Secret sharing schemes and an application to e-voting

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Preeti

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2015

Supervisor: Dr. Ayan Mahalanobis

This is to certify that this dissertation entitled Secret sharing schemes and an application to e-voting towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents the research carried out by Preeti at Indian Institute of Science Education and Research under the supervision of Dr. Ayan Mahalanobis, Assistant Professor, Mathematical Sciences , during the academic year 2014-2015.

Dr. Ayan Mahalanobis

Committee:
Dr. Ayan Mahalanobis
Dr. Baskar Balasubramanyam

Dedicated to my friend M. Sainath

Declaration

I hereby declare that the matter embodied in the report entitled Secret sharing schemes and an application to e-voting are the results of the investigations carried out by me at the Mathematical Sciences, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Ayan Mahalanobis and the same has not been submitted elsewhere for any other degree.

Preeti

Acknowledgments

I would like to express my sincere gratitude towards my supervisor, Dr. Ayan Mahalanobis, Assistant Professor, Department of Mathematics for his support, guidance and belief in me. His constant motivation helped me to improve immensely, especially in expressing my ideas clearly. I am also grateful to the Mathematics Viva Committe and Dr. Baskar Balasubramanyam for attending my presentations throughout the year and pointing out problems being overlooked.

Finally, I thank to my parents and friends for their encouragement, advice and support throughout the course of this work.

Abstract

We present a way of sharing a secret S into n shares such that the collusion of any k shares results in the reconstruction of secret S and no $k-1$ shares can do so. This way of sharing secret was first introduced by Shamir in 1979 and is named after him as Shamir's secret sharing scheme. We then mention some of the useful properties of Shamir's secret sharing schemes. Various approaches towards constructing a perfect secret sharing scheme are made, one of them has been constructed by Simmons using projective varieties. The theory of projective varieties helps us to construct different types of schemes according to their requirements. We show that these schemes are perfect. These enable us to secure the secret S and are reliable. They are used in many practical applications and one of them is e-voting using the internet. With the wide availability of the internet everywhere these days, there is a need for the development of an e-voting scheme. It is easy for a person to vote over the internet, hence e-voting schemes help in increasing the number of electors and thus participation in democracy. It is being used in a number of countries presently, for example Switzerland. In India, it was first introduced in Gujarat in 2011. We introduce the construction of an e-voting scheme using secret sharing schemes. Later we discuss the advantages and issues of e-voting scheme.

Contents

Chapter 1

Introduction

Liu [7] considered the following problem:

Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry? To answer it, we have to first observe that for any group of scientists, there must be at least one lock they cannot open. Moreover, for any two different groups of five scientists, there must be two different locks they cannot open because if both groups cannot open the same lock, there is a group of the six scientists among these two groups who will not be able to open the cabinet. Thus atleast $\binom{11}{5} = 462$ locks are needed. As to the number of keys each scientist must carry, let A be one of the scientists. Whenever A is associated with a group of five other scientists, A should have the key to the locks that these five scientist were not able to open. Thus A carries at least $\binom{10}{5} = 252$ keys. These numbers are clearly impractical and they become exponentially worse when the number of scientists increases.

Let's consider another example. In a bank, there is a vault which must be opened everyday. The bank employs three seniors tellers but they do not trust any one teller completely. To solve this problem, we would like to design a system whereby any two of the senior tellers can gain access to the vault but one teller can not do so. The problem can be solved by means of a secret sharing scheme described below.

Secret sharing scheme is a method by which a group of people reconstruct a secret S, using each of their allocated shares. The secret S can be recovered only when a sufficient number of people, each with their own share, work together. The individual shares are of no use to anyone. Such schemes are highly useful in daily life purposes such as in number bank tellers mentioned above. Other places where it is widely used include missile launch codes [12], encryption keys, e-voting, multiparty computation, etc.

In the latter part of the thesis, we show how secret sharing schemes are useful in constructing an e-voting scheme. An e-voting scheme is a method by which a voter votes in an election using the internet. Different e-voting schemes can be constructed according to the countries' requirements. We will discuss about constructing an e-voting scheme using secret sharing schemes that safeguards privacy of votes.

The concept of verifying and counting votes using e-voting schemes through cryptographic solutions has introduced transparency and trust in electronic voting system. It allows voters and election workers to verify that votes have been recorded and placed correctly.

E-voting is presently used in various countries, for example Switerland, Netherland, France, Finland, Estonia, Canada. In April 2011, Gujrat became the first Indian state to experiment with e-voting.

The shares in secret sharing scheme must be confidential as their exposure can lead to knowledge of the secret S. The secret S should be kept in one location for maximum privacy, but doing so can be very difficult, as once if it is lost, it cannot be recovered. So multiple copies of the secret S are needed to keep in different locations for better reliability. This lowers confidentiality because of more opportunities for a copy to fall into the hands of unauthorized people.

Secret sharing schemes enable us to address such problems by allowing high levels of confidentiality and reliability. Here we present different types of secret sharing schemes. Let us define some terms and notations used in such schemes in the next chapter.

Chapter 2

Terms and definitions

Term 2.0.1. (Threshold scheme) Let (k, n) be positive integers and $k \leq n$. A (k, n) *threshold scheme* is a method of sharing a secret S among n shareholders in such a way that any subset of k shareholders out of n shareholders can compute the secret S. However, any subset of stricly less than k shareholders cannot construct the secret S.

Definition 2.0.1. (Perfect scheme) A threshold scheme is perfect if any $(k-1)$ or fewer than $(k-1)$ shareholders who work together with their corresponding shares cannot get any information about the secret.

Definition 2.0.2. (Secret sharing schemes) A secret sharing scheme is a method of dividing a secret S in n equal parts of information as shares $P_i = (x_i, y_i), i = 1, \cdots, n$ such that any k (k is threshold) or more than k out of n shares can reconstruct the secret S and no $k-1$ or less than $k-1$ shares can do so. In other words, this is a threshold scheme where the secret S can be recovered if only k or more than k parts of secret information is known. It is impossible for any other situation to reconstruct or get any information about the secret S. Hence secret sharing threshold scheme is perfect.

In 1979, Shamir [9] constructed a (k, n) threshold secret sharing scheme. In his construction, a dealer D construct a random polynomial $f(x) = a_0 + a_1 + \cdots + a_{k-1}x^{k-1}$ of degree *k-1* with constant term as $a_0 = S$, where S is a secret and a_i's are random coefficients, $i = 1$ to $k-1$ in a finite field $\mathbb{Z}_p$, where p is a prime. Dealer D chooses n random points (x_i, y_i), where $n < p$ in $\mathbb{Z}_p$ satisfying the constructed polynomial. Then D distributes the (x_i, y_i) as shares to n number of shareholders P_i. The points

$x_i's$ are publicly known whereas $y_i's$ are private. By using Langrange interpolation, any subset of $k < n$ shareholders P_{i_k} with shares (x_{i_k}, y_{i_k}) can reconstruct the secret S.

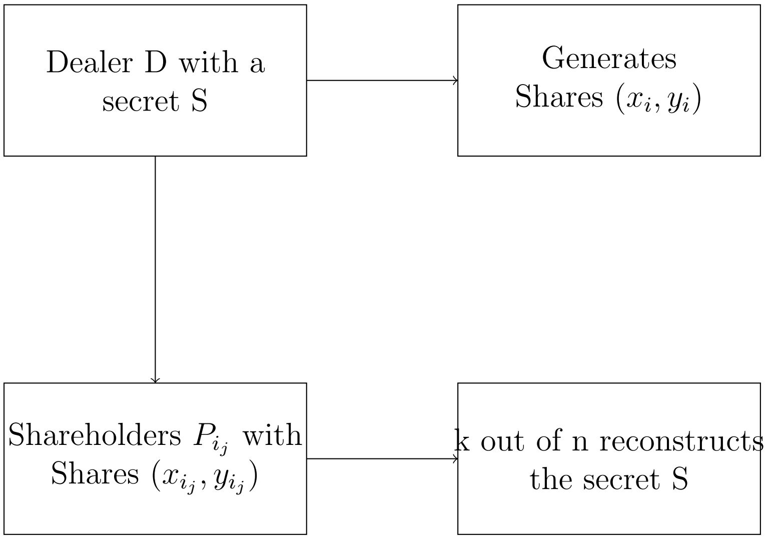
Dealer D with a secret S
Generates Shares (x_i, y_i)
Shareholders P_{i_j} with Shares (x_{i_j}, y_{i_j})
k out of n reconstructs the secret S

Figure 2.1: A schematic way of (k, n) Shamir's threshold secret sharing scheme

For finding the secret S using the secret sharing scheme, we must find the polynomial $f(x)$. Langrange interpolation is a basic way to find a $(k-1)$ degree polynomial that passes through given k points. We now recall how interpolating k points results in a unique $k-1$ degree polynomial.

Theorem 2.0.1. (Lagrange interpolation formula [11, page 404]) Suppose p is prime, $(x_0, \ldots, x_k)$ are distinct elements in finite field $\mathbb{Z}_p$, and $(y_0, \ldots, y_k)$ not necessarily distinct elements in $\mathbb{Z}_p$. Then there is a unique polynomial $f(x) \in \mathbb{Z}_p[x]$ having degree at most k, such that $f(x_i) = y_i, 0 \leq i \leq k$. The polynomial $f(x)$ is as follows:

$$f(x) = \textstyle\sum_{i=0}^{k} y_i \prod_{0 \leq j \leq k, i \neq j} \frac{x - x_j}{x_i - x_j}$$

Proof. `1.Existence:` Denote the lagrange interpolation polynomial

$$f(x) = \textstyle\sum_{i=0}^{k} y_i l_i(x), l_i(x) = \prod_{0 \leq j \leq k, i \neq j} \frac{x - x_j}{x_i - x_j}$$

The polynomial $f(x)$ with degree $\leq k$ satisfies $f(x_i) = y_i, i = 0, \cdots, k$ since $l_i(x_j) = 0$ if $i \neq j$ and $l_i(x_j) = 1$ if $i = j$.

`2.Uniqueness:` Suppose $q(x)$ is another polynomial of degree $\leq k$, satisfying

$$q(x_i) = y_i, i = 0, 1, \cdots, k$$

Define $r(x) = f(x) - q(x)$, then degree of $r(x) \leq k$ and

$$r(x_i) = f(x_i) - q(x_i) = 0, i = 0, 1, \cdots, k$$

Since $r(x)$ has $k + 1$ zero, we must have $r(x) \equiv 0$. Thus $f(x) = q(x)$. This completes the proof of the theorem. □

Example: We Wish to find a polynomial interpolating the points given in the table below:

x	2	4	5
y	1494	1942	4414

First we find the polynomials $f_i(x)$, $i = 0, 1, 2$ where
$f_i(x) = \prod_{0 \leq j \leq k-1, i \neq j} \frac{x - x_j}{x_i - x_j}$
Solving $f_i(x)$, $i = 0, 1, 2$,
$f_0(x) = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x^2}{6} - \frac{3x}{2} + \frac{10}{3}$
$f_1(x) = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{-x^2}{2} + \frac{7x}{2} - \frac{5}{1}$
$f_2(x) = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x^2}{3} - \frac{2x}{1} + \frac{8}{3}$
And thus, using the Langrange interpolation we find
$f(x) = \sum_{i=0}^{2} y_i \cdot f_i(x)$
$f(x) = 1234 + 166x + 94x^2$

Now let us talk about a real situation where secret sharing threshold schemes are applied. A person Amit keeps some amount of money in a bank with a number lock. The lock can be opened only when the correct key is provided. Let this key be the secret S. Since Amit doesn't trust any one of the n persons in charge of the lock fully, he wants to distribute an equal amount of information about the secret S to them such that any 3 can reconstruct S and no less that 3 can do so. How would he construct and distribute his shares to the n people? How is the (k, n) secret sharing scheme applied here?

The shares $P_i = (x_i, y_i)$ by Amit are constructed as follows. He takes a quadratic polynomial $f(x) = a_0 + a_1x + a_2x^2$ with constant term a_0, where $a_0 = S$ and a_1, a_2 are random numbers. He chooses random $x_i, i = 1, 2, 3$ and calculates coresponding $y_i, = 1, 2, 3$ by substituating x_i in $f(x)$. Thus the shares $P_i = (x_i, y_i)$ are obtained.

Knowing any 3 shares $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, the polynomial $f(x)$ is determined using Guassian elimination or Langrange interpolation and thus the secret $S = a_0$.

Definition 2.0.3. (Multilevel secret sharing scheme) The multilevel secret sharing scheme is the scheme where multiple levels are required to find the secret S. Different levels $L_i, i = 1, m$ are first formed by forming a partition of n shareholders based on their designation and a threshold $k_i, 1 \leq k_i \leq |L_1| + |L_2| + \cdots + |L_i|, 1 \leq i \leq m$ is fixed where $|L_i|$ represents the number of shareholders at level L_i. The thresholds $k_i, i = 1, \cdots, m$ are choosen as $k_1 \leq k_2 \cdots \leq k_m$. Here L_1 is the highest level and L_m is the lowest level. Higher levels get more access to reconstruct the secret S than lower levels. Each level L_i, requires k_i number of shareholders out of n_i people to reconstruct the secret S. Here n_i stands for the total number of share holders from L_1 to L_i, so $n = n_m$. Thus k_i shareholders at level L_i can reconstruct the secret S. We see that the number of shareholders required at a higher level is less than the number of shareholders required at a lower level for the threshold scheme. Since the secret S at each level L_i is determined using the secret sharing threshold scheme, the multilevel threshold scheme is also perfect.

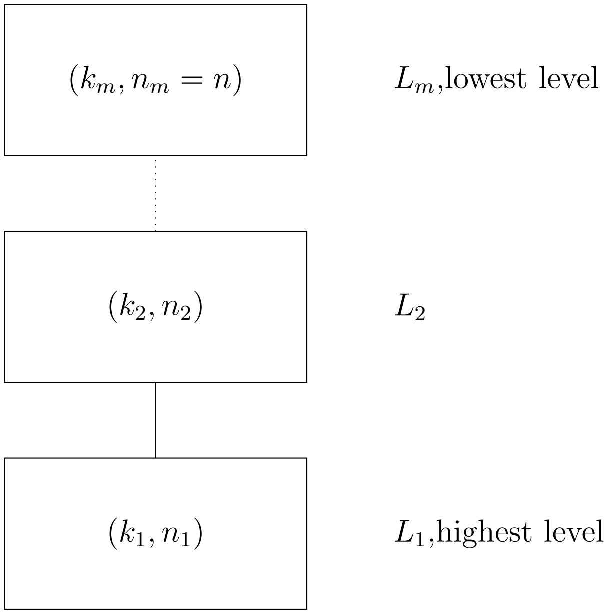

Figure 2.2: A schematic outline of (k, n) multilevel threshold secret sharing schemes

Consider a situation in a bank where a number lock can be unlocked by two senior-most employees. In the absence of any one senior-most employee, a certain number of junior employees are needed to access the secret S. Let us assume L_1 comprises 2 senior employees and L_2 comprises 4 junior employees. We fix $k_1 = 2$ and $k_2 = 3$ i.e. when any 2 senior employees, any 3 junior employees or in the absence of anyone senior employee, 2 junior employee and 1 senior employee collude their shares together, they are able to reconstruct the secret S. This type of situation requires the multilevel secret sharing scheme.

Changlu [6] considered the distribution of shares in multilevel secret sharing scheme as follows:

- For level $1, L_1$-Choose any degree one polynomial $g(x) = a_0 + a_1x$. Take any 2 random points x_1, x_2 and generate shares $(x_1, y_1), (x_2, y_2)$, where $g(x_i) = y_i, i = 1, 2$. Using the basic secret sharing scheme, the secret $S = a_0$ can be determined.

- For level $2, L_2$-Choose a polynomial $g'(x)$ with the same coefficient a_0 passing through the shares $(x_1, y_1), (x_2, y_2)$ of L_1. The constructed multilevel scheme requires the lower level L_2 to have more shares than those of L_1 and the points of L_1 should also satisfy $g'(x)$. The polynomial $g'(x)$ must pass through at least 2 or more points different from the shares in L_1 and also through the shares of $L_1, (x_1, y_1), (x_2, y_2)$. So at least 5 points are needed to determine $g'(x)$. The minimum possible degree of $g'(x)$ is $2 + 2 + 1 - 1 = 4$. Again, using the basic secret sharing scheme, the shares are constructed in L_2 and the secret S can be determined.

- In the absence of one person in level $L_1, 4$ shares of L_2 and 1 share of L_1 are used to determine $g'(x)$, which results in the secret S.

Another way to construct a multilevel secret sharing scheme is to think about lines and planes.

- For L_1, a line l_i can be determined and intersection of l_i with a given public line l_d will give the point s which is the secret S.

- For L_2, a plane v_i which contains the line l_i can be determined using 3 non collinear points and thus the intersection of v_i with l_d gives the secret S.

Definition 2.0.4. (Compartment Secret sharing scheme) The compartment secret sharing scheme is a method of distributing shares of the secret S into a different compartment such that when a certain number of shares from every compartment comes together, the secret S is reconstructed. In other words, for any action to be taken, approval from each compartment is necessary.

Assume that there is some treaty controlled action that requires the approval of two countries, say U.S.A. and Russia, for its initiation [10]. Each country has a team of its own representatives at the site and requires that at least two of their controllers must consent before their national input to the shared control scheme is decided. In the present case, even if all n of the Americans and one of the Russians agree, the controlled action is to be inhibited.

This situation can be solved by constructing a compartment threshold secret sharing scheme. Two members from each country can use their shares to determine the lines l_1, l_2. The intersection of these two lines will give the secret S.

Definition 2.0.5. (Information rate): Information rate of a secret sharing scheme is the ratio between the length, in bits, of the secret and the maximal length of shares distributed to shareholders. Let a be the number of bits of the secret and $b = max(b_1, \cdots, b_n)$ be the number of bits of the maximal share. The information rate is then defined as

$$\mathtt{I} = \tfrac{a}{b}$$

Definition 2.0.6. (Ideal) : The secret sharing scheme is called ideal if the maximal length of shares and the length of the secret are identical, i.e., the information rate $\mathtt{I}$=1.

Definition 2.0.7. (Skew lines) : Skew lines l_1, l_2 are two lines that do not intersect and are not parallel. In other words, they are a pair of lines which neither lie in the same plane nor intersect each other. A simple example of a pair of skew lines is the pair of lines through opposite edges of a regular tetrahedron [12].

Theorem 2.0.2. The space spanned by $\langle l_1, l_2 \rangle$ is a 3 dimensional subspace.

Proof. Lets define $l_1 = a_0 + tb_0$ and $l_2 = m_0 + sn_0$. Take l' to be a linear combination of $l_1, l2$.

$$l' = l(a_0) + (1 - l)(m_0) + tb_0 + sn_0 \; l' = m_0 + l(a_0 - m_0) + tb_0 + sn_0$$

We see that, to determine l' we need four variables. Hence the dimension of l' is 3. □

Theorem 2.0.3 (Simmons [10])**.** In $\mathbb{Q}^n, n > 3$, there is a unique line incident with each pair of skew line and with an $(n-3)$-dimensional subspace independent of each of these lines.

Proof. In $\mathbb{Q}^3$, there is a unique line passing through a given point s and intersecting each of the skew lines l_1 and l_2 neither of which pass through s. To see this, note that s and l_1 determine a plane α. The line l_2 intersects α at a point q, where $q \neq s$ and by construction l_2 does not pass through s. The line $w = \langle s, q \rangle$ is in α, as is the line l_1. So they intersect in a point r. Hence w is the unique line lying on s, intersecting l_1, l_2 at r, q. Now consider any space $\mathbb{Q}^n, n > 4$. Let l_1 and l_2 be a pair of skew lines in $\mathbb{Q}^n$. The lines l_1 and l_2 span a 3 dimensional subspace S of $\mathbb{Q}^n$. Given an arbitrary $(n-3)$- dimensional subspace T of $\mathbb{Q}^n$ independent of S, T intersects S in a single point s by rank theorem. Let this point s be the point in above construction. We have therefore proven that in $\mathbb{Q}^n, n > 3$, there is a unique line incident with each pair of skew lines and with an $(n-3)$-dimensional subspace independent of each of these lines. □

Definition 2.0.8. A hyperplane H is a $n-1$ dimensional subspace in n dimensional space. It is given by the following equation:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

The $n-1$ dimensional hyperplane is uniquely determined by $n-1$ points.

When we take a translation of the above hyperplane by a constant c, it is called as an affine hyperplane and is given by equation [12]:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

In a n-dimensional space, an affine hyperplane is uniquely defined by n points.

Chapter 3

Affine and projective space

An affine space $\mathbb{A}^n$ over a field k is a set whose elements are called points and set of subset are called lines, satisfying following axioms [2, chapter1]:

1. Given two distinct point P and Q, there is one and only one line containing both P and Q.
2. Given a line l and a point P, not on l there is one and only one line m which is parallel to l and which passes through P.
3. There exist three non collinear points.

In simple terms, the affine space $\mathbb{A}^n$ over the field k is the set of n tuples, $(x_1, x_2, \cdots, x_n) \in k$. These elements are called points and staisfies the above axioms. An Euclidean plane $\mathbb{R}^2$ consists of points (x_1, x_2) is an example of an affine space.

Equation of a line in euclidean plane $\mathbb{R}^2$ over k is given by

$$x_2 = mx_1 + c$$

The affine space deals with the intersection of lines and other higher dimension curves. It doesn't provides any information about points at infinity or lines meeting at infinity. To solve such difficulties we study the projective plane which deals with the intersection of lines at infinity. If we add all the points at infinity to affine space, we get projective space. For each line l in affine space, will denote by $[l]$ the pencil of lines parallel to l and we call $[l]$ an ideal point or point at infinity P^* in the direction of l.

A projective space $\mathbb{P}^n$ over a field k is a set, whose elements are point and a set of subset satisfying the following axioms [2]:

1. Two distinct points of S lie on one and only one line.
2. Any two lines meet atleast at one point.
3. There exist three non collinear points.
4. Every line conatins at least three points.

Real projective plane $\mathbb{P}^2$ over $\mathbb{R}$ is an example of a projective space. It is a collection of triples $x = (x_1, x_2, x_3)$ of real numbers $\mathbb{R}$. Two triples $x = (x_1, x_2, x_3)$ and $x' = (x'_1, x'_2, x'_3)$ represents same point in $\mathbb{R}^2$ if $x' = ax$, $a \in \mathbb{R}^2, a \neq 0$. The point $(x_1, x_2, 1)$ determines a line in $\mathbb{R}^3$ that passes through $(0, 0, 0)$ and $(x_1, x_2, 1)$. Every line through $(0, 0, 0)$ except those lying in the plane $x_3 = 0$ corresponds to exactly one point $(x_1, x_2) \in \mathbb{R}^2$. The lines through $(0, 0, 0)$ in the plane $x_3 = 0$ corresponds to point at infinity.

Equation of a line in $\mathbb{P}^2$ over $\mathbb{R}$ is given by [1]:

$$a_1x_1 + a_2x_2 + a_3x_3 = 0$$

In other words, projective n space over a finite field k written as $\mathrm{PG}(n, k)$ or $\mathbb{P}^n(k)$ is defined to be set of all lines passing through $(0, 0, \cdots, 0) \in \mathbb{R}^{n+1}(k)$. Any point $x = (x_1, x_2, \cdots, x_{n+1}) \neq (0, 0, \cdots, 0)$ determines a unique such line namely $\{(ax_1, ax_2, \cdots, ax_n), a \in k\}$. Two such points (x) and (y) determines the same line if there exist a non zero $a \in q$ such that $y_i = ax_i$ for $i = 1, \cdots, n+1$. Then the line (x), (y) are equivalent. The projective space $\mathbb{P}^n(k)$, may be identified with the set of equivalance classes of points in $\mathbb{R}^{n+1}(k)(0, 0, \cdots, 0)$. We say that $(x_1, x_2, \cdots, x_{n+1})$ are homogeneous coordinates for point $P \in \mathbb{P}^n(k)$. We indicate P as $[x_1 : \cdots : x_{n+1}]$. If x_i coordinate is non zero then x_j/x_i are well defined.

We let $\mathbb{U}_i = \{[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^n | x_i \neq 0\}$. Each $P \in \mathbb{U}_i$ can be written uniquely in the form [4, chapter1]

$$P = [x_1 : \cdots : x_{i-1} : 1 : x_{i+1} : \cdots : x_{n+1}]$$

The coordinates $(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{n+1})$ are called the non homogeneous coordinates for point p with respect to $\mathbb{U}_i$. We define hyperplane at infinity by:

$$\mathbb{H}_\infty = \{[x_1 : \cdots : x_{n+1}] | x_{n+1} = 0\}.$$

The hyperplane at infinity can be identified with $\mathbb{P}^{n-1}$. Thus $\mathbb{P}^n = \mathbb{U}_{n+1} \cup \mathbb{H}_\infty$. For examples [4]:

1. The projective plane $\mathbb{P}^2$. Here $\mathbb{H}_\infty$ is called line at infinity.

2. Point (x, y) on a line $Y = mx + b \in \mathbb{R}^2$ correspond to the points $[x : y : z] \in \mathbb{P}^2$ with $y = mx+bz$, a homogeneous equation, so that the solution will be invariant under equivalence. The set $\{[x : y : z] \in \mathbb{P}^2 | y = mx + bz\} \cap \mathbb{H}_\infty = \{[1 : m : 0]\}$. So all lines with the same slope, when extended in this way, pass through the same point at infinity.

3. Consider again the curve $Y^2 = X^2 + 1$. The corresponding set in $\mathbb{P}^2$ is given by the homogeneous equation $Y^2 = X^2+Z^2, Z \neq 0$. $\{[x : y : z] \in \mathbb{P}^2 \mid y^2 = x^2+z^2\}$ intersects $\mathbb{H}_\infty$ in the two points $[1 : 1 : 0]$ and $[1 : -1 : 0]$. These are the points where the lines $Y = X$ and $Y = -X$ intersect the curve.

3.1 Algebraic and projective sets

The exposition in this section is from Fulton [4, Chapter 4]. For any ring R, let $R[X]$ denotes the ring of polynomials in the variable X with coefficient in R. Then the ring of polynomials in n variables over R is written as $R[X_1, X_2, \cdots, X_n]$. The monomials in $R[X_1, \cdots, X_n]$ are the polynomials $X_1^{i_1} \cdots X_n^{i_n}$, where i_j non negative integer $i, j = 1, \cdots, n$ and the degree of monomials is $i_1 + \cdots + i_n$. Every $F \in R[X_1, \cdots, X_n]$ has a unique expression $F = \sum a_i X^i$, where X^i is the monomials and $a_i \in R$. We call F homogeneous or a form of degree d if all the coefficients a_i are zero except for the monomials of degree d. Any polynomial F has a unique expression $F = F_0 + \cdots + F_d$ where F_i is a form of degree i. The degree of F is the largest d such that $F_d \neq 0$. The terms $F_0, F_1, \cdots$ are called the constant, linear,$\cdots$ terms of F. F is constant if $F = F_0$.

If $F \in k[X_1, \cdots, X_n]$, a point $P = (a_1, \cdots, a_n) \in \mathbb{A}^n(k)$ is called a zero of F if $F(P) = 0$. If F is not constant, the set of zeros of F is called hypersurface defined by F and is denoted by $V(F)$.

A hypersurface in $\mathbb{A}^2(k)$ is called an affine plane curve. If F is a polynomial of degree one, $V(F)$ is called a hyperplane in $\mathbb{A}^n(k)$ and if n=2 it is a line.

For a set S of polynomial in $k[X_1, \cdots, X_{n+1}]$, we let

$$V(S) = \{P \in \mathbb{P}^n \mid P \text{ is a zero of each } F \in S\}$$

Such a set is called an algebraic set in $\mathbb{P}^n$ or a projective algebraic set [4, chapter4].

For any set $X \in \mathbb{P}^n$, we let

$$I(X) = \{F \in k[X_1, \cdots, X_{n+1}] | \text{ every } P \in X \text{ is a zero of F } \}.$$

The ideal $I(X)$ is called the ideal of X.

An ideal $I \subset k[X_1, \cdots, X_{n+1}]$ is called homogeneous if for every $F = \sum_i^m F_i \in I$, where F_i is a form of degree i, we have also $F_i \in I$. For any set $X \subset \mathbb{P}^n, I(X)$ is a homogeneous ideal.

An algebraic set $V \subset \mathbb{P}^n$ is irreducible if it is not a union of two smaller algebraic sets. The algebraic set V is irreducible if and only if $I(V)$ is prime. An irreducible algebraic set in $\mathbb{P}^n$ is called a projective variety. Any projective algebraic set can be written uniquely as a union of projective varieties, its irreducible components.

We will see how these varieties are used in constructing secret sharing schemes, in the next chapter.

Chapter 4

A construction of secret schemes using projective varieties

The (k, n) threshold secret sharing scheme can be geometrically constructed using projective varieties. Consider a projective plane $\mathbb{P}^2$ over q. We can construct $(2, n)$ threshold scheme by taking two lines l_i and $l_d \in \mathbb{P}^2(q)$. Any n shares $(x_1, y_1), \cdots, (x_n, y_n)$ of shareholder are chosen as points on l_i. The secret S is the intersection of the line l_i with a publicly known line, l_d. When any 2 shareholders collude their shares together, they are able to reconstruct the line l_i and thus the intersection point S of l_i with l_d. The secret S is a 1-dimensional uncertainty, a point S on line l_i, excluding the n points which are given as shares. The projective plane $\mathrm{PG}(2, q)$ ensures that the two lines meet exactly at a point. The point of intersection of l_i with l_d is the secret S in this example.

What if a point r_i on l_i is already known? Is there a possibility of guessing the point S?

For every choice of r_d on l_d there exists a line $\langle r_i, r_d \rangle$ which is equally probable to the line l_i. Thus, everyone point on l_d is equally likely to be the secret S irrespective of knowing one private piece or no information about private piece. The probability of getting the point S is $1/(q + 1)$.

Since the points on line l_i are taken to be shares, the number of shareholders could be as great as q except the point S, i.e. any point on l_i is available to use as a share except the point S.

The secret S can be point S itself or a function f on S. We assume f conserves

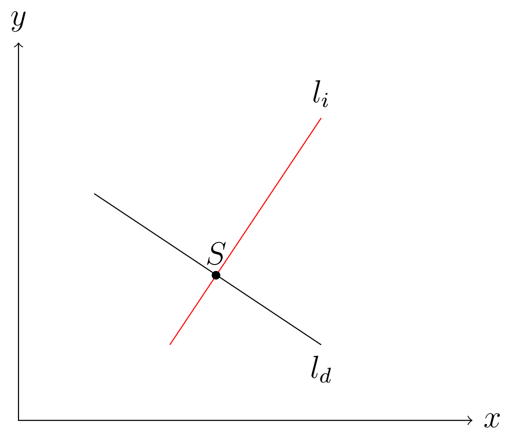

Figure 4.1: A geometrical representation of $(2, n)$ threshold secret sharing scheme

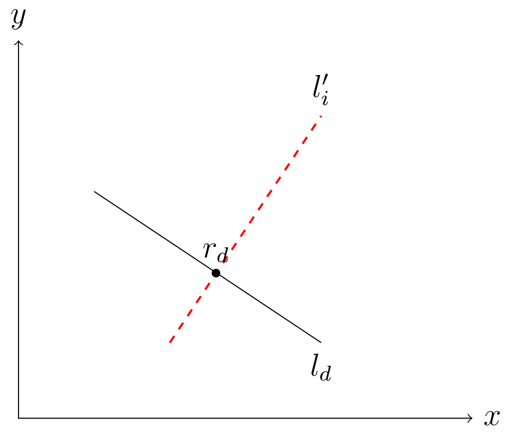

Figure 4.2: A representation showing any point on l_d is equally probable to be S

entropy i.e. the uncertainty about $f(S)$ is same as uncertainty about S.

The above example can be replaced by a more general type of geometric object, a projective variety. The (k, n) threshold secret sharing scheme using varieties was first constructed by Simmon [10]. For constructing a (k, n) threshold scheme, we replace l_i and l_d in the above example by a domain variety V_d and an indicator variety V_i in n dimensional subspace. A point S is taken in domain variety V_d. The shares are the points in V_i, whose function is to point to index S in V_d. In other words, the intersection of V_i and V_d is the unique point S.
Note: Here, variety V_i is referred to as indicator variety as it indicates a specific item, in this case, pointing to the secret S. The point S is called as index.

The (k, n) threshold secret sharing scheme looks like the following pictorially.

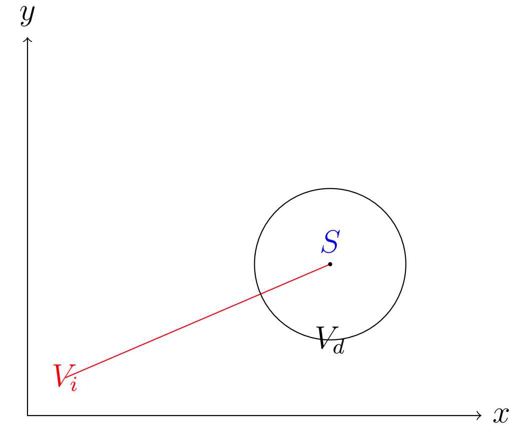

Figure 4.3: A geometrical representation of (k, n) threshold secret sharing schemes

For the scheme to be perfect, no less than k out of n number of people should be able to reconstruct V_i and hence the index S. So similar to $(2, n)$ threshold secret sharing scheme, in this construction every point on V_d is equally likely to be the point S.

A $(3, k)$ threshold scheme can be pictorially shown as in figure 4.4.

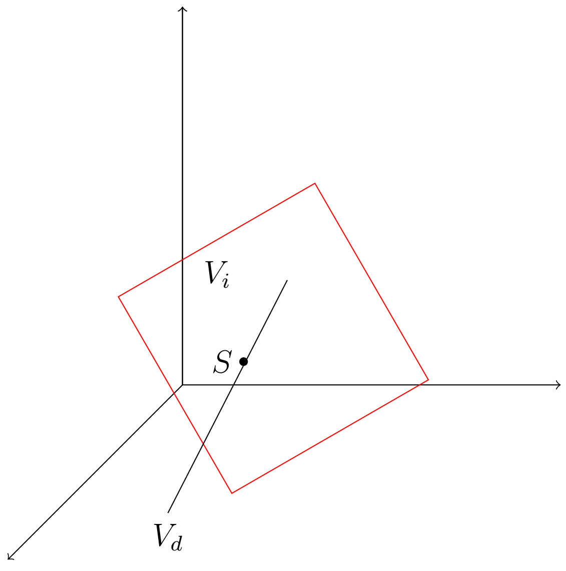

Figure 4.4: A representation of $(3, n)$ threshold secret sharing scheme with a 2 dimensional secret

Here the secret S is 2 dimensional uncertainity. We can make the index S in $(3, n)$ threshold secret sharing scheme, a 1 dimension unknown as shown in figure 4.5.

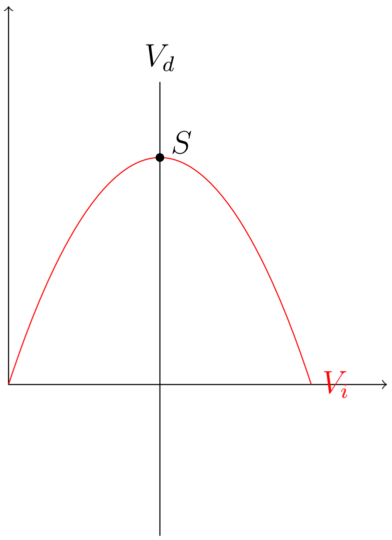

Figure 4.5: A representation of $(3, n)$ threshold secret sharing scheme with a 1 dimensional secret

In this case the probability of guessing secret is more compared to the constructed scheme where secret was 2-dimensional uncertainty. It is better to construct a secret sharing scheme where the secret S has a large dimension n, so that any outsider has less probability to guess the correct secret S. So we try to construct a secret sharing scheme where the dimension of the index S is large.

4.0.1 Construction of (4,n) threshold secret sharing scheme using affine hyperplane H:

Step 1. We choose a random affine hyperplane H, given by:

$$\text{H}= 2X_1 + 3X_2 + X_3 - X_4 = 1$$

over a finite field, Z_{11} and a secret $P = (1, 1, 1, 5) \in$ H.

Step 2. Now we take a point $Q = (2, 3, 2, -1)$ which does not belong to H and find the line l_d passing through P and Q.

$$y_1 = 1 + 1t$$
$$y_2 = 1 + 2t$$
$$y_3 = 1 + t$$
$$y_4 = -5 - 6t$$

We put any arbitary $t, t \neq 0, 1$ and find a point R on l_d. Let us take $t = 2$ and so, the point R on l_d is given by $y_1' = 3, y_2' = 5, y_3' = 3, y_4' = -7$. Now we rewrite the equation of line l_d using points Q and R.

$$y_1 = 3 - t'$$
$$y_2 = 5 - 2t'$$
$$y_3 = 3 - t'$$
$$y_4 = -7 + 6t'$$

The above line l_d is the domain variety V_d which is public known to everyone, in this example.

Step 3. We then distribute n points $P_1, \cdots, P_n \in$ H as shares to n shareholders without disclosing any information about the equation of hyperplane H. Any four of these points should determine the hyperplane H and thus its intersection with l_d will reveal the secret P.

For example, if H is not known and is given by H$\equiv aX_1 + bX_2 + cX_3 + dX_4 = e$, where a, b, c, d, e are unknown coefficients and the points satisfying the equation of H are given by $(1, 1, 3, 7), (2, 2, 1, 10), (2, 1, 5, 0), (1, 2, 2, 9)$ as shares, then we get the following system of linear equations:

$$a + b + c + 7d = e$$
$$2a + 2b + c + 10d = e$$
$$2a + b + 5c = e$$
$$a + 2b + 2c + 9d = e$$

By solving the above linear system of equations, we will get the values of a, b, c, d in terms of e as.

$$a = 2e$$
$$b = 3e$$
$$c = e$$
$$d = -e$$

Substituting equation of line l_d in H, we get the value of t' and thus the secret S i.e. point P.

$$2(y_1) + 3(y_2) + (y_3) - (y_4) - 1 = 0$$
$$2(3 - t') + 3(5 - 2t') + (3 - t') - 1(-7 + 6t') - 1 = 0$$
$$t' = 2$$

Hence, $y''_1 = 1, y''_2 = 1, y''_3 = 1, y''_4 = 5$ which is the point $P =$ secret S.

4.1 Construction of multilevel secret schemes

Consider the electronic funds transfer problem. Electronic funds transfer is used by the banking industry to exchange account information over secured networks. We consider a person who wants to transfer money from his account to another account. To do so, he must enter his password. The password acts as a secret key here. If some other person is able to find the password he will be able to break in. So in this process the password is the secret S and the share of password is distributed to different individuals depending upon their designation. We assume that the password can be found, if any 2 presidents or 3 senior tellers collude their shares. We take domain variety V_d to be a line. The shares of senior tellers determine a plane V_2, which intersects V_d at S. The shares of presidents determine a line V_1 which intersects V_d at S.

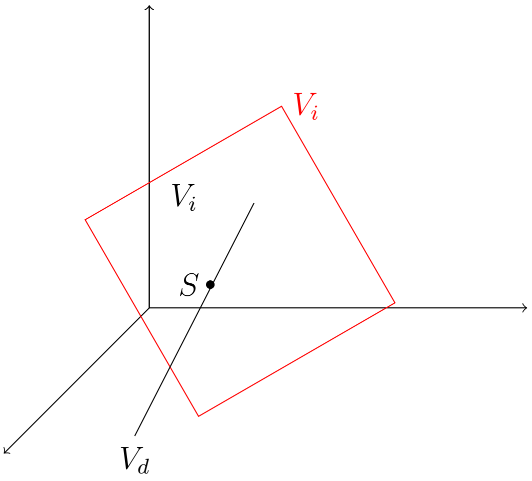

Figure 4.6: A geometrical construction of a multilevel secret sharing scheme

Knowing one point on V_1 or two points on V_2 leaves V_1 and V_2 undetermined, hence the point of intersection S with V_d. Thus, this scheme is perfect.

To think about the case when any 2 senior tellers and 1 president can find the secret in the absence of other president, we construct another way of multilevel secret sharing scheme. We take V_d as a plane. The intersection of plane V_2 and V_d is point S. We take V_1 to be line lying on V_2 and intersecting V_d at S. In the absence of other point on V_1, the two other points of V_2 can be taken to determine V_2, which results in finding S. Thus the combination of 1 president and 2 senior tellers are able to find the secret S.

Knowing only a point on V_1 or two points on V_2 leaves the point S totally undetermined. Hence this scheme is also perfect.

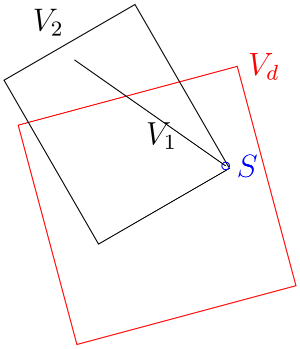

Figure 4.7: A different representation of constructing multilevel secret sharing scheme

4.2 Construction of compartment secret schemes

There are two approaches to construct the (k, n) compartment secret sharing schemes.

The first approach is to construct the indicator variety V_i as the union of subvarieties $V'_{i'}, i' = 1, k$. The subvariety V'_j is a $k_j - 1$ dimensional subspace and is determined by k_j out of n_j people from jth team. Thus V_i is constructed when all k teams determine their subvarieties and collude together. Domain variety V_d as usual is a variety in a space, where every point is equally probable to be index S. The intersection of domain variety V_d and indicator variety V_i is the secret S.

Consider a $(2, n)$ compartment threshold secret sharing scheme. Here 2 out of n_1 from first team determines the first variety V'_1 and 2 out of n_2 determine the second variety V'_2. The V_i is determined as $V'_1 \cup V'_2$. The domain variety V_d is determined by some polynomial constraint. The index S is the point satisfying all the polynomial constraint of V_i and V_d. Pictorially it looks like:

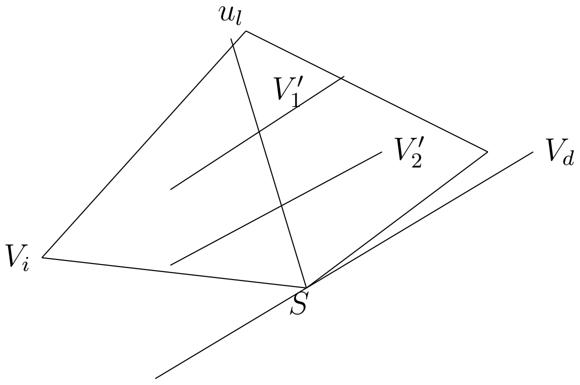

Figure 4.8: Two skew lines spanning a 3 dimensional space and intersecting V_d at s

By theorem 2.2 we deduce that the subvarieties V_1' and V_2' span a 3 dimensional space V_i. The intersection of V_i with V_d is the secret S. We see in this case that there exists a unique line u_l intersecting V_1', V_2' and V_d at r_1, r_2, S respectively.

The most threatening form of cheating in this case would be when 2 out of n_1 and 1 out of n_2 collude their shares together. With no loss of generality, assume that the subvariety V_1' and a point $x \neq r_2$ on V_2' are all accessible to a person. To prove that this scheme is perfect we need to show that every point on V_d is still equally like to be the point S. We assume that the geometrical construction is known to both outsider and insider i.e. to all cheaters.

Choose u on domain variety V_d. If u is the secret, then the person knows that it should be collinear to a point on V_1' and a point on V_2'. Let w be an arbitrary point on V_1'. Take line w^* which intersects V_1' at w and V_d at u. If u is the secret, then $V_2' \cap \langle V_1', V_d \rangle = r_2$. Therefore, for each point z on $w*$, $z \neq u, w$ a line $V_2'' = \langle x, z \rangle$ is determined which is independent of $\langle V_1', V_d \rangle$ and for which

$$V_2'' \cap \langle V_1', V_d \rangle = z$$

Thus, if $V_2' = V_2''$, then one can conclude that in the constructed scheme point u is the secret. It is possible only if the line V_2' is already known, so the constructed scheme is perfect.

Another approach for constructing a compartment secret sharing scheme is to consider the points of intersection p_1, p_2 of V_1', V_2' with V_d as input for a perfect $(2, 2)$ scheme defined on V_d. Then S is determined. This is a two part scheme.

Consider the case when V_1' and a point from V_2' say $x \neq p_2$ is known to inside and outside cheaters. Our task is to show that the scheme is perfect. Knowledge of point

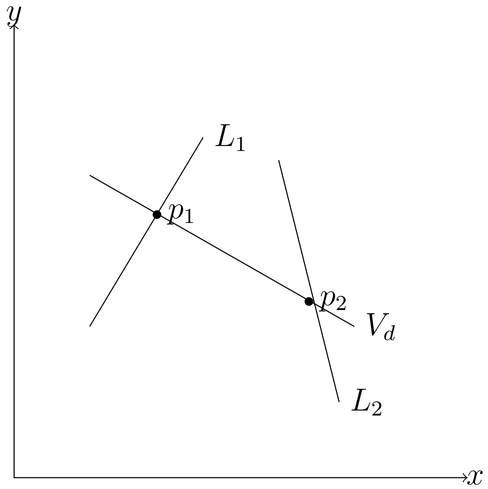

Figure 4.9: A geometrical representation of a compartment secret sharing scheme

x on V_2' gives q many possible lines intersecting V_d, out of which one line is V_2'. Since V_2' is equally probable as any other line, every point on V_d is equally probable to be the point S.

Note: A perfect $(2, 2)$ threshold secret sharing scheme is constructed as:

1. The dealer gives a random point, say p_1, to one of the shareholders.
2. The second point p_2 is calculated as a vector sum of p_1 and secret datum S. The point $p_2 = S - p_1$
3. Clearly when both points p_1, p_2 are added together, it results in the secret S.

It can be extended to a perfect (k, k) threshold secret sharing scheme. The $k - 1$ random points are chosen as shares and the kth share is calculated as the vector sum of $k - 1$ shares and the secret S. Thus the addition of k shares together results in secret S. The drawback of this scheme is that the kth share is dependent on the $k - 1$ shares.

Chapter 5

Shamir's secret sharing scheme using algebraic variety

In Shamir's secret sharing scheme, we take domain variety V_d to be y axis and the indictar variety V_i to be a $(k-1)$ degree polynomial $f(x)$. When any k points which are zeros of $f(x)$ given as shares, are colluded together, the indicator variety V_i is determined and thus the intersection of V_i with V_d, which gives us the secret S.

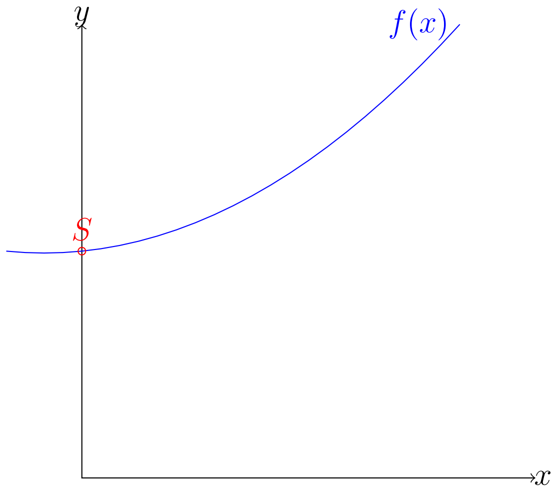

Figure 5.1: A geometrical representation of Shamir's secret sharing scheme

Here is a small example to illustrate.

Suppose $p = 17$ and there are five people. Any three of them are required to recover the secret S, i.e., a $(3, 5)$ secret sharing threshold scheme. Each of them have a public x-coordinate, x_i, $1 \leq$ i ≤ 5. Let's take a subset= P_1, P_3, P_5 out of five people and let their shares be $y_1 = 8, y_2 = 10$ and $y_3 = 11$. Now the polynomial $f(x) = a_0 + a_1x + a_2x^2$ can be determined by these three points if we solve the following system of linear equations.

$$\begin{aligned} a_0 + a_1 + a_2 &= 8 \\ a_0 + 3a_1 + 9a_2 &= 10 \\ a_0 + 5a_1 + 8a_2 &= 11 \end{aligned}$$

This system has a unique solution in $\mathbb{Z}_{17}; a_0 = 13, a_1 = 10$ and $a_2 = 2$. So $f(x)$ is determined as $13 + 10x + 2x^2$. The intersection of $f(x)$ with y axis is the constant term $a_0 = 13$ and hence the secret $S = 13$ is reconstructed.

It is important that the system of k linear equations has a unique solution as in the above example. Lagrange interpolation is one way of finding a unique solution polynomial $f(x)$ of degree $k-1$, for given k points which are zeros of $f(x)$.

5.1 Shamir's secret sharing algorithm

`Intialization Phase:`

1. A Dealer D chooses $k \leq p$ distinct, non zero elements in $\mathbb{Z}_p$, denoted by x_i, 0$\leq i \leq k-1, p$ is prime. For $0 \leq i \leq k-1$, D gives the value x_i to shareholder P_i. The values of x_i are public.

`Share distribution:`

1. Suppose the Dealer D wants to share a secret S in finite field $\mathbb{Z}_p$. The Dealer D secretly chooses random k elements of $\mathbb{Z}_p$,which we denote by $a_0, \cdots a_{k-1}$ and constructs $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ with $a_0 = S$.

2. For $0 \leq i \leq k-1$, D computes $y_i = f(x_i)$, where $x_i's$ are random elements in $\mathbb{Z}_p$ and

$$f(x_i) = a_0 + a_1x_i^1 + \cdots + a_{k-1}x_i^{k-1}$$

3. For $0 \leq i \leq k-1$, the dealer D gives the share y_i to the share holder P_i.

4. Any k shares should be able to determine $f(x)$ and find the secret S.

Given $k-1$ shares,what is the probability of guessing the secret S?

The number of elements in $\mathbb{Z}_p$ is p. For x coordinate there are p choices and for y coordinate there are p choices. So total number of choices $p * p = p^2$. But since the secret S belongs to $\mathbb{Z}_p$, it has p possibilities. So the probability of the secret S is:

$$P(S) = \frac{p}{p^2} = \frac{1}{p}$$

5.2 Some properties of (k, n) Shamir's threshold scheme

1. `Secure` : Suppose $k-1$ people out of n people try to collude together to find the $k-1$ degree polynomial and thus the constant $a_0 = S$. They have $k-1$ points. There are p^2 degree $k-1$ polynomial passing through these $k-1$ points and one random point in the field $\mathbb{Z}_p$. The probability of guessing the polynomial used by the dealer, D is $\frac{1}{p^2}$. If p is very large then it is difficult to get the correct polynomial. So this method makes the secret secure.

2. `Minimal` : The size of shareholders P_{i_j} does not exceed the size of secret S.

3. `Extensible` : If we keep the threshold fixed i.e. if number people who can reconstruct is fixed then we can dynamically add or delete the shares P_{i_k}'s without affecting other shares, since any k subset of P_{i_k} can reconstruct the secret S.

4. `Dyanamic` : It is easy to change all shares by taking another polynomial $f(x)$ with the same constant term. There are p many possibilities of polynomials with same constant term a_0. Changing shares with time helps in keeping the secret confidential.

5. `Flexible` : In an organization where hierarchy is important, we can supply each participant a different number of shares according to their importance inside organisations. In multilevel threshold secret sharing schemes and compartment threshold secret sharing schemes which are modifications of Shamir's secret sharing scheme, the shares are distributed to different levels, such that when a specified threshold number of people from different levels come together, the secret S is reconstructed.

Shamir's (k, n) threshold secret sharing scheme is ideal and perfect. These schemes are very secure since the only possibility for $k-1$ people to know the secret is to guess it. For example, if the secret is a function such as coordinate or norm of the coordinate of a point in some n dimensional vector space over Z_p, then by choosing p large enough we can make the system more secure. However, in real world applications, these schemes require considerably more in the way of capabilities in shared scheme than a simple (k, n) threshold for an action to be initiated. Shamir's schemes and its modified schemes are used in critical applications such as e-voting, cryptographic key distribution and sharing, secure online autions, information hiding and secure multiparty computation [12].

Chapter 6

Introduction to e-voting

An electronic voting is the system in which election data is recorded, stored and processed primarliy as digital information [5]. It can be done using various ways, for examples [12] punched cards, optical scan voting system, direct recording electronic voting system (DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, i.e., internet.

There are mainly two types of electronic voting:-

- **Electronic voting via machines located at polling stations:** In this type of voting system, a voter casts his vote using the electronic machines present at polling stations in front of the authorities who participate in counting of votes. The identity of a voter and his vote is physically supervised by these authorities. Thus the authorities might be able to know about the identity of the voter's ballot.

- **Electronic voting via internet using computer/mobile phones:** In this type of voting system, also called e-voting, a voter casts his votes using his personal computer network without any need of going to the polling stations. Voting is performed through various steps:

  1. The central authority sets up the voting scheme. It publishes all the possible voters and verifies the eligibiltiy of voters.
  2. Only eligible voters are able to make an online account by signing up and are allowed to cast their votes.
  3. The votes are stored in the form of a ballot and then sent for counting.

In this method, the physical presence of any authority is not required during casting of votes. Thus the identity of the ballots is not revealed.

The first type of voting system requires the presence of the voter at the polling station. The ballots of voters are directly marked by the hands of electoral authorities, thus increasing the chance of electoral fraud.

In the other type, a voter can easily vote online through their personal laptop without the need to go to the polling booth. This method has lots of advantages such as:

1. Saving paper, reducing human work and human errors.
2. Saving time of an individual; no long queues.
3. Quick results of elections.
4. Auditable setup of e-voting scheme which provides accessibility to disabled people.
5. It provides access to vote for people living abroad, thus improving the participation in democracy.

The e-voting scheme involves a number of steps-

1. A Set up of an e-voting scheme by the central authority.
2. Distribution of votes and assigning each possible voter with a unique number, $m_1, \cdots, m_l$, where l is the total possible number of votes;
3. Voting only by an eligible voter;
4. Collecting the votes as a secret ballot;
5. Counting of secret ballots and then publishing the final result.

It is able to offer an integrated end to end electronic voting from registration to results.

Different countries need different designs of electronic voting system to meets their own laws and requirements which lead to a fast and legitimate result. Below are important factors needed to devise an efficient electronic voting system.

6.1 Requirements

Some requirement for having a practical and usable electronic voting scheme are the following:

- **Eligibility:** A person is allowed to vote only when he meets the eligibility criteria for voting. For example, a minimum age, valid voter id, etc. Each person can vote only once in an election. In other words, a person who has all the documents approved by the department or the authorities in charge of elections is eligible to vote.

- **Privacy:** Its easy to construct a voting scheme where no privacy is required. But the votes must be kept private so that no one is able to threaten a voter to vote for a particular person or party. Privacy is a key factor in voting scheme. The vote should not be known to anyone other than the voter himself. The vote should be stored in such a way that it is impossible for any individual to know the original vote or any information about the voter linked to the vote. The vote remains a secret throughout the voting process. The question which is of concern in this case is, if no one is able to know the vote then how can a vote be counted? Different types of schemes are used to tackle such a problem. In the following scheme, we use a version of Shamir's secret sharing scheme. Instead of distributing the shares of secret s, we distribute the share of g^s. The secret s is constructed in the same way as in the secret sharing scheme by taking a $k-1$ degree polynomial with constant term s. When any k persons collude their share then they can find the secret g^s and thus the vote. No $k-1$ authorities can find the secret g^s or have any information regarding it. Trusting k authorities compared to 1 authority is better and thus makes the scheme more secure. We assume that out of n authorities, at least k authorities can be trusted.

- **Individual verifiability:** Suppose a voter casts a vote, $m \in \{m_1, \cdots, m_l\}$. He votes and the vote E_m is encrypted in the form of secret ballot and is further proceeded for counting. The encypted votes should be published so that a voter can cross check their votes. How would the voter know that E_m is the encryption of m? There must be a way to convince the voter that his vote is correctly encrypted and counted. The constructed voting scheme should be able to allow a voter to verify whether the vote recorded is correct or not. Failure to verify encrypted vote as the original vote m will interrupt the election, since a person is allowed to vote exactly once.

- **Universal verifiability:** The authority in charge of handling all the voting stages should be able to verify that votes are counted properly. The final published tally should match the number of votes. If it doesn't match, then we can conclude that the counting was not done fairly.

- **Fairness:** Knowing the number of votes before the election is risky. Any authority who has power to edit the voting scheme can change the number of votes if they already know the results before the end of the election. So no participant should be able to gain knowledge about the number of votes before the counting stage. For example, suppose there is a voting scheme with vote A and vote B. While counting, suppose a person in authority knows the number of votes A and B and suppose he wants Vote A to win and he finds the number of vote B to be more. Then he may change the number of votes in such a way that the total number of votes remain same but the number of vote A is more and then pass it to the next person in authority, thus making the election unfair.

- **Robustness:** The machine or internet used while voting should not change the vote. It can happen that a person votes $m \in \{m_1, \cdots, m_l\}$, but due to some error or cheating, the stored vote is $m' \in \{m_1, \cdots, m_l\}$ instead of m. This affects the original vote and results in an incorrect number of votes. So the machine and the online server should be error free. In other words, any cheating should be detected easily.

6.2 Various approaches

E-voting schemes are based upon various approches [8]. These approaches solve different requirements needed in the scheme. The most difficult requirement of a voting scheme is privacy. It is easy to design a voting scheme which doesn't have privacy. For example, the eligible voter can directly write his vote at the bulletin board and anyone can read. Since the voters' votes must be kept secret, privacy is important. There are a few approaches which have been invented to achieve privacy. It can be accomplished in three ways:

- **Knowing the vote but not the identity of it :** It is easy to vote, but hard to trace it back to the voter. In other words, it means that when a person votes, his vote is stored and proceeded for counting, but in the counting stage it is impossible to know whom the counted vote belongs to. In this approach, the identity of the voter with their own votes cannot be tracked once the vote is proceeded for counting.

- **Knowing the identity of vote but not the vote:** It is hard to know or see the vote, but easy to see the identity of the voter. When a voter votes, his vote is stored in an encrypted form. The identity of the person with the encrypted vote is not removed and the vote is enclosed in a ballot. The identity of the voter is plainly available in the secret ballot, but not the vote. After the final result of counting is published, encrypted votes can also be published. All encrypted votes are permuted and then assigned a unique number. By providing the permutation key and secret key to a voter, he can decrypt his encrypted vote and can verify that his vote was counted properly. We use this approach to construct an e-voting scheme in the presented scheme.

- **Knowing the vote and identity of vote:** Both seeing the actual vote and the identity of the voter is impossible or computationally infeasible. Consider the scheme in which a voter votes and his vote is stored with his identity. It is obvious to see that in such a case, privacy is compromised. Thus constructing a scheme where the voter and his vote are both publicly known is not feasible.

6.3 Stages of e-voting

Electronic voting scheme consisits of three main stages:

- **Initialization:** The central authority sets up the system. It announces the date of elections, formulates the questions and possibilities for an answer and creates a list of eligible voters. Eligible voters are assigned with some unique numbers. The vote is stored in binary form. The binary form represents the encrypted vote. The central authority also generates their public and secret keys. It publishes the public values. The secret key is given to the voter as a token of eligibility. We will not talk about the details of how a voter is verified for eligibility and will focus only on how the vote of an eligible voter is counted.

- **Voting stage:** Voters cast their votes using ‘secret channels’ to communicate with the authorities and get their secret key. Here ‘secret channels’ refers to transferring the secrets from A to B through a channel such that no third person C who might have access to the channel, can change the secret or know about it. Since it is out of scope for the present discussion, we will not discuss it here and proceed to see how the vote is counted using Shamir’s secret scheme. The stored vote is then divided into n indistinguishable parts. Once the election gets over it is proceeded for counting.

- **Counting stage:** Before the counting starts, the authorities verify their shares. Once verified, any k authorities use their public and secret information to decrypt the encrypted votes and count the votes. At the end, they publish the result of the election. Thus the voter can cross-check his vote.

It can be pictorically shown as:

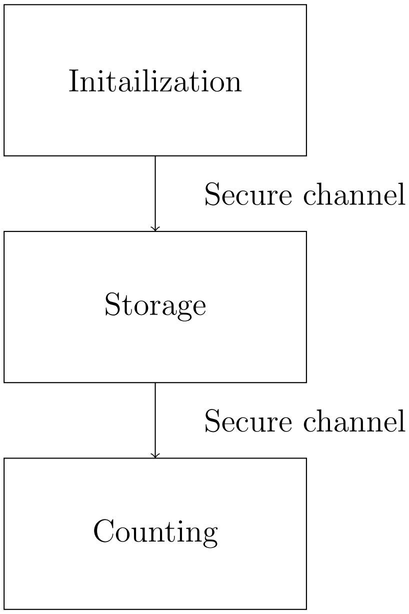

Figure 6.1: Stages of e-voting

There could be more than three stages for seting up a scheme.

6.4 Non interactive zero-knowledge proof of knowledge

Non interactive zero-knowledge proof of knowledge is a method for proving a secret to a verifier without telling about the secret or revealing any information related to it. It was first introduced by Blum, Feldman and Naor Micali [3]. For example, a person Amit has a 100 rupee note and he claims to have the 100 rupee note to Sumit. Sumit does not believe Amit. How would Amit prove that he has a 100 rupee note? If he shows the money to Sumit, he might snatch it and run away. In this scenario, Amit needs to prove to Sumit that he has 100 rupee note without showing the money. Intuitively, the non interactive zero-knowledge proof of knowledge is a non interactive zero-knowledge proof of language membership from which, given certain information, a witness of language memebership can be recovered [3]. The information in our case is $(x, y) = (g^\alpha, h^\alpha)$ and the prover wants to show that there is such an α without revealing any information about α. In other words the exponent value of g and h determining (x, y) which is publicly known must be same. The value of α is not known to anyone except the prover. Here non interactive zero-knowledge proof of knowledge is applied as described below:

1. The prover finds (x, y) as g^α, h^α, he knows α. He wants to prove to a verifier that he has used the same α in g, h for finding (x, y).

2. The prover first commits some value, say w and finds $(a, b) = g^w, h^w$. He then sends (a, b) to the verifier.

3. The verifier issues the challenge first which the prover has committed by giving a random value c

4. The prover receives c and then forms r as $r = w + (\alpha)c$. He sends r to the verifier.

5. The verifier verifies the challenge without having any understanding of α by calculating the value of g^r, h^r and checking it with the value of (ax^c, by^c).

The verifier can be replaced with the hash function (or something similar) above. Instead of a prover, the hash function will produce a challenge. We won't discuss about it since it is out of scope for the constructed non interactive zero proof of knowledge.

The constructed non interactive zero-knowledge proof of knowledge is represented in figure 6.2. The prover must know the value of α. If the prover doesn't know α, he cannot prove to anyone the existence of an exponent α that satisfies $x = g^{\alpha}, y = h^{\alpha}$ simultaneously.

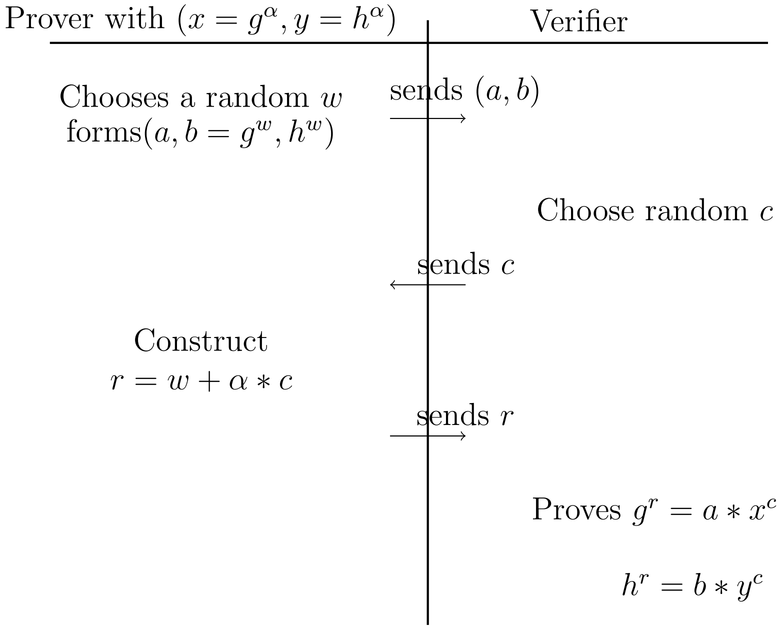

Figure 6.2: A schematic presentation of non interactive zero-knowledge proof of knowledge

- Suppose the prover doesn't know α.

- He forms $(a, b) = (g^{w}, h^{w})$ by taking a random w.

- He gets challenge c from the verifier.

- He then constructs $r_1 = w + \alpha_1 * c$ and sends r_1 to verifier.

- Let us compute g^{r_1} and $a * x^{c}$ separately and compare them. First, we will find out what the left hand side, g^{r_1} looks like: $g^{r_1} = g^{w+\alpha_1 * c} = g^{w} g^{\alpha_1 * c}$ Multiply by inverse of g^{w} and taking $1/c$th root of expression, we get g^{α_1}. Doing the same operation to the right hand side, we get g^{α}.

- To prove that L.H.S.=R.H.S., we need to show that $\alpha_1 = \alpha$.
- Hence, without knowing α, the prover cannot challenge the verifier.

The verifier must not give the challenge (in this case c) to the prover, before prover choose a random w. Challenging prover before receiving $(a, b) = (g^w, h^w)$ to the verifier may result in cheating and end up in receiving incorrect shares. What the prover can do is the following:

- He chooses a different value of exponent for (x, y) as $(g^{\alpha_1}, h^{\alpha_2})$.
- Since he gets the value c by prover first, he chooses a random w_1 and constructs $w_2 = c(\alpha_1 - \alpha_2) + w_1$ and sends the prover (a, b) as (g^{w_1}, h^{w_2}).
- He then calculates r as $w_1 + c\alpha_1$ which is also equal to $w_2 + c\alpha_2$.
- When the verifier tries to verify using this r, he finds that $(g^r, h^r = a * x^c, b * y^c)$ is correct without knowing that he has been cheated by the prover, who took advantage of knowing the value of c beforehand and computed a and b using two different exponents.

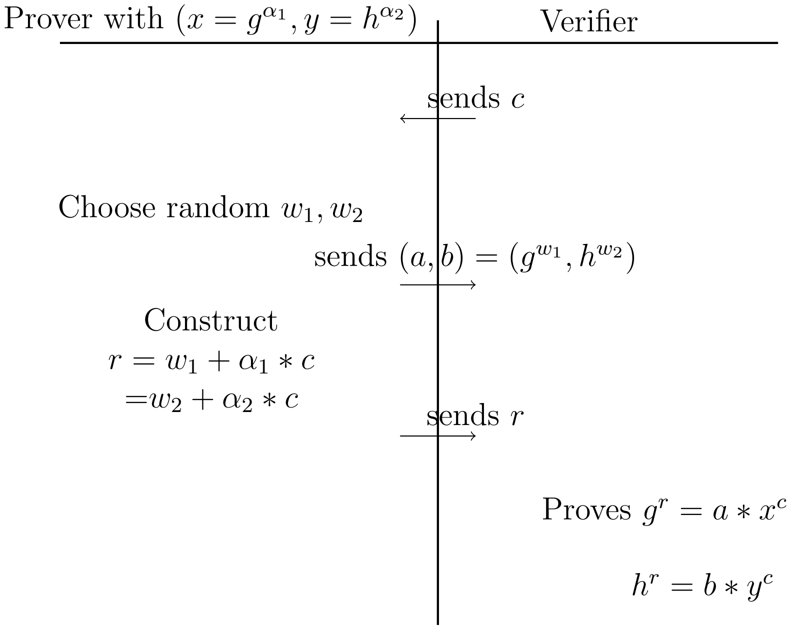

Figure 6.3: How challenging by verifier before prover commits affects

6.5 An e-voting scheme using public verifiable secret sharing schemes

A secret sharing scheme is a (k, n) threshold scheme, where a dealer D divides a secret S into n parts and distributes it to n people as shares such that when any k shares come together, the secret S can be reconstructed. No less than $k-1$ shares can do so. The scheme presented below describes how an eligible voter V can vote for his vote $m \in \{m_1, \cdots, m_l\}$, (where $m_i = 1, l$ are all the possible votes) without anyone else knowing any information about the vote. The central authority A is trusted and deals with the lower level authorities $A_i, i = 1, n$ and voter V.

- **Initialization:** The central authority assigns all the possible number of votes with a unique number as $(m_1, m_2, \cdots, m_l)$, where l is the total number of votes available for election. It publishes a group $\mathbb{Z}_p$, where p is a prime, and a generator g of the group and G. It generates s_1 by taking a $k-1$ degree polynomial, $f(x) = a_0 + a_1x^1 + \cdots + a_{k-1}x^{k-1}$ where $a_0 = s_1$ and keeps it secret. The secret s_1 is given to the voter V_1 as proof of eligibility for voting by the central authority. When the voter V_1 votes, his vote is stored in an encrypted form as $E_1 = mg^{s_1}$. The encrypted vote of the voter and the voter are then connected together by assigning a number without disclosing any identity of the voter. Here we assume that the central authority doesn't know how the encrypted vote looks. For example, a person votes and forms a ballot inscribed with his vote. Then he submits the ballot. When he sumbits, some of the authorities assign a number to the ballot and the same number is assigned to the voter. Later the ballot is removed without knowing the identity of it and it proceeds for counting purposes.

- **Distribution of the shares:** The central authority distributes the secret g^{s_1} to n lower authorities. The secret g^{s_1} recovers the encrypted vote E_1 which belongs to the voter V_1.

  The point s_1 is randomly chosen by the central authority by constructing the $k-1$ degree polynomial $f_1(x) = a_0 + a_1x^1 + \cdots + a_{k-1}x^{k-1}$, where $a_0 = s_1$. The lower authorities A_j choose their secret keys z_j and publish their public keys $h_j = g^{z_j}$. With the help of the public key h_j, the central authority constructs shares as $H_j = h_j^{f(j)}, j = 1, 2, \cdots, n$ and gives them to the n authorities. The central authority also publishes $C_0 = G^{a_0}, C_1 = G^{a_1}, \cdots, C_{k-1} = G^{a_{k-1}}$. The purpose of publishing the values $C_i, i = 1, \cdots, k-1$ by the central authority is for the n lower authorities to verify that the shares they have received are consistent. He defines $X_j = \pi_{i'=1}^{k-1} C_{i'}^{j^{i'}}$, whose exponent $f_1(j)$ is the same as the exponent in $H_j = h_j^{f(j)}, j = 1, 2, \cdots, n$ which are given as shares to n authorities. If he is able to show that both the exponent are same, then he would be able to prove that his shares are correctly distributed.

He verifies that $log_G X_j = log_{h_j} H_j$ i.e. both the exponent to be same, using non interactive zero-knowledge proof of knowledge, where $X_j = \pi_{i'=1}^{t-1} C_{i'}^{j^{i'}}$.

- **Reconstruction of the secret g^s:** The lower authorities A_j then decrypt their shares $S_j = g^{f(j)}$ by computing $S_j = H_j^{1/z_j}$.

  Before sharing their shares, the lower authorities need to verify to the central authority that they had not changed their own secret key and are truthworthy. To do so, they show that the exponent term in h_j is same as the negative of the exponent term of S_J. By the non interactive zero-knowledge proof of knowledge, the jth lower authority shows that $log_g h_j = -log_{H_j} S_j$. If any k of them are able to prove the above, they are allowed to share their shares and reconstruct the secret g^s using Langrange interpolation as:

  $$\prod_{j \in A} S_j^{l_{j,A}} = \prod g^{f(j) l_{j,A}} = g^{\sum p(j) l_{j,A}} = g^{f(0)} = g^{s_1}$$

  where $l_{j,A}$ is a langrange coefficient.

- **Counting votes** Once the lower authorities A_j find g^{s_1} using Lagrange interpolation, they decrypt the encrypted vote E_1 of voter V_1 using the inverse of g^{s_1}. Then the vote is counted and stored till all the votes are counted. After counting is over, the central authority declares the results.

6.5.1 Properties of the above scheme

- Privacy: The vote m is kept private throughout the scheme. Thus it keeps the vote confidential. Encrypted vote is of the form $m * g^{s_1}$ and then g^{s_1} is divided into n parts. It is distributed as shares to n shareholders. The authorities using their own secret key z_i have access to the shares for reconstructing the secret

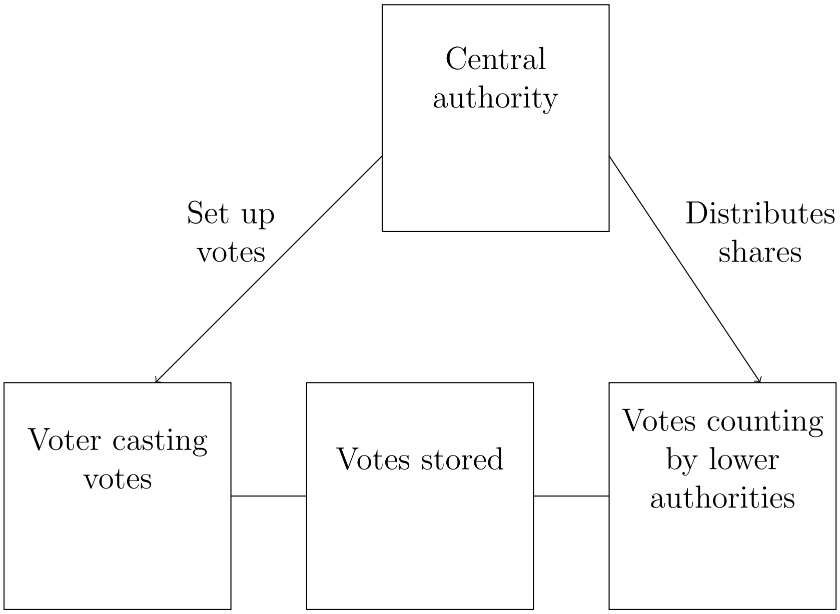

Figure 6.4: Schematic presentation of e-voting

g^{s_1}. The vote m is determined and counted after the election is over. In the whole process, the identity of the vote m is not known to anyone, thus keeping the vote m a secret.

- Correctness: The scheme uses the secret sharing scheme i.e. when any k out of n people come together, the secret g^{s_1} is reconstructed. Any $k-1$ out of n people can not get any information about the secret. If any k' shareholders try to cheat then the remaining k out of $n-k'$ can use their shares to cross-check the secret g^{s_1} and find out the defects.

- Verifiability: The final result of votes is published as encyrpted votes. Thus, one can easily verify their own shares using the secret key they receive from the central authority. Now if the voter V_1 knows s_1, he can easily verify whether the outcome vote matches with his vote or not.

6.6 Issue and drawbacks in this scheme

1. In the presented scheme, the central authority handles the scheme from the first step to the final step. It constructs shares, distributes and publishes the results.

So we must trust the central authority. We don't trust the lower authorities individually.

2. Any fault in the system will lead to failure of the election.

3. Since when any k authorities out of n authorities can find g^{s_1} and no $k-1$ can do so, we must have k trustworthy authorities to operate this scheme.

4. Another problem with this scheme is the process of assigning numbers to the voter and his vote and passing to n lower authorities. Since the central authority knows g_1^s, he is not allowed to see the encrypted vote, but he has to link up Voter V_1's encrypted vote E_1 with the shares of the secret g^{s_1}. How would he verify that for decrypting E_1, he has sent shares of secret g^{s_1}? Using the shares of secret g^{s_1} with some other encrypted vote $E_i, i \neq 1$ would result in an error.

5. In this case rearranging of votes is a difficult task. But it could be solved if the rearranging is done by the lower authorities without giving any information about rearranging to central authority.

Bibliography

[1] Beutelspacher Albrecht and Ute Rosenbaum. *Projective geometry: from foundations to application.* Cambridge University Press, 1998.

[2] Simeon Ball and Zsuzsa Weiner. *An Introduction to Finite Geometry.* 2011.

[3] Daniel R. Simon Charles Rackoff. Non-interactive zero knowledge proof of knowledge and chosen ciphertext attack. *Advances in Cryptology-CRYPTO'91(pp. 433-444)*, 1992.

[4] William fulton. *Algebraic curves.* Benjamin-Cummings Publishing Co., Subs. of Addison Wesley Longman,US, 1969.

[5] 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.

[6] lein Harn Lin, Changlu and Dingfeng Ye. Ideal perfect multilevel threshold secret sharing scheme. *Information Assurance and Security*, 2009.

[7] C. L. Liu. *Introduction to combinatorial mathematics.* McGraw-Hill, Inc, 1968.

[8] Zuzana Rajaskova. *Electronic voting scheme.* PhD thesis, Comenius University, Brastislava, April 2002.

[9] Adi Shamir. How to share a secret. *Communications of the ACM 22, no.11:612-613*, 1979.

[10] Gustavus J. Simmons. How to (really) share a secret. *Proceedings on Advances in cryptology(pp.390-448)*, 1990.

[11] Douglas R. Stinson. Cryptography theory and practice, 1995.

[12] Wikipedia.