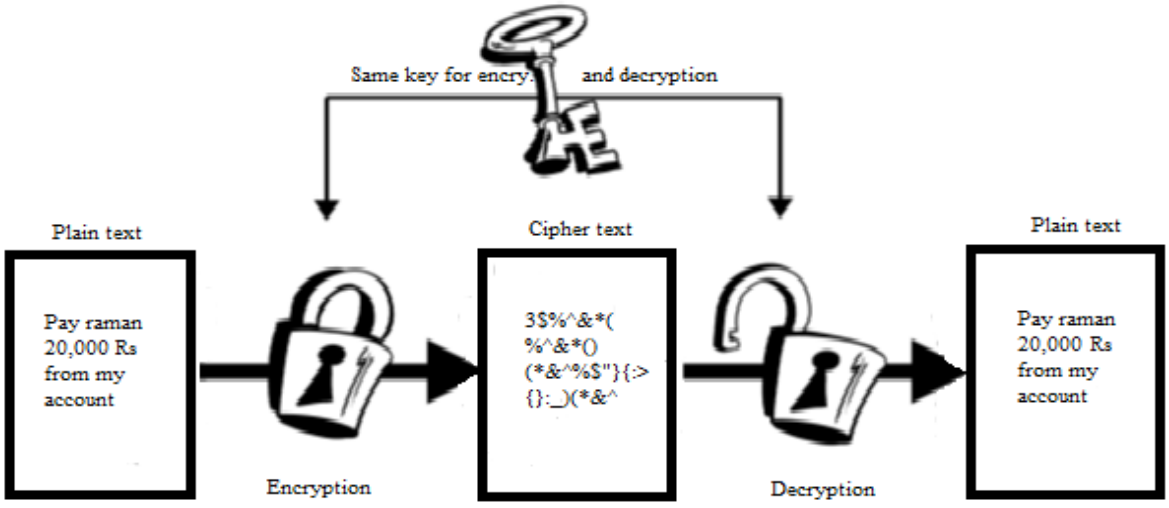

Figure 2.1 Encryption and Decryption Process in Cryptography

A cryptographic computation is a logical limit which is used for the encryption and unscrambling process. A cryptographic estimation works in blend with a keyword, number, or expression to encode the plaintext. The same plaintext encodes to different figure content with different keys. The security [18] of encoded data is absolutely dependent on two things specifically the nature of the cryptographic estimation and the secret of the key.

Cryptographic estimation, close by all possible keys and each one of the traditions that make it work include a cryptosystem. Cryptography system based upon key use is of two types, Symmetric and Asymmetric. In symmetric system same key is used for encryption and decryption, whereas in case of Asymmetric system keys used for encryption and decryption are different. Based upon mode of encryption and decryption cryptographic system can be classified as Stream cipher and Block cipher. In stream cipher plaintext is encrypted bit by bit or byte by byte, whereas in case of block cipher encryption is done over a chunk of bits.

There may be various possible scenario of the attack on the data. Cryptanalyst may have knowledge of algorithm and some pairs of cipher and plain text may also be available with him. Possible attacks are differentiated on the basis of cipher and plain text pairs known as cipher text attack and known plain text attack respectively. In this chapter section 2.2 presents symmetric and asymmetric cipher system. Stream and block cipher is being presented in the section 2.3. Section 2.4 presents the types of attacks in cryptographic system.

2.2 Cryptography Based on Symmetric and Asymmetric Cipher System

2.2.1 Symmetric Cipher System

Symmetric system is also known as conventional encryption. In conventional encryption, also called as single secret-key encryption, one key is utilized both for encryption and decoding. The Data Encryption Standard (DES) is a case of a customary cryptosystem that is broadly utilized by the USA and other Government. Figure 2.2 is a delineation of the traditional encryption prepare. The fundamental elements of symmetric frameworks are as per the following.

Plaintext: This is the first message or information that sender needs to send and is encouraged into the encryption calculation box as info.

Secret key: Secret key is another commitment to the encryption estimation. The key is free of the plaintext and of the encryption computation. The estimation will make another yield (figure content) dependent upon the specific key being used at the time i.e. two keys will convey two unmistakable figure messages the right substitution and changes performed by the estimation depends on upon the key.

Encryption calculation: Encryption calculation performs different substitution and change on the plaintext alongside the secret key i.e. showing in the figure 2.2. Some of symmetric systems are DES, AES, Blowfish, and RC5 etc.

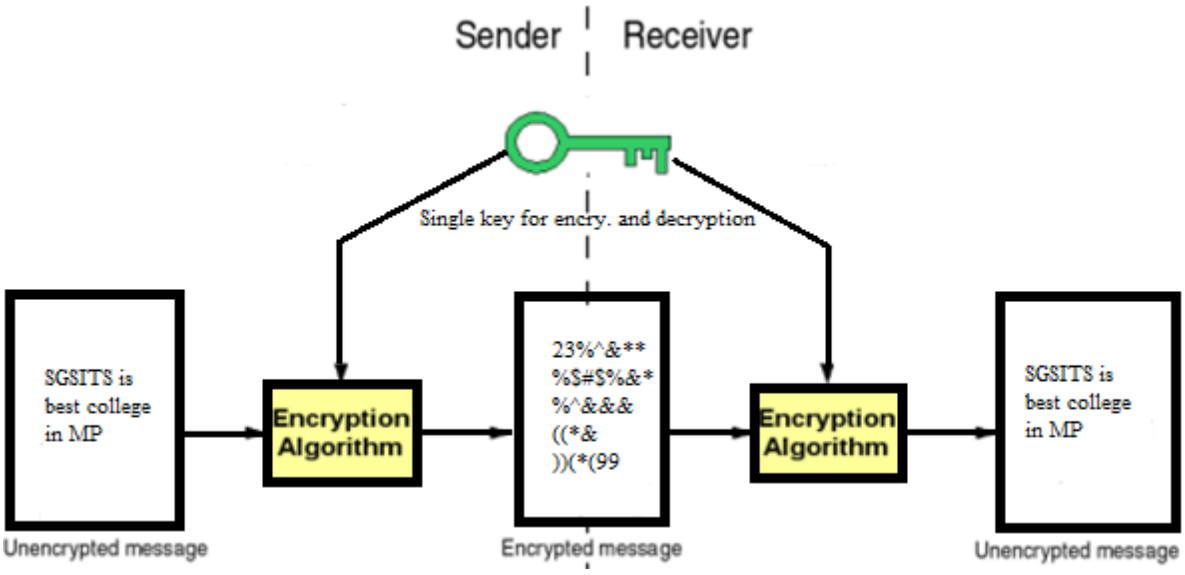

Figure 2.2 Conventional Encryption System

Cipher text: This is the blended message made as yield of encryption figuring. It depends on upon the plaintext and the riddle key. The figure content is a clearly sporadic stream of data and, the way things are, is unfathomable.

Decryption algorithm: This is basically the encryption calculation keep running backward. It takes the figure content and the secret key and delivers the first plaintext.

Cryptanalysis: The study of recuperating data from figures without information of the key.

The major requirements for strong symmetric system are strong encryption algorithm and secret key must be shared to the sender and receiver by a secure channel. Encryption algorithm should be complicated in such a manner that even if any opponent knows the algorithm and has one or more copies of cipher texts or cipher text plaintext pairs he/she must not able to decrypt the plaintext and the key.

2.2.2 Asymmetric cipher system

An asymmetric cipher system, also known as open key cryptography, has isolate encryption key and unscrambling key. Open key cryptography utilizes two or three keys for encryption to be particular an open key, which scrambles data, and a relating private, or riddle key for unscrambling. That is the reason the framework is called awry. Dissimilar to symmetric key calculations, it doesn't require a safe beginning trade of at least one secret keys to both sender and collector. Anyone with a copy of your open key can then encode information that nobody however you can read. Any individual who has an open key can encode data however can't decode it. Just the individual who has the relating private key can decode the data. Indeed, even individuals you have never met can send you data subtly. Utilization of open and private keys permits security of the legitimacy of a message by making an advanced mark of a message utilizing the private key, which can be checked utilizing the general population key. It permits assurance of the privacy and furthermore the honesty of a message.

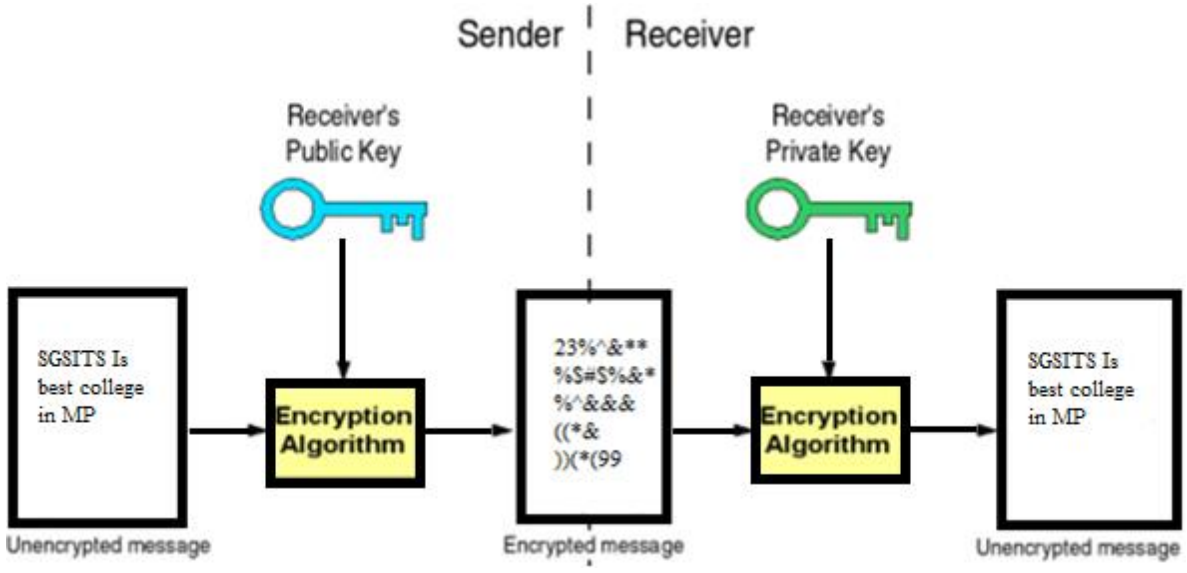

Figure 2.3 Public Key Encryption System

Asymmetric cipher systems have a tendency to be fundamentally more computationally escalated. Along these lines, they are generally utilized as a part of mix with symmetric figures to actualize compelling open key cryptography. This gives the key-trade advantages of awry

figure 2.3 with the speed of symmetric figures. Deffie–Hellman key [7] of exchange algorithm is used in such cases.

The two primary branches of open key cryptography are:

1) **Public key encryption:** A message mixed with a recipient's open key can't be unscrambled by anyone beside a holder of the planning private key. Clearly, this will be the proprietor of that key and the individual related with general society key used. Figure 2.4 explains the simple working of general public key system, this type of structure is used for confidentiality.

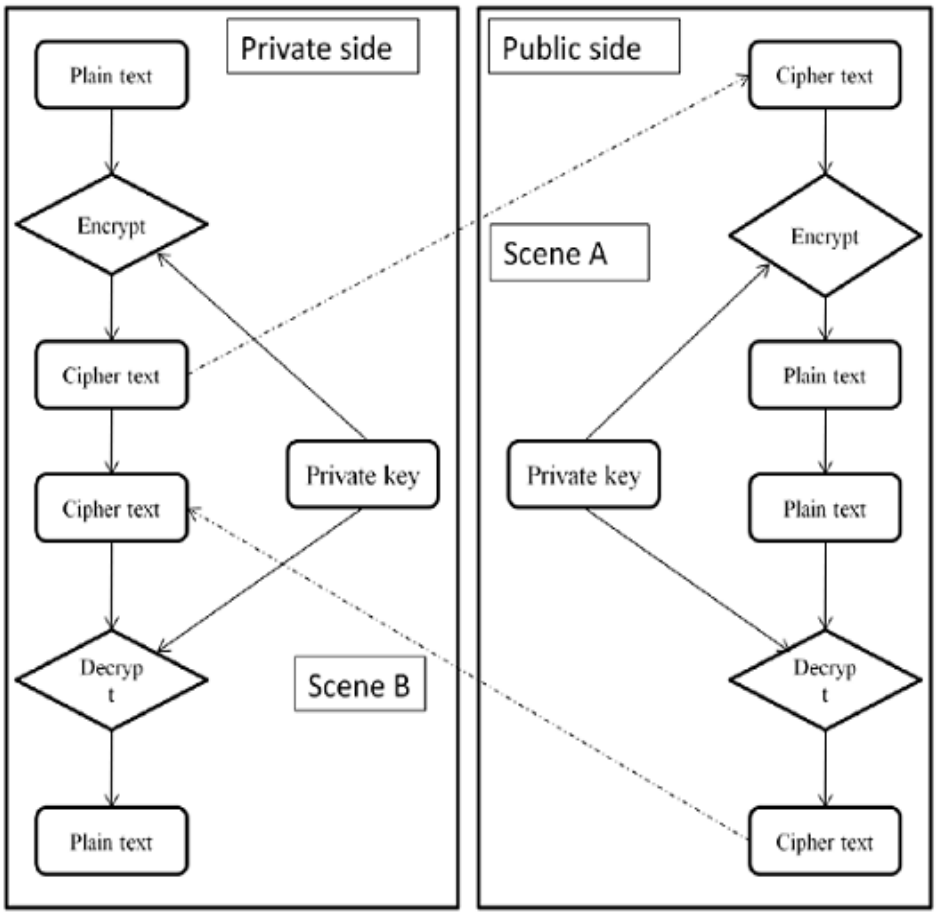

Figure 2.4 General Public Key System for Confidentiality

2) **Digital signatures [13] :** A message set apart with a sender's private key can be affirmed by any person who approaches the sender's open key, in this way showing

the sender has send it since only sender had access to the private key. It also gives assurance that the part of the message that has not been tampered with.

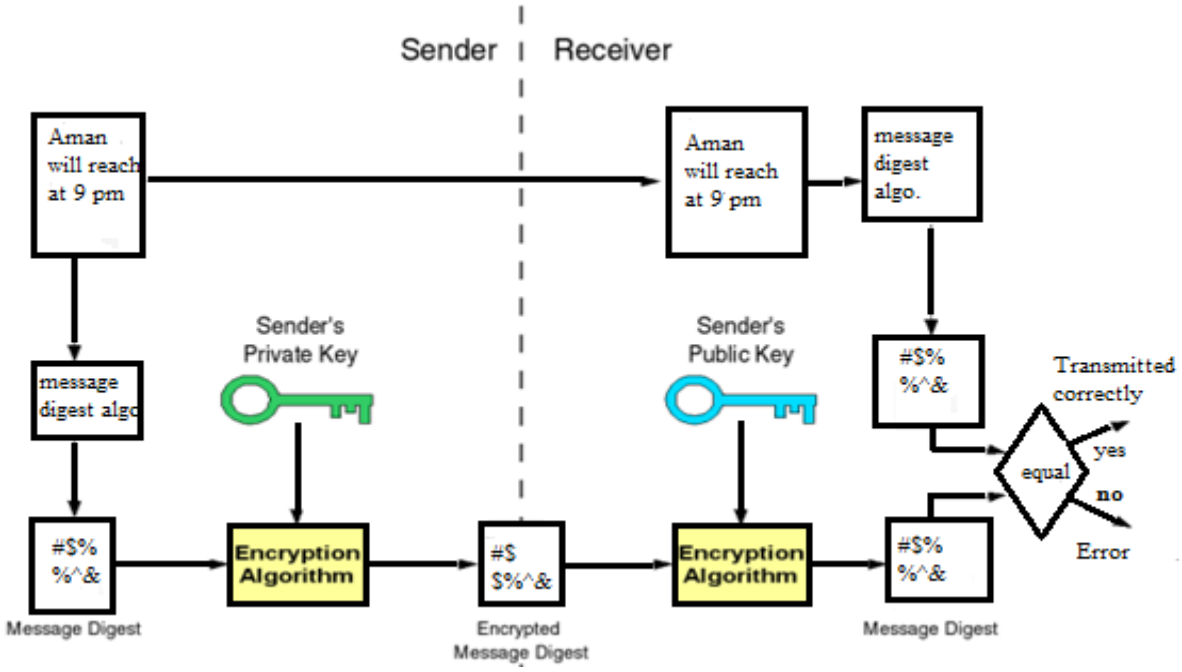

Figure 2.5 Simple Digital Signatures Process

In Figure 2.5 we can understand the method or working of asymmetric key system with a given simple example. A similarity to open key encryption is that of a bolted letter box with a mail space. The mail opening is presented and available to the general population; its area (the road address) is basically the general population key. Anybody knowing the road deliver can go to the entryway and drop a composed message through the opening. Notwithstanding, just the individual who has the key can open the letter box and read the message. Another similarity for computerized marks is the fixing of an envelope with an individual wax seal. The message can be opened by anybody, however the nearness of the seal verifies the sender. A focal issue for utilization of open key cryptography is certainty (in a perfect world confirmation) that an open key is right, has a place with the individual or element asserted (i.e., is 'bona fide'), and has not been messed with or supplanted by a malignant outsider. The standard way to deal with this issue is to utilize an open key foundation (PKI), in which at least one outsiders, known as endorsement specialists, and guarantee responsibility for sets.

Chapter 3

Polynomial and Hash Function Used in Cryptography

3.1 Groups, Rings, and Fields

Groups**,** rings and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra. Cryptographic systems use polynomials based arithmetic over a field. Before starting the polynomial evaluation we will have to study about these terms are describe in the following figure.

3.1.1 Groups

A group G, sometimes denoted by {G, ·} is a set of elements with a binary operation, (denoted by ·) that associates to each ordered pair (a, b) of elements in G an element (a.b) in G, such that the following axioms are obeyed.

(A1) Closure: If a and b belong to G, then a.b is also in G.

(A2) Associative: a· (b·c) = (a·b) ·c for all a, b, c in G.

(A3) Identity element: There is an element e in G such that a·e = e·a = a for all a in G.

(A4) Inverse element: For each a in G there is an element a′ in G such that a· a′ = a′·a = e.

(A5) Commutative: a·b = b·a for all a,b in G.

Cyclic Group

A group G is cyclic if every element of G is a power a^k (k is an integer) of a fixed element a € G. The element a is said to generate the group G, or to be a generator of G. A cyclic group is always abelian and may be finite or infinite. Thus, Cyclic group is defined as exponentiation with in a group as repeated application of the group operator, so that a^3 = a·a·a. Further we define a^0=e, the identity element; and $a^{-n} = (a')^n$.

3.1.2 Rings

A ring R, sometimes denoted by {R, +, ×}, is a set of elements with two binary operations, called addition and multiplication, such that for all a,b,c in R the following axioms are obeyed:

(A1-A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as −a.

(M1) closure under multiplication: If a and b belong to R, then ab is also in R.

(M2) Associativity of multiplication: a(bc) = (ab)c for all a,b,c in R.

(M3) Distributive laws: a (b+c) = ab + ac for all a, b, c in R

(a+b) c = ac + bc for all a, b ,c in R.

(M4) Commutatively of multiplication: ab =ba for all a,b in R.

(M5) Multiplicative identity: There is an element 1 in R such that a.1=1.a=a for all a in R.

(M6) No zero divisors: If a, b in R and ab=0, then either a=0 or b=0.

3.1.3 Fields

A field F, sometimes denoted by {F,+, ×}, is a set of elements with two binary operations, called addition and multiplication, such that for all a,b,c in F the following axioms are obeyed:

(A1-A5), (M1-M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $a\ a^{-1} = (a^{-1})\ a = 1$.

3.2 Modular Arithmetic

In cryptography, randomness in the cipher text is more desirable to prevent attacks. The modular arithmetic increases the level of randomness at the time of computation and randomness increase the complexity and at the same time decreases the possibility of prediction of plain text. Thus it increases overall level of security [19] which is desirable thing one can understand modular arithmetic with small examples. Given any positive whole number n and nonnegative whole number and, on the off chance that we isolate a by n, we get a number remainder q and a number leftover portion r that comply with the accompanying relationship: $a= qn+r$ where $0 \leq r < n$; $q= \lfloor a/n \rfloor$ that is represent in the figure 3.1 where $\lfloor x \rfloor$ is the biggest number not exactly or equivalent to x (i.e. floor of x).

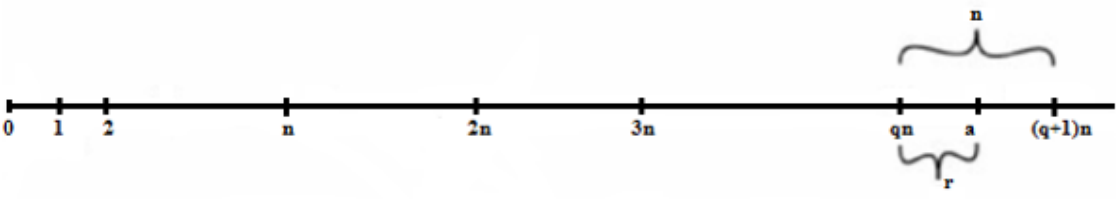

Figure 3.1 The Relationship a = qn + r, 0≤ r < n

The following examples with numeric values will illustrate the procedure

(1) a= 11, and n=7; 11=1×7+4; Therefore r = 4, q = 1

(2) a=-11, and n=7; -11=(-2) ×7+3; Therefore r = 3, q = -2

The integer n is called the modulus. Thus for any integer a, we can always write

a= $\lfloor a/n \rfloor$ × n + (a mod n). Therefore,

11 mod 7 = 4; -11mod7 = 3

3.3 Finite Fields of the Form GF (p) [5]

In segment 3.1 we examined about field as a set that complies with the greater part of the maxims and represent it with a few cases. We likewise examined about unbounded fields, however limitless fields are not quite compelling with regards to cryptography. In any case, limited fields assume an essential part in numerous cryptographic calculations. A limited field is a field with a limited field arrange (i.e., number of components) and is likewise called as Galois field. The request of such a limited field is dependably a prime or an energy of a prime. For each prime power, there exists precisely one (with the standard proviso that "precisely one" signifies "precisely one up to an isomorphism") limited field GF (p_n) where n is a positive whole number, regularly composed as GF (p_n). Here GF remains for Galois field, to pay tribute to the mathematician who initially examined limited fields. Two uncommon instances of GF are of enthusiasm for cryptography. For n=1, we have the limited field GF (p). This limited field has an alternate structure than that for limited fields with n>1. In cryptography one uses limited fields of the frame GF (2n).

3.4 Polynomial Arithmetic

It is well known that all the cryptographic algorithm works on the principal of polynomial arithmetic, and in our case of secret sharing schemes, polynomial arithmetic is also used and even evaluated the polynomial according the finite fields. Here we will discuss about polynomial evaluation over finite fields.

3.4.1 Polynomial Evaluation [9]

We begin by depicting some essential properties of polynomials. Give us a chance to consider a ring R and indicate the arrangement of all polynomials over R by R[x]. Let f(x) = (f_0+f_{1x}+… … +$f_{k)}$ x_k be a polynomial in R[x]. We likewise settle a vector a = [a_0…..a_n] € Rn with the goal that all esteems a_i are distinctive and nonzero. At that point we characterize the polynomial assessment mapping eval: R[x] → Rn as takes after. We assess the polynomial f(x) on the vector and present the outcome as a vector.

eval (f):= [f (a_0)… … .. f (a_n)] ^{T}.

In the accompanying operations between vectors in Rn is characterized component astute. That is, if u and v € Rn and ⊕ is a parallel administrator, at that point:

u ⊕v:= [(u_1⊕ v_1)… (u_n⊕ v_n)]^T

For any two polynomials f and g in R[x] and a scalar esteem r € R the accompanying conditions hold:

i. Additively: eval (f + g) = eval (f) + eval (g).
ii. Multiplicatively: eval (f · g) = eval (f) · eval (g).
iii. Multiplicatively with respect to scalar values: eval (r · f) = r · eval (f)

The mapping eval is a direct change.

The conditions hold due to the duality with the individual polynomial operations:

i. Additively: (f + g)(a) = f(a) + g(a)
ii. Multiplicatively: (f · g)(a) = f(a) · g(a)

iii. Multiplicatively with respect to scalar values: $(r \cdot f)(a) = r \cdot f(a)$

The conclusion i.e. equation no. 3.1 that the mapping is a straight change specifically takes after from the above conditions. Consequently it has been demonstrated that eval is a direct mapping between the assessment places of the polynomial and the resultant vector. In encourage talk we consider a polynomial f being identical to the vector of its coefficients. We will now give a further investigation of the properties of this mapping. Let $\vec{f}$ = $[f_0 \ldots f_k]$ be the variety of coefficients of the polynomial f. We can now compute the vector

$\vec{y}$ = eval (f) = $[f_0 \ldots f_k]^T$

$\vec{y} = \sum_{i=0}^{k} f_i \ eval\ (x_i) = \sum_{i=0}^{k} f_i\ [a_0^i, \ldots\ldots\ldots, a_n^i]^T$

$$= f_0 \begin{bmatrix} 1 \\ 1 \\ . \\ . \\ 1 \end{bmatrix} + f_1 \begin{bmatrix} a_0 \\ a_1 \\ . \\ . \\ a_n \end{bmatrix} + \ldots\ldots\ldots + f_k \begin{bmatrix} a_0^k \\ a_1^k \\ . \\ . \\ a_n^k \end{bmatrix} \qquad \textbf{(3.1)}$$

3.5. Basis of Matrix

3.5.1. Introduction

Matrix is arrangement of numbers in a rectangular form in rows and columns. It is denoted by single capital letter and enclosed by [ ]. For example

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ & & . & & & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ & & . & & & \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix}$$

In a matrix $m \times n$ elements are arranged in such a way that m is rows and n is columns. The matrix is given as $m \times n$ order. To refer an element in matrix number is denoted by name of element followed by two suffixes, which denote number of the row and number of column respectively. For example, a_{ij} represent an element which is i^{th} in row and i^{th} column in the matrix. A matrix is a single entity.

3.5.2. Types of Matrix

Row matrix*:* The matrix has single row as

$A = \begin{bmatrix} 1 & 3 & 6 & 9 \end{bmatrix}$

Column matrix*:* The matrix has single column as $A = \begin{bmatrix} 3 \\ 4 \\ 6 \\ 8 \end{bmatrix}$

Square matrix*:* A matrix is a square matrix which has equal number of rows and columns equal i.e. (i = j) as $A = \begin{bmatrix} 2 & 4 & 9 \\ 3 & 5 & 1 \\ 8 & 2 & 7 \end{bmatrix}$

Diagonal matrix*:* It is a square matrix in which all elements except elements in diagonal are zero as $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 23 & 0 \\ 0 & 0 & 5 \end{bmatrix}$

Unit matrix*:* A diagonal matrix is one in which all diagonal elements are unity. It is also called as identity matrix of order n, where n is the order of matrix as $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Null matrix*:* A matrix is a null matrix if all elements are zero as $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

3.5.3. Operation of Matrix

Addition of matrices: Two matrices A and B can add, if both are of same order. Addition is defined as addition of elements at respective position.

For ex. Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$.

Then $A+B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix}$.

Subtraction of matrices: Two matrices A and B can be subtracted, if both are same order. Subtraction is defined as subtraction of elements at respective position. For ex

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$.

Then $A-B = \begin{bmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & a_{22} - b_{22} \end{bmatrix}$

Multiplication of matrix by a scalar*:* Multiplication of matrix by a scalar k is defined as multiplication of k to each element of matrix.

For e.g. Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and k be the scalar, then the multiplication is defined as

$kA = \begin{bmatrix} ka_{11} & ka_{12} \\ ka_{21} & ka_{22} \end{bmatrix}$.

Multiplication of matrices: Two matrices can be multiply if number of columns in first matrix is equal to number of rows in second matrix. For ex.

Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{bmatrix}$

Then AB = $\begin{bmatrix} a_{11}\ b_{11} + a_{12}\ b_{21} + a_{13}\ b_{31} & a_{21}\ b_{11} + a_{22}\ b_{21} + a_{23}\ b_{31} \\ a_{21}\ b_{12} + a_{21}\ b_{22} + a_{23}\ b_{32} & a_{21}\ b_{12} + a_{22}\ b_{22} + a_{23}\ b_{32} \end{bmatrix}$

The order of multiplication is important because it is not necessary that AB = BA. It is also not necessary that both multiplication exist.

Minor: Minor of element of square matrix is calculated by eliminating the row and column in which element is present. For example

Let A = $\begin{bmatrix} 1 & 3 \\ 5 & 9 \end{bmatrix}$

Then minor of 1 = 9, 3 = 5, 5 = 3, and 9 = 1.

Cofactor of matrix: If minor of element is multiplied by -1^{i+j}, where i, j are the value of row-number and column-number of element in matrix. For ex. let A = $\begin{bmatrix} 1 & 3 \\ 5 & 9 \end{bmatrix}$, then cofactor of element, 1 =$(-1)^{1+1}$* 9 = 9, 3 =$(-1)^{1+2}$ * 5 = -5, 5 =$(-1)^{2+1}$ * 3 = -3, 9 =$(-1)^{2+2}$ *1= 1.

Transpose of matrix: Transpose of matrix is defined as a matrix in which rows of matrix and column of matrix are interchanged. It is denoted byA^T, where A is the matrix. As, let

A = $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$. Then

$A^T = \begin{bmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{bmatrix}$.

Ad joint of Matrix: If cofactors of a square matrix are arranged in matrix then the transpose of that matrix is called ad joint of that matrix. It is denoted as Adj (A), where A is matrix. For example

Let A = $\begin{bmatrix} 1 & 3 \\ 5 & 9 \end{bmatrix}$ and matrix of cofactor is $\begin{bmatrix} 9 & -5 \\ -5 & 1 \end{bmatrix}$. Then Adj (A) = $\begin{bmatrix} 9 & -5 \\ -5 & 1 \end{bmatrix}$

Invertible matrix: A square matrix A is an invertible matrix if the determinant of matrix is non-zero . It is also called non-singular matrix.

Inverse of matrix*:* Let A be matrix then Inverse of matrix A is defined as matrix B such that AB = Z_n. For the existence of inverse of a matrix it is necessary that determinant of matrix should be non-zero. The inverse of A denoted as A^{-1} and defined as $A^{-1}= \frac{Adj(A)}{\Delta}$ **.** Where Δ is determinant of the matrix.

Rank of matrix: If A is a square matrix then rank is defined as the maximum order of sub matrix for which determinant is non-zero.

Chapter 4

Various Secret Sharing Schemes

4.1 Introduction

The meaning of sharing the secret is splitting the secret data or information in small pieces and regenerates the unique information by utilizing a few or the majority of the little pieces. In cryptography [15] , a secret sharing plan is a strategy in which a secret is to isolated in covering parts and afterward get the entire secret from specific offers (or shadows) which are dispersed to clients. The secret might be recouped just by certain foreordained gatherings which have a place with the get to structure. Numerous secret sharing plans had been produced for this. Sharing schemes based on one way function, polynomial based, matrix based and Chinese remainder theorem based etc. [10]. Some of these schemes are perfect sharing schemes and some are less effective.

Secret sharing plans were first presented by Blakely [3] and Adi Shamir [2] as an answer for protecting cryptographic keys. Secret sharing plans can likewise be utilized for any circumstance in which the entrance to a critical asset must be limited.

In this section we right off the bat show review of single secret sharing plans and various secret sharing plans and after that Dynamic multi-secret sharing plans are clarified.

4.2 Single Secret Sharing Schemes

In single secret sharing arrangement, one riddle is shared among the picked assembling of people. Such an arrangement relies on upon ability to such a degree, to the point that if fitting subset of offers is known then the secret is imitated; else it is farfetched to revamp the riddle without knowing honest to goodness number of offers.

4.2.1 Shamir's Scheme of Secret Sharing [2]

In 1979, Adi Shamir created strategy called edge technique for secret sharing. In this technique secret is shared among n members and out of n, any k member shares are required for recreation of secret. It is called (k, n) limit secret sharing plan. The estimation of n and k are connected by the condition.

$n=2k-1$ or $\lfloor n/2 \rfloor + 1 = k$.

Limit technique for secret sharing depends on the rule that for a polynomial of degree n, if all coefficients of polynomial are obscure at that point (n+1) focuses that fulfill the condition are required to discover the estimations of the coefficients. Let p(x) be polynomial speaking to condition of a line, it is defined as

P(x) is a function and it is defined by linear equation i.e. $mx + c$. simply it is equal to y. (4.1)

In (4.1) eq. on the off chance that we put distinctive estimation of x, we get diverse estimation of y.

Let's take one simple e.g. If $m = 3$, $c = 8$.

Then, the equation becomes $y = 3x + 8$ and for

$x = 4$, $y = 3*4+8 = 20$

$x = 5$, $y = 3*5+8 = 23$

$x = -2$, $y = 3*(-2) +8 = 2$ etc.

So if the estimations of m, c are known it is anything but difficult to discover connection amongst x and y. presently, on the off chance that it is given that for x = 1, y = 7. It is unrealistic to discover connection amongst x and y, regardless of the possibility that it is expressed that x and y are connected as condition of straight line, as estimation of m, c are obscure. Since there are two factors, so we required two concurrent conditions to discover the estimations of m, c.

So from above dialog we can reason that for a condition of degree n, with (n+1) obscure factors, we require (n+1) conditions to get the correct connection between the reliant and autonomous variable, however we can get numerous more combines as much we required for sharing the secret. One sets that fulfills the condition is the produced offer of member for secret circulation, and (n+1) is the estimation of k for secret recreation.

1. Shares Generation Phase

i. Select the limit plot (k, n) for conveyance of secret and in view of estimation of k, compose a polynomial p(x) of degree k-1.

ii. It can be randomly chosen (k-1) degree i.e. polynomial according to mathematical equation, like

$q(x) = (a_0 + a_1 x + ... + a_{k-1}\, x^{k-1}) \bmod P$

i.e. a_o is a value to be used for secret key. Select an constant value for a_1 , $a_{2,\ldots\ldots}$ a_{k-1}.

iii. Find more valuable result for modular arithmetic to be applied on GF(P) ,hence

P is greater than (S, n). Here S = secret value that will be shared.

iv. Select n diverse estimations of x to get the distinctive estimations of y. The sets framed by gathering (y, x), are diverse offers for members. Appropriate these offers among the members.

2. Secret Reconstruction Phase

i. Gather k or more number of members share.

ii. Utilizing Lagrange's introduction strategy, reproduce the secret. Secret from the interjection strategy is ascertained from this equation

$$q(x) = \sum_{i=1}^{k} (D_i) \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{(x - x_j)}{(x_i - x_j)} \qquad (4.2)$$

Here, put the value of x= 0 then formula is reduce to

$$q(0) = \sum_{i=1}^{k}(D_i) \prod_{\substack{j=1 \\ j\neq i}}^{k} \frac{(-x_j)}{(x_i - x_j)} \quad (4.3)$$

$$q(0) = \sum_{i=1}^{k}(D_i)\, L_i \quad (4.4)$$

q (0) provide the value of secret data.

So, we can see that how one can distribute and reconstruct the secret using Shamir's secret sharing scheme.

4.2.1.1 Implementation of Shamir's method

For understanding of the method, let us understand it by this example. Let 5 be the secret to be shared.

1. Share generation phase

Step-1: Pick an edge plan to share the secret. Suppose it is (3, 5)

Step-2: Select prime no. for modular arithmetic. Suppose p = 19.

Step-3: To select polynomial (k-1) degree to share the secret,

Let's take an e.g. Where k = 3 so the equation is

y is equal to $a_0x^0 + a_1x^1 + a_2x^2$. (4.5)

Pick value of coefficient a_1, a_2. Suppose $a_1 = 2$, $a_2 = 6$. If the value of $a_0 = 2$. The equation 4.5 reduces to

$y = 5 + 2x^1 + (6*x^2)$.

Step-4: Computation of share of the members.

i) For member-1: suppose x = (-1),

Then y = $(5+2*(-1) + 6*(-1)^2) \bmod 19 = 9 \bmod 19 = 9$.

Hence, the share of 1st member is (-1, 9).

ii) For member-2: suppose x = 0,

Then y = $(5+2*(0) + 6*(0)^2) \bmod 19 = 5 \bmod 19 = 5$.

Hence, the share of 2nd member is (0, 5).

iii) For member-3: suppose x = (1),

Then y = $(5+2*(1) + 6*(1)^2) \bmod 19 = 13 \bmod 19 = 13$.

Hence, the share of 3rd member is (1, 13).

iv) For member-4: suppose x = (2),

Then y = $(5+2*(2) + 6*(2)^2) \bmod 19 = 33 \bmod 19 = 14$.

Hence, the share of 4th member is (2, 14).

v) For member-5: suppose x = (3),

Then y = $(5+2*(3) + 6*(3)^2) \bmod 19 = 65 \bmod 19 = 8$.

Hence, the share of 5th member is (3, 8).

2. Secret reconstruction phase

Step-1: Gather k no. of member's shares.

Suppose

1st member = (-1, 9) = (x_1 , D_1).

2nd member = (0, 5) = (x_2 , D_2).

3rd member = (1, 13) = (x_3 , D_3).

Step-2: Here, first compute the value of L_i (0) using eq. (4.2)

$$L_1(0) = \frac{(-x_2)}{(x_1 - x_2)} \times \frac{(-x_3)}{(x_1 - x_3)} = \frac{(0)}{(-1-0)} \times \frac{(-1)}{(-1-1)} = 0 \bmod (19) = 0$$

$$L_2(0) = \frac{(-x_1)}{(x_2 - x_1)} \times \frac{(-x_3)}{(x_2 - x_3)} = \frac{(1)}{(0+1)} \times \frac{(-1)}{(0-1)} = 1 \bmod (19) = 1$$

$$L_3(0) = \frac{(-x_1)}{(x_3 - x_1)} \times \frac{(-x_2)}{(x_3 - x_2)} = \frac{(1)}{(1+1)} \times \frac{(-0)}{(1-0)} = 0 \bmod (19) = 0$$

So $q(0) = D_1 \times L_1(0) + D_2 \times L_2(0) + D_3 \times L_3(0)$

$= (9\times0) + (5\times1) + (13\times0) = 5 \bmod (19) = 5$ i.e. secret.

Thus, from the above case obviously if k-members enter their offers then secret information can recuperated.

4.2.2 Other Single Secret Schemes

In the same year i.e. in 1979, Blakely [3] developed a method of secret sharing based on hyper-plane. Two non-parallel lines intersect at exactly one point on a plane, three non-parallel planes intercepts exactly at one point. Analogous to this theory any n non-parallel planes intersect exactly at one point. Blakely proposed method of secret sharing by using the above said property of non-parallel planes. According to his algorithm any secret to be shared can be encoded as single coordinate or all coordinates of the intersected point. His method of secret sharing was not as secure as to Shamir's method as any person (participant) who owns any one plane information can encode other plane because the point will also lie in the other plane. So it is not theoretically secure for information sharing.

4.3 Multiple-Secret Sharing Schemes

Consider a situation in which there is more than one missile whose launch codes are different codes and these codes are to be distributed among the scientist. As the codes are different, sharing of codes can be handled in two ways.

- Using single secret scheme multiple time.

- Using multiple-secret sharing scheme.

First method requires each secret to be shared independently and each participant requires remembering shares equal to numbers of shares. If we use multiple-secret sharing schemes then all secrets are treated as a single entity. The participant then requires remembering the less than shares. Many multiple secret sharing schemes have been developed in the past. In 2006, Li Bai developed multiple-secret scheme based on matrix projection.

4.3.1 Li Bai Method [6]

In 2006, Li Bai proposed a procedure of multiple-secret sharing based matrix projection. So it was threshold method of secret sharing. Secrets can be rearranged in matrix form. The projection matrix is calculated and added to the secret matrix. Then a remainder matrix is calculated. Set of non-linear vectors are then used to calculate participant shares using random matrix and vector x.

4.3.1.1 Projection Matrix

Suppose A be matrix of (m*k) order. If matrix (A) rank is k, then the following relation is valid

$$M = A ((AA')^{-1}) A', \quad (4.6)$$

Where A' is transpose of matrix A is called projection matrix.

4.3.1.2 Li Bai Method of Multiple-Secret Sharing

Li Bai method of multiple-secret sharing consists of two phases. Phase-1 is for shares generation and remainder matrix calculation. Phase-2 is for secret matrix reconstruction.

1. Share Construction Phase

i. Arrange m^2 number of secrets in sq. mat S of (m×m) order.

ii. Choose threshold scheme (k, n) and prime no. P > (secrets values, n).

iii. Taken an arbitrary matrix A of (m×k) order.

iv. Pick n- linearly independent x_i vectors of (k×1) order.

v. Calculate vector $v_i = Ax_i$. These are the shares of users.

vi. Calculate the projection matrix $M = A((AA')^{-1})A'$ of order (m×m).

vii. Calculate the remainder matrix R = (S+M) mod P of order (m×m).

Distribute vector v_i as share of user i among the users. Remainder matrix is made public and is known to all.

2. Share reconstruction phase

i. Collect shares from k-users and form matrix $B = [v_1, v_2 \ldots v_k]$ of order (m×k).

ii. Collect remainder matrix R of order (m×m).

iii. Calculate projection matrix $M = B((BB')^{-1})B'$ of order (m×m).

iv. Calculate secret matrix S = (R-M) mod P of order (m×m).

Thus, we can see that how multiple-secret is distributed and reconstruction on Li Bai method of secret sharing. The complexity of the method depends upon finding out of combination of non-linear vectors and calculation of random matrix A.

4.3.1.3 Implementation of Li Bai's Method

Let secrets to be shared are as: 100, 20, 79, 37, 88, 40, 2, 90 and 8. Let the threshold scheme used be (2, 3). Then according to Li Bai's scheme algorithm the sharing and reconstruction of the secrets take place as follows:

1. Shares construction phase

Step-1: Arrange secrets in square matrix form. So secret matrix S is

$$S = \begin{bmatrix} 10 & 40 & 79 \\ 37 & 81 & 40 \\ 21 & 9 & 28 \end{bmatrix}.$$

The order of secret matrix for example is (3×3). So the value of m = 3.

Step-2: Choose threshold scheme (k, m), such that m = (2×k-3). In the example value of m = 3 and according to threshold scheme value of k is selected as 2 and let the total numbers of participants be 3. So threshold scheme is (2, 3). Let pick prime no. used for modular arithmetic be 113.

Step-3: Select a random matrix of order (3, 2).

$$A = \begin{bmatrix} 17 & 88 \\ 111 & 70 \\ 2 & 80 \end{bmatrix}$$

Step-4: Choose n-linear independent vectors of order (k, 1). The value of n is 3, so the vectors chosen are,

$$x_1 = \begin{bmatrix} 17 \\ 4 \end{bmatrix}, \; x2 = \begin{bmatrix} 12 \\ 2 \end{bmatrix}, \; x3 = \begin{bmatrix} 21 \\ 13 \end{bmatrix}.$$

Step-5: Calculation of share vectors.

$$v_1 = A\, x_1 = \begin{bmatrix} 17 & 88 \\ 111 & 70 \\ 2 & 80 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \end{bmatrix} \bmod (113) = \begin{bmatrix} 76 \\ 20 \\ 15 \end{bmatrix}$$

$$v_2 = A\, x_2 = \begin{bmatrix} 17 & 88 \\ 111 & 70 \\ 2 & 80 \end{bmatrix} \begin{bmatrix} 12 \\ 2 \end{bmatrix} \bmod (113) = \begin{bmatrix} 41 \\ 03 \\ 71 \end{bmatrix}$$

$$v_3 = A\, x_3 = \begin{bmatrix} 17 & 88 \\ 111 & 70 \\ 2 & 80 \end{bmatrix} \begin{bmatrix} 21 \\ 13 \end{bmatrix} \bmod (113) = \begin{bmatrix} 32 \\ 77 \\ 65 \end{bmatrix}$$

Step-6: The projection matrix of A is

$$M = A((AA')^{-1})A' = \begin{bmatrix} 91 & 84 & 110 \\ 84 & 102 & 65 \\ 110 & 65 & 35 \end{bmatrix}$$

Step-7: The remainder matrix R = (S- M) mod (p)

$$R = \begin{bmatrix} 10 & 40 & 79 \\ 37 & 81 & 40 \\ 21 & 9 & 28 \end{bmatrix} - \begin{bmatrix} 91 & 84 & 110 \\ 84 & 102 & 65 \\ 110 & 65 & 35 \end{bmatrix} \bmod (113)$$

$$= \begin{bmatrix} 32 & 69 & 82 \\ 66 & 92 & 88 \\ 24 & 57 & 106 \end{bmatrix}.$$

The remainder matrix is made public.

3. Secret reconstruction phase

Step-1: Gather k participant shares. Let 1_{st} participant and 2_{nd} participant use their shares for secret reconstruction, so collected shares are $v_1 = \begin{bmatrix} 76 \\ 20 \\ 15 \end{bmatrix}$, $v_2 = \begin{bmatrix} 41 \\ 03 \\ 71 \end{bmatrix}$.

So the matrix B equal to $B = [v_1, v2] = \begin{bmatrix} 76 & 41 \\ 20 & 03 \\ 15 & 71 \end{bmatrix}$.

Step-2: collect remainder matrix $R = \begin{bmatrix} 32 & 69 & 82 \\ 66 & 92 & 88 \\ 24 & 57 & 106 \end{bmatrix}$

Step-3: The projection matrix $M = B((BB')^{-1})B' = \begin{bmatrix} 91 & 84 & 110 \\ 84 & 102 & 65 \\ 110 & 65 & 35 \end{bmatrix}$

Step-4: The secret matrix S = (R+ M) mod (113).

$$S = \begin{bmatrix} 32 & 69 & 82 \\ 66 & 92 & 88 \\ 24 & 57 & 106 \end{bmatrix} + \begin{bmatrix} 91 & 84 & 110 \\ 84 & 102 & 65 \\ 110 & 65 & 35 \end{bmatrix} \text{ mod } (113)$$

$$= \begin{bmatrix} 10 & 40 & 79 \\ 37 & 81 & 40 \\ 21 & 9 & 28 \end{bmatrix}$$

Thus, we see that secret matrix calculated at step-4 is equal to secret matrix actually distributed. Hence, above example explain how secret can be shared and reconstructed.

4.4 Dynamic Multi-Secret Sharing Scheme

Every one of the techniques characterized above are single time utilize plans i.e. on the off chance that we need to change privileged insights then we need to appropriate mysteries shares among clients. Nonetheless on the off chance that we need to utilize a plan so we can change a secret without changing the offers of clients. At that point such a plan is called dynamic multi secret sharing plan. How about we take a case, at the point when there is more than one number of rockets. All the secret dispatch codes of the rockets are segregated into riddle offers and puzzle shares are appropriated between the customers. However when the new rockets have doled out new dispatch code then we have to again create new offers and scatter among customers. Appropriating offers to every part is a computationally and correspondence clever complex process. Appropriately to avoid this issue dynamic multi-secret scheme are made.

In 2008, Lin and Yeh [1] developed a dynamic multi-puzzle sharing using hash work. By using this arrangement each time when rocket dispatches then customer does not have to reveal his novel riddle share. It can create a pseudo puzzle share with the help of hash limit and his exceptional secret offers, so that when new rockets are made the new dispatch code is doled out to each by then by changing around an impetus in scheme, conveying various figured a motivator by dealer, same riddle shares having with each customer can be go about as secret offers of new dispatch code and can be used to fabricate the dispatch code of new rockets. So same puzzle share is used for various secret and this arrangement is usable various number of times.

Chapter 5

Proposed Method of Dynamic Multi-Secret Sharing Scheme

5.1 Introduction

As explained in the previous chapter, dynamic multi-secret sharing scheme using hash function is used for multiple secrets. The method is quite tedious for cryptanalyst to find out the secrets, if he does not knows the shares. Even if cryptanalyst [12] know about the pseudo secret shares generated using original secret shares and hash function, he will not able to find original secret shares as hash function is one way function. Thus it is not possible to know the input by knowing output. The strength of the scheme depends upon the randomness of hash function used. Since the proposed scheme uses Shamir's threshold scheme therefore the security of this scheme is similar to that of Shamir's scheme.

Let us consider a scenario in which the dealer selects shares of secret and distributes them to the users. During the distribution if secret shares are revealed to someone then he can know about secret. Moreover the dealer can act as cheater as he knows the secret shares. Lin Yeh method of dynamic multi-secret sharing does not protect this type of attack.

In Lin-Yeh method if any participant tries to cheat the group by entering his private share wrongly as then secret cannot be reconstructed correctly. However Lin Yeh method of dynamic multi-secret sharing does not provide any scheme of detecting the cheater in the group.

In this thesis two methods are proposed which remove the need of secret share distribution by the dealer using secure channel and to find out the cheater in the group. The following section explains the proposed algorithm stating the method of secret distribution and secret reconstruction.

5.2 Proposed Scheme

In proposed method of Dynamic multi-secret sharing scheme employs hash function and modular arithmetic concept on primitive element. In first proposed method modular arithmetic operation are applied on primitive elements. Master secret shares x_j are choosing by user. Then

user calculate y_j using equation ($y_j = g^{x_j} \bmod p$, where g is a primitive element) and send this value to the dealer. The dealer can checks that no two users choose same secret shares by comparing their respective y_j values he got from users. There is no secure channel is required by the dealer to distribute secret shares and users choose their master secret shares by themselves.

In second proposed method we calculate a W matrix by applying hash function on C matrix so that during reconstruction of secrets firstly, k-participants shares are collected and C matrix is calculated. If the participants entered the shares correctly the secret matrix can be calculated correctly. However if any one or more than one participants try to cheat then the proposed method is able to detect it.

5.2.1 Algorithm of Proposed Scheme

The proposed method comprises of three phases, the system initialization stage, shares generation phase and secret reconstruction phase. The algorithms of these phases are mentioned below.

Let there be k group secrets S_1, S_2 …S_k.

Phase1: The Framework Initialization Stage

In the framework initialization phase the dealer D is select the accompanying parameters.

1. P: A vast prime number can have any value depend on number of client and group secrets value, p > (group secrets, n).
2. g: The primary component upon GF (p).
3. h (.): The safe one - way hash work that acknowledges contributions of the any dimension i.e. creates a settled length yield.
4. IDj : With respect to the client the value assigned to Identifiers is Uj (user) for j = 1 to n. here n is the number of clients which are having the secret share value.

Phase2: The Pseudo Secret Share Generation Stage

Suppose there is a Dealer with name D that can share group i.e. k secrets ($S_1, S_2, \dots, S_i$), for i= 1 to k i.e n clients.

1. Each user Uj (j=1, 2, 3… n) select value of master secret share x_j itself. Then it compute $y_j = g^{x_j} \bmod p$, keeps x_j secretly and send y_j to the dealer by public channel so that dealer can ensure that $y_j, \neq y_j$.

   Thus there is no need of secure channel to deliver master secret shares. Therefore there is no possibility that secret shares are revealed to any third person during distribution. Since the dealer does not select master secret shares x_j and has only y_j dealer also cannot become a cheater as is possible in the case of Lin Yeh method.

2. k number of secrets the D i.e. dealer has $(S_1, S_2, \dots, S_i)$. At that point he creates k is the no. of polynomial $f_{i(x)}$ of (i-1) degree, for i= 1 to k, comparing to the privileged insights takes after

$$\left.\begin{aligned} f_1(x) &= S_1 && \text{where } f_1(0) = S_1 \\ f_2(x) &= S_2 + d_1 x && \text{where } f_2(0) = S_2 \\ &\vdots \\ f_i(x) &= S_i + d_1 x + \dots + d_{i-1} x^{i-1} && \text{where } f_i(0) = S_i \end{aligned}\right\} \quad (5.1)$$

   Where $(S_1, S_2, \dots, S_i)$ are the insider facts themselves whose equation. that equation is polynomial to be computed and d_1 to $d_{(i-1)}$ i.e. chosen arbitrarily by the merchant of any constants from GF (p).

3. To evaluate for i= 1 to k and j= 1 to n

$$V_{ij}\ (i \in k, j \in n) = f_i(ID_j) \bmod p = \left.\begin{bmatrix} f_1(ID_1) & f_1(ID_2) & \cdots & f_1(ID_n) \\ f_2(ID_1) & f_2(ID_2) & \cdots & f_2(ID_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(ID_1) & f_k(ID_2) & \cdots & f_k(ID_n) \end{bmatrix}\right\} \quad (5.2)$$

4. Each user compute C_{ij}(pseudo secret share) by using hash function and master secret share x_j.

   $C_{ij} = (h^i(x_j) \oplus x_j) \bmod p$, where $h^i(x_j)$ indicates i progressive uses of h to x_j.

   i.e. $C_{1j} = (h(x_j) \oplus x_j)$ modulo (p)

   $C_{2j} = (h(h(x_j)) \oplus x_j)$ modulo (p)

   .

   .

   $C_{kj} = (h^k(x_j) \oplus x_j)$ modulo (p)

   (5.3)

   And then sends C_{ij} to the dealer.

5. Dealer now compute

   $R_{ij} = V_{ij} - C_{ij}$ modulo (p). (5.4)

   $W_{ij} = h(h^i(x_j) \oplus x_j)$ modulo (p). (5.5)

   The dealer calculates matrix W_{ij} by applying hash function on the matrix C_{ij} (a matrix of pseudo secret shares calculated by users using their master secret share, hash function and ex-or function) and publish it publically.

The dealer publish the calculated values of R_{ij} and W_{ij} publically and known to all. m^{th}

Phase 3: The Group Secret Reconstruction Stage

To reproduce m^{th} bunch secret, called $S_m$out of (S_1,S_2 ,… ,S_k) i.e. S_m is belongs to (S_1,S_2 ,… ,S_k) at any rate m members out of n clients should helpfully play out the accompanying strides with the gathering secret merge.

1. To compute the pseudo secret share of every user U_j, for j = 1 to m, (condition is $m \leq n$) as follows:

   C_{mj}= (h^m (x_j) $\oplus x_j$) mod p and at that point it will post to the gathering secret merge over a protected channel.

   The gathering secret combiner checks legitimacy of every member's pseudo secret share C_{mj} by the accompanying conditions:

   W_{mj} = h ($h^m(x_j) \oplus x_j$) mod p.

   If any user is cheating at the time of reconstruction of secret by giving wrong secret share then we can check by analyzing hash function on its share scheme and match it with respective value in W_{ij} matrix and find that secret share given is right or wrong. This cheater detection technique is not available in Lin Yeh method.

2. After accepting all C_{mj}, for j = 1 to m, effectively gathering secret combiner remakes the m_{th} assemble secret S_m takes after: [4]

$$S_m = \sum_{j=1}^{m}(C_{lj} + R_{lj}) \prod_{r=1,r\neq j}^{m} \frac{-ID_r}{ID_j - ID_r} \text{ mod p.}$$

As framework R_{ij} is publically known in this way the gathering secret combiner get R_{mj} relating to the particular C_{mj} and ID_j of the individual clients from R_{ij} lattice (i.e. in the event that third secret is to be recreate and first, second and third clients are takes an interest in secret remaking then R_3j have values R_31 R_32 R_33 taken from R_{ij} lattice known publically).

Thusly one can disperse insider facts and remaking of privileged insights should be possible by utilizing above depict plans. The plan can be effectively executed. In the event that another secret is to be included by merchant then he doesn't need to convey the ace secret shares among clients.

5.3 Implementation of Proposed Scheme

We can understand the appropriate working of plan with a basic case of numeric values. Suppose there are six number of user i.e. (n=6)

Phase1: The system initialization stage

First initializes the following public parameters of the dealer D is.

1. To select vast prime no. i.e. p. suppose the prime no. is p=17.
2. Then select primary component g upon GF (p).
   Give the primary component a chance to be 4, It is pick the route that by taking different energy of g = 4 and applying modulo p on its energy one can produce every component of GF (p). From above estimation of p and g, we ascertain different esteems as takes after:
   GF (17) = 4^bmod 17 (b= 0, 1… 16).
3. Select h (.) a safe one - way hash work which acknowledges contributions of any dimension and produces a settled dimension yield. Take MD5 hash-function [14] that acknowledges any dimension input message and deliver a message process of 128 bits as yield.
4. IDj: Regarding to client the identifiers Uj i.e. client for j = 1, 2… n. In this manner identifiers dole out to every client i.e. IDj for each jth client, here value j= {1 to n}. Let the qualities doled out of different clients b:-

ID of client 1 is ID1 = 1

ID of client 2 is ID2 = 2

ID of client 3 is ID3 = 3

ID of client 4 is ID4 = 4

ID of client 5 is ID5 = 5

ID of client 6 is ID6 = 6

Phase 2: The generation stage of pseudo secret share:

Step 1: If merchant D can share k aggregate mysteries S_i, for i= 1 to k, among n clients. Leave the alone number of privileged insights be, k= 4. At that point the insider facts Si, i.e. i = {1 to k}. Let the mysteries taken be as per the following:-

S_1 = Master i.e. m secret 1 = 11

S_2 = Master i.e. m secret 2 = 13

S_3 = Master i.e. m secret 3 = 15

S_4 = Master i.e. m secret 4 = 16

Step 2: Each user Uj (where j=1, 2, 3… 6) selects value of master secret share x_j itself.

Compute $y_j = g^{x_j}$ modulo p, and keep x_j secretly and post y_j to dealer by the public channel. The dealer thus collects y_j 's of all the users. So that dealer can ensure that $y_j, \neq y_j$.

There is no need of secure channel to deliver master secret shares x_j . It is not possible to extract $x_j's$ by knowing the value of $y_j's$

Suppose there be six user i.e. (n=6) and their corresponding x_j 's be are: -

For user 1 Secret share is x_1 and x_1 = 01

For user 2 Secret share is x_2 and x_2 = 05

For user 3 Secret share is x_3 and x_3 = 07

For user 4 Secret share is x_4 and x_4 = 10

For user 5 Secret share is x_5 and x_5 = 09

For user 6 Secret share is x_6 and x_6 = 03

Respective values of y_j can be calculated as follows:

$y_1 = 3^{01} \text{mod} 17 = 03$

$y_2 = 3^{05} \text{mod} 17 = 05$

$y_3 = 3^{07} \text{mod} 17 = 11$

$y_4 = 3^{10} \text{mod} 17 = 08$

$y_5 = 3^{09} \text{mod} 17 = 14$

$y_6 = 3^{03} \text{mod} 17 = 10$

y_j are sent to the dealer by respective user's j ($1 \leq j \leq n$). Dealer then checks that no two different y_j's have same value. If any of two or more y_j's values are equal, then dealer inform those users whose values are same. Such users re-select their x_j and send new value of y_j to the dealer. The dealer rechecks the condition of different y_j and the process is repeated till the condition of all y_j's being different is satisfied.

Step 3: The merchant has k number of privileged insights ($S_1, S_2 \ldots S_i$). At that point he produces $f_{i(x)}$ of degree (i-1), for i= 1 to k, (k number of polynomial relating to the insider facts takes after

$f_1(x) = S_1$ $\qquad$ $f_1(0) = S_1$

$f_2(x) = S_2 + d_1 x$ $\qquad$ where $f_2(0) = S_2$

.

.

$f_i(x) = S_i + d_1 x + \ldots + d_{i-1} x^{i-1}$ threrefor $f_i(0) = S_i$

Where $(S_1, S_2, \ldots, S_i)$ are simply the insider facts that polynomial is figured for that reason $d_1 \ldots d_{i-1}$ are any const. from GF (p), which are chosen arbitrarily by the merchant.

For instance, if the merchant has 4 insider facts specifically (11, 13, 15, 16) the relating polynomials produced by the merchant for d1 = 4, d2 = 5 and d3 = 6 is follow:-

$f_1 = 11$

$f_2 = 13 + 4x$

$f_3 = 15 + 4x + 5x^2$

$f_4 = 16 + 4x + 5x^2 + 6x^3$

Step 4: Ascertain matrix V_{ij} by utilizing polynomial shaped in step 3. For i= 1 to k and

j= 1 to n

$$V_{ij}\ (i \in k,\ j \in n) = f_i(ID_j) \bmod p = \begin{bmatrix} f_1(ID_1) & f_1(ID_2) & \cdots & f_1(ID_n) \\ f_2(ID_1) & f_2(ID_2) & \cdots & f_2(ID_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(ID_1) & f_k(ID_2) & \cdots & f_k(ID_n) \end{bmatrix}$$

For instance for k=4 quantities of insider facts and n=6 clients with ID_j = (1, 2… 6) grid condition [5.2] utilizing f1 to f4 as above diminish to.

$$V_{4X6} = \begin{bmatrix} 11 & 11 & 11 & 11 & 11 & 11 \\ 16 & 02 & 05 & 08 & 11 & 14 \\ 05 & 03 & 09 & 06 & 11 & 07 \\ 08 & 03 & 13 & 16 & 07 & 15 \end{bmatrix}$$

Step 5: computes pseudo secret share C_{ij} for secret S_i by applying hash function on the master secret share x_j i.e. client j and $\oplus$ with x_j is takes after

$C_{ij} = (h^i(x_j) \oplus x_j)$ modulo (p), where, $h^i(x_j)$ means i progressive utilizations of h to x_j.

i.e. $C_{1j} = (h(x_j) \oplus x_j)$ modulo (p)

$C_{2j} = (h(h(x_j)) \oplus x_j)$ modulo (p)

.

.

$C_{kj} = (h^k(x_j) \oplus x_j)$ modulo (p)

It then post C_{ij} to the dealer.

The over 4 stages might be rehashed for all estimations of x_j for j= (1, 2 ...n) to get the last C_{ij} lattice. Therefore the C_{4X6} for k =4 and n = 6, calculated using above steps is as follows

$$C_{4X6} = \begin{bmatrix} 14 & 08 & 11 & 15 & 05 & 15 \\ 12 & 14 & 03 & 11 & 05 & 09 \\ 08 & 03 & 03 & 02 & 04 & 00 \\ 07 & 14 & 11 & 05 & 14 & 09 \end{bmatrix}$$

Step 6: In the wake of getting every one of the estimations of C_{ij} network, merchant D now calculates R_{ij} and W_{ij} using equation 5.4 and 5.5 as follows:-

$R_{ij}= V_{ij} - C_{ij} \bmod p$

In the present case the condition moves toward becoming

$R_{4\times6} = V_{4\times6} - C_{4\times6} \bmod 17.$

$$R_{4\times6}=\begin{bmatrix} 11 & 11 & 11 & 11 & 11 & 11 \\ 16 & 02 & 05 & 08 & 11 & 14 \\ 05 & 03 & 09 & 06 & 11 & 07 \\ 08 & 03 & 13 & 16 & 07 & 15 \end{bmatrix} - \begin{bmatrix} 14 & 08 & 11 & 15 & 05 & 15 \\ 12 & 14 & 03 & 11 & 05 & 09 \\ 08 & 03 & 03 & 02 & 04 & 00 \\ 07 & 14 & 11 & 05 & 14 & 09 \end{bmatrix} \bmod 17$$

$$= \begin{bmatrix} 14 & 03 & 00 & 13 & 06 & 13 \\ 04 & 05 & 02 & 14 & 06 & 05 \\ 14 & 00 & 06 & 04 & 07 & 07 \\ 01 & 06 & 02 & 11 & 10 & 06 \end{bmatrix}$$

$W_{ij}= h (h^i(x_j) \oplus x_j) \bmod p$

In the present case the condition moves toward becoming

$W_{4\times6} = h (C_{4\times6}) \bmod 17.$

$$W_{4\times6} = h\begin{bmatrix} 14 & 08 & 11 & 15 & 05 & 15 \\ 12 & 14 & 03 & 11 & 05 & 09 \\ 08 & 03 & 03 & 02 & 04 & 00 \\ 07 & 14 & 11 & 05 & 14 & 09 \end{bmatrix} \bmod 17 = \begin{bmatrix} 08 & 11 & 01 & 00 & 04 & 00 \\ 02 & 08 & 06 & 01 & 04 & 01 \\ 11 & 06 & 06 & 03 & 11 & 09 \\ 05 & 08 & 01 & 04 & 08 & 01 \end{bmatrix}$$

The dealer publishes R_{ij} and W_{ij} openly. However the secrets $(S_1, S_2, \dots, S_k)$ are known just to the merchant

Phase3: The group secret reconstruction stage

To reproduce m_{th} assemble secret, called S_m out of (S_1,S_2 ,… ,S_k) i.e. S_m ϵ(S_1,S_2 ,… ,S_k) in any event m members out of n clients should agreeably play out the accompanying strides with the gathering secret is merge.

Step 1: Every client Uj, for j to m, where (m ≤ n) registers his pseudo secret share as C_{mj} utilizing x_j , hash work and ⊕ operation and afterward posts it to the gathering secret merge over a protected channel.

$C_{mj}=(h^m(x_j) \oplus x_j) \bmod p$

Give the client a chance to element i.e. (no.) 3, 4, 5 and 6 compute their C_{mj} and post it to aggregate secret to merge. With the goal that he can discover fourth secret. In display case C_{43} = [11], C_{44} = [05], C_{45} = [14] and C_{46} = [09]

Along these lines, the gathering secret combiner shape C (1×4) network utilizing above qualities$C_{1\times4} = \begin{bmatrix}11 & 05 & 14 & 09\end{bmatrix}$

If the group secret combiner wants to check that every pseudo secret share given by each user is correct, then he can check by calculating hash of each pseudo secret and match it with respective values from W_{ij} matrix publish publically by dealer.

Step 2: The equation to calculate hash of pseudo secret share given by users is as follows:-

$W = h (h^m(x_j) \oplus x_j) \bmod p$

For example $W = h (C_{1\times4}) \bmod 17$

$W_{1\times4} = \begin{bmatrix}01 & 04 & 08 & 01\end{bmatrix}$

Which is same as four entries of last row of $W_{4\times6}$ matrix knowing publically.

After accepting all C_{mj}, accurately for j = 1 to m, the gathering secret merge remakes the m_{th} amass secret Sm, said underneath.

Step 3: The matrix R_{ij} is publically known consequently gathering secret merge can acquire R_{mj} relating to the particular C_{mj} and IDj of the individual clients who gives their secret share.

For instance in representation under thought

$R_{1\times4} = [02 \quad 11 \quad 10 \quad 06]$

ID = [3, 4, 5, 6]

Step 3: The ace secret Sm is gotten from C_{mj}, IDj, and R_{mj} utilizing the accompanying condition.

$$S_m = \sum_{j=1}^{m}(C_{lj} + R_{lj}) \prod_{r=1,r\neq j}^{m} \frac{-ID_r}{ID_j - ID_r} \bmod p$$

To instance below thought the fourth secret S4 is produced takes after:

$$S_4 = [((11+2)\times \frac{-4}{3-4} \times \frac{-5}{3-5} \times \frac{-6}{3-6}) + ((5+11)\times \frac{-3}{4-3} \times \frac{-5}{4-5} \times \frac{-6}{4-6}) + ((14+10)\times \frac{-3}{5-3} \times \frac{-4}{5-4} \times \frac{-6}{5-6})$$

$$+ ((9+6) \times \frac{-3}{6-3} \times \frac{-4}{6-4} \times \frac{-5}{6-5})] \bmod 17$$

$$= [((13) \times 20) + ((16) \times -45) + ((24) \times 36) + ((15) \times -10)] \bmod 17$$

$$= [260 + (-720) + 864 + (-150)] \bmod 17$$

$$= [254] \bmod 17$$

$S_4 = 16$. (4^{th} Secret)

In summary, a secret Sm is generated by the group secret combiner by knowing publically known R_{ij} and ID_j and values of C_{mj} obtained on secure channel from users 1 to m.

5.2.3 Advantages of Proposed Scheme

1. Proposed scheme have cheater detection property.
2. Complexity is direct function of value of secret to be reconstructed i.e. if lower secret is to be reconstructed then less number of users is required and if higher level secret is to be reconstructed then more number of users is required.
3. No need of secure channel for distribution of master secret shares decrease complexity

Chapter 6

Security Analysis and Conclusion

6.1 Introduction

Any secret sharing [11] scheme is considered to be strong if the complexity of cryptanalysis is very high. In cryptography the brutal attack [16] is the type of attack in which all the possible keys of the algorithm are tried for obtaining the secret. Various types of cryptanalytic methods for a given scheme are compared with complexity of the brute force attack. If the complexity of various cryptanalytic attacks is of the same order as that of brute force attack, then the system is said to be computationally strong.

In our method of dynamic multi-secret sharing the security analysis mainly depends upon the application of hash function to calculate C matrix and modular arithmetic over primitive element.

6.2 MD5 Hash Function Security Analysis

The MD5 calculation makes them intrigue property that all of the yield is a component of all of the information. The multifaceted nature in the rehashed utilization of the primitive capacities and the added substance steady T[i] together with the roundabout left moves which are exceptional to each round create a very much blended hash result. This system makes it improbable that two messages which have same comparability will have a similar hash result. Implying that, MD5 has second pre-picture assault resistance.

MD5 produces a solid 128-piece hash code. It has been demonstrated that discovering two messages having a similar hash esteem requires 264 operations and finding a message given its comparing message process will take 2128 operations, this is known as the pre-picture assault.

Brute-Force Attack

The unadulterated animal compel assault if there should arise an occurrence of secret sharing plans is one in which all conceivable expression of a specific length are attempted until the right one is found. This assault is wasteful yet ensured to work. That is the reason one generally picks the length of the hash so extensive that outcome such that the animal compel assault winds up plainly unrealistic or too moderate and along these lines less appealing.

6.3 Analysis of Proposed Method

The possible types of attacks which can take place at various stages in the proposed scheme and their possible complexities are as follows:-

Attack 1:- In the introduction stage, every member picks secret share by her/himself. In this way is totally incomprehensible that merchant can turn into a con artist moreover it is not possible for any other person to know about secret shares except the dealer.

Attack 2:- Assailant may endeavor to get the secret offer of client j, x_j from $y_j = g^{\wedge}(x_j) \bmod p$. The many-sided quality to get the secret shadow x_j is equivalent to illuminating discrete logarithm. In this way it is computationally costly for the assault to get x_j from y_j.

Attack 3:- Every member's secret share is picked without anyone else. So the secret share is classified. Regardless of the possibility that the pseudo secret share C_{ij} is traded off, any vindictive foe can't effectively get x_j from C_{ij} as hash function is one way function [8].

Attack 4:- A malignant member U_j may send a false secret share C_{ij} which can be confirmed by the group secret combiner since he have the knowledge of W_{ij} which can be used for verification.

Attack 5:- The group secret combiner cannot reconstruct corresponding group secret, if the number of shares received less than threshold because it is based on Shamir's secret sharing scheme.

6.4 Comparison of the Performance of Two Schemes

In summary we can explain the major difference between Lin Yeh's scheme and proposed scheme as follows:-

In Lin Yeh's scheme the dealer has to select master secret shares x_j where j=1 to n Where n is number of users) and master secrets S_i i.e. i = 1 to k. where k is number of master secrets). Dealer distribute with the respective user's j master secret shares x_j over secure channel shown in Figure 6.1. Second, there is no method to verify the secret shares given by user at the time of secret reconstruction. Therefore, any user can give a wrong share to group secret combiner.

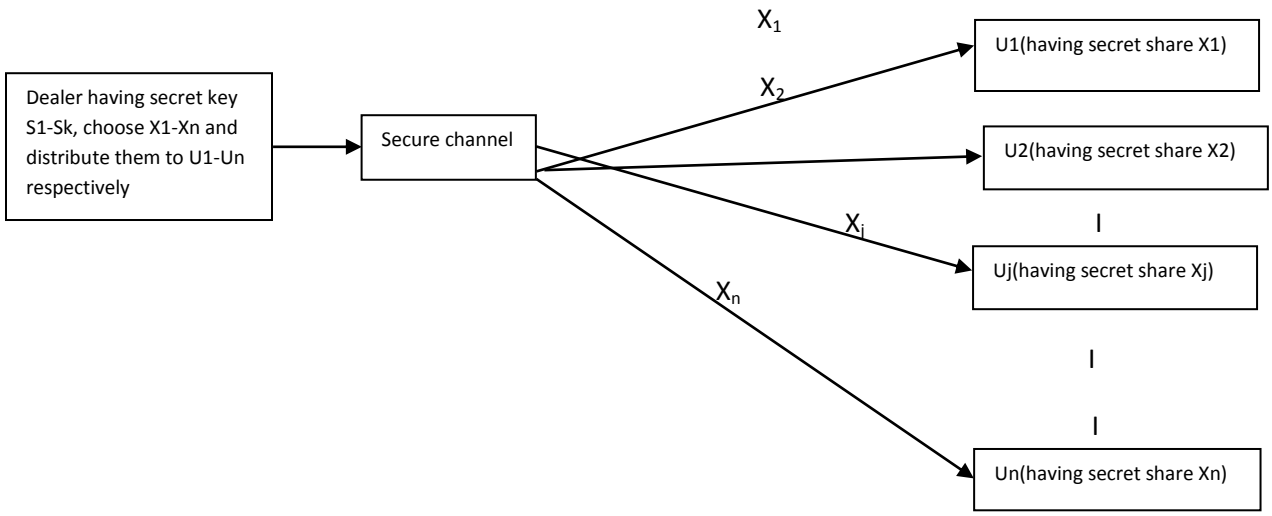

Figure 6.1 Lin Yeh Method of Share Distribution

In proposed scheme the user's themselves select the master secret shares x_j (Therefor j= 1 to n. where n is number of users). Dealer has to select only master secrets S_i (Therefore i = 1 to k. where k is number of master secrets). Each of the users calculates a value y_j using his master secret share x_j and a primitive element g by using equation $y_j = (g^{xj}) \bmod p$ and post it to the dealer over public channel, so that he can verify that no two y_j have same values shown in Figure 6.2. Therefore there is no need of secure channel in initial distribution of master secret shares; moreover it is not possible for any other person to know about master secret shares. Second, there is a method to verify the secret shares given by user at the time of secret reconstruction. A W_{ij} matrix is calculated by applying hash function on C_{ij} matrix. Therefore, in

the event that a pernicious member U_j may post a false secret share C_{ij} which can be checked by the group secret combiner by applying hash function on the received C_{ij} values and verify it with the respective values in W_{ij} matrix since he have the knowledge of W_{ij} matrix.

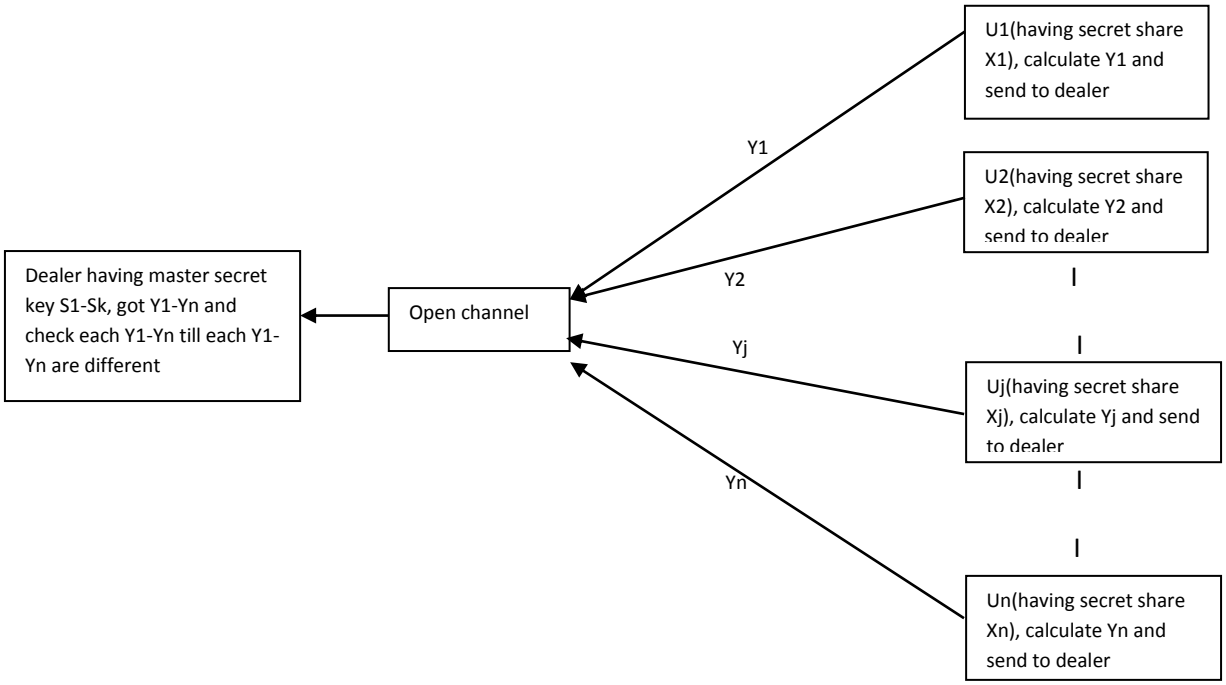

Figure 6.2 Proposed Method of Share Distribution

The comparison of system performance among the two schemes using various parameters discussed. How our scheme takes equal time as taken by Lin-Yeh's scheme but it provides more security with decrease in complexity level. Here, we introduce a method due to which even dealer cannot think of becoming a cheater. Various parameters are being discussed below in the Table 6.1:

TABLE 6.1. Comparison Our Scheme with Lin-Yeh's Scheme

Capability	Lin Yeh's scheme	Our scheme
Need of security channel during secret share distribution	Yes	No
Need of security channel during sending pseudo secrets to dealer as well as group secret combiner.	Yes	Yes
Participant choose his secret share	No	Yes
Group secrets corresponding threshold value	Yes	Yes
The group secret combiner is able to check whether participant's pseudo secret share is true or not	No	Yes

6.5 Conclusion

The secret sharing is a critical technique to understand the disseminated data security utilizing information encryption. It is additionally a basic apparatus in multi-party setting. It has been connected in numerous applications, for example, secret mission information, and computerized money, amass marks et cetera. Over twenty years has gone since the main secret sharing convention has been designed. Various secret sharing plans were proposed from that point forward, which viably quickened the improvement of the hypothesis of data security and the broadly utilization of results of data security. Here we propose a dynamic secret sharing arrangement, in light of XOR operation, the unmanageability of discrete logarithm and hash capacities. The proposed plot has justifies then Lin-Yeh's plan. In proposed conspire each member picks the secret share by her/him. Is completely incomprehensible for merchant to wind up plainly a con artist and it needn't bother with a protected channel during initial distribution phase. The scheme has simple verifiable phase. So this scheme can be used in same practical cases such as secret sharing in electronics commerce, electronic government etc.

6.6 Future Scope

Cheater detection in secret sharing checks if any participant tends towards enter his secret share wrong. However, some other person may also attempt dynamic multi-secrets sharing with cheater detection scheme to enter the share vector of other participant due to some rivalry. So there must be technique for some authentication so that only authorized participant must has right to enter his shares. One old concept of secret sharing is that changing key frequently keeps more secure. Therefore, once the secret matrix is reconstructed there should be process of changing pseudo matrix C and shares of participants in case of detection of intrusion in the system. The future scope can be summarized as.

1. Insertion of authentication scheme.
2. Some more complicated cryptographic technique as elliptic cryptographic curve techniques can be used at time of secret distribution process. The elliptic curve cryptography is a way to deal with open key cryptography in view of the arithmetical structure of elliptic curve over limited fields and has strong algebraic properties.

References

1. Atul Kahate, Cryptography and network security, second edition, India: Tata McGraw-Hill.
2. Shamir Adi, "How to share a secret", Communication of ACM, vol. 22(11), pp. 612-613, November 1979.
3. Blakely G., "Safeguarding cryptographic keying", In Proc. Of AFIPS, National computer conference, 1979.
4. Lin Han-Yu and Yeh Yi-Shiung, "Dynamic Multi-Secret Sharing Scheme", Int. J. Contemp. Math. Sciences, Vol. 3, no.1, pp. 37-42, 2008.
5. William Stallings, Cryptography and Network Security, third edition, India: Pearson Education
6. Li Bai, "A strong ramp secret sharing scheme using matrix projection" , Proceeding of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 652-656, 2006.
7. Diffie W., Hellman M., "New directions in cryptography", IEEE Transactions, on Information Theory, IT-22 (6), pp. 644-654, 1976.
8. He J., Dawson E., "Multistage secret sharing based on one-way function", Electronics Letters, vol. 30 (19), pp. 1591-1592, 1994.
9. Bogdnav Dan, "How to securely perform computation on secret share data" ,Master's thesis, University of Tartu, 2007
10. Wikipedia, Article from encyclopaedia, internet.
11. Jackson W.A., Martin K. M., Keefe C. M. O Keefe, "On sharing many secrets", Advances in Cryptology − ASIACRYPT'94, Springer-Verlag, pp. 42-54.
12. Menezes, P. Oorschot, S. Vanstone, Handbook of applied cryptography, CRC Press.
13. C.J. Mitchell, F. Piper, P. Wild, Digital signature, In: Simmons, G.J. (Ed.), Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992, pp. 325-378.
14. Joseph Sterling Grah, Hash functions in cryptography.
15. Forouzan, Cryptography and network security, Tata McGraw-Hill.
16. Mironov Ilya, "Hash functions: Theory, attacks, and applications", Microsoft Research, Silicon Valley Campus, November, 2005.

17. Anish Mathuria & Colin Boyd, Protocols for authentications and key establishment, Springer
18. Eric Cole, Network Security Bible, India: Wiley.
19. Parode Terry & Gordon Snyder, Network security, Delmor Publication.
20. Olifer, Computer networks, Wiley.
21. D. Gollman, Computer security, Wiley.
22. Hallberg, Networking a beginning guide, TMH.
23. Ata Elahi & Mehran Elahi, Data, network & internet communication technology, Delmor learning publication