Undergraduate Research Opportunity
Programme in Science

Secret Sharing Schemes

A Cryptographic Application of Finite Projective Geometry

Kiah Han Mao
Supervisor: Dr. James Quah (CSIT)

Department of Mathematics
National University of Singapore
2003/2004

Summary of author's contributions

This report was written under the umbrella of the Undergraduate Research Opportunities Programme in Science(UROPS). It is primarily a survey of the many papers written on secret sharing. However, the author has modified some proofs and generalised constructions so as to make this report a coherent one.

Namely,

- **Chapter 3 and 4** The algorithms for the general construction of a compartment/mulit-level scheme were modified from the basic constructions in [3].
- **Chapter 7** In [8], the secret sharing schemes were constructed over an affine geometry. As we only refer to projective geometry in this report, the author has modified the construction to the projective setting.
- **Examples** All examples of secret sharing schemes in this report were original and were contrived by the author.

Contents

Chapter 1

Introduction

> *The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others.*
>
> John Chadwick

However, it is not just curiosity that drives the desire to intrude on secrets. In a war, the attainment of vital intelligence is tantamount to victory. In the financial market, inside information would mean a windfall. Indeed, it is to the selfish interests of many individuals to be able to take a peek at some confidential information, or, as we shall call it – the secret.

Therefore, we must be able to protect the secret from these intruders. There are many ways of protecting a secret, but let us consider the following traditional method.

> Boss keeps the secret in a safe. The safe can only be opened with a key. Boss keeps the key.

Now, it is apparent that the safe can only be opened by Boss. Hence, we conclude that the secret is safe within the safe. But is this solution perfect?

What if Boss loses the key? Then the secret information will become inaccessible. There is also the option whereby Boss arranges for engineers to pry open the safe. Naturally, this will render the safe useless and another safe have to be bought. Hence, it will be costly if Boss loses the key.

Can we trust Boss? Of course, we assume we can. However, if Boss is going on a vacation, then who can Boss entrust the key to? Having a singular key means that Boss have to trust a single person to hold onto this key. The question is how Boss can be sure that this person will not exploit the secret information?

The answer to both these questions – Split the key! We divide the key into pieces and distribute them to different persons so that certain subsets of these people are able to reconstruct the key. We observe that, even if some portions of the keys are lost, we are still able to reconstruct using the other portions. Moreover, a group of people is less likely to exploit the secret information, because the chances of getting caught or being betrayed by the other group members is higher.

Hence, this is basic idea behind secret sharing schemes and we give a formal definition of secret sharing schemes in chapter 3.

The Principle

However, is this concept of splitting the key realistic? Yes, and in fact secret sharing schemes work on the wellknown principle of **reduced trust**. The principle states that in order to keep a secret, the less knowledge or power each participant has the better. So, instead of giving out an entire key (which represents the actual trust) to a participant, we give him a portion (the reduced trust) of it.

The following paragraph written by *Williscroft* describes a plausible (probably, actual) launching procedure of a nuclear missile.

> Launching a nuclear weapon takes the specific simultaneous action of several designated individuals. For example, to launch a missile from a ballistic missile submarine, two individuals must insert keys into separate slots on separate decks within a few seconds of each other. Barring this, the system cannot physically launch a missile. Because the time window for key insertion is less than that required for one individual to accomplish, it is physically impossible for a missile to be launched accidentally by one individual.

Here, the authority to launch the missiles is divided into two portions and this power manifests itself in the two keys. In other words, each key (or keyholder) is entrusted with less power. So it is difficult, or rather impossible, for one keyholder to exploit his power to launch the nuclear weapon.

Indeed, secret sharing schemes are common at areas which deal with sensitive information.

The Construction

When mathematicians look at secret sharing schemes, the natural question is if such schemes are constructable using present mathematical structures. C. L. Liu. posed a similar problem and gave his own solution.

> Suppose eleven scientists are working on a secret project. They want to lock up their documents containing secret information. They want to permit the cabinet to be opened if and only if six of the scientists are present. He asks the rhetorical question: how many locks are required to properly secure the cabinet in this circumstance? The answer is 462 locks, obviously not a practical number. Then to seal the fate of this concept he asks, what is the smallest number of keys required for each scientist? The answer is 252 keys for each scientist.

Well, Liu was badly mistaken. A. Shamir and G. Blakley independently presented their constructions which ingeniously used polynomial interpolation and finite geometries respectively. Solving the Liu's problem with Blakley's scheme, each scientist holds onto a share or a point in space. And this point contains only 7 bits (quite far off from the figure 252).

Hence, Shamir's and Blakley's ideas became more acceptable and these schemes were named **threshold schemes**. As this report is about finite geometries, we naturally study Blakley's more in detail. We first introduce Blakley's scheme in chapter 3, and make modifications to the original scheme in the subsequent chapters to include some interesting properties.

Geometry

Before we examine secret sharing schemes, we shall first in the next chapter introduce the ideas of projective geometry – the basis which Blakley's scheme is built upon. Geometry is nearly a well forgotten branch of mathematics. Most modern mathematical education systems have neglected this subject, putting geometry off as a subject that deals with meaningless abstraction. Indeed, one might question the relevance of projective geometry in the physical world if the concept of parallelism (which is present in the real world) is excluded.

Yet ironically it is this exclusion that makes projective geometry friendly to computer scientists. Computation wise, we can obtain an easy way to represent of points and lines in vector spaces. This fact, fuelled with recent developments of combinatorial connections, have uncovered many interesting applications in modern communications. Today, finite geometry is commonplace to describe structures in coding and cryptography.

To conclude, the author must admit that this report is an elementary one that merely introduces secret sharing schemes. Many interesting ideas are not discussed in depth and many proofs to theorems have been omitted due to the author's incompetence. There are many times when the author wanted to delete the entire document and start writing afresh. However, the time factor did not allow so.

Nevertheless, the author wants to express his immense gratitude to Dr. James Quah for patiently guiding the author through this project and unveiling the world of research mathematics; Dr. Victor Tan for his undying support, especially in typesetting this report; and to all friends who gave the author the moral support and encouragement.

The author wishes the reader an enjoyable and fulfilling tour of secret sharing.

Chapter 2

Projective Geometry

An incidence structure, or *geometry*, comprises a set of *points*, a set of *lines* and a relation, *incidence*, between them. However, by this definition alone, one cannot obtain any meaningful result. Hence, constraints are added to this definition by including other assumptions. In mathematical terms, we call them *axioms*.

In this chapter, we will explore the fundamentals of a geometry called *projective geometry*. Projective geometry is a class of geometry that is slightly different from the Euclidean or affine geometry – the geometry of the physical space. The main difference is the exclusion of parallel lines in the former. Yet, the two geometries are the same in many ways. However, we shall develop our secret sharing schemes based on the projective setting for the simple reason that projective spaces are easier to deal with.

In this chapter, we shall make many statements without proof. Instead, we shall explore the concepts behind the theorems and look at the consequences that follow. Basic examples will play an important role in helping us understand the construction of the secret sharing schemes. For a good reading of the topic, the author recommends the following: [3],[4],[5].

From now on, the following notations will be adopted. Points shall be denoted by uppercase letters, while lines denoted by lower case letters. When point P is incident with line g, we say 'P *lies on* g', 'g *passes through* P' or even '$P \in g$' . Points and lines only exist as indicated and that lines are simply collection of points.

2.1 Axioms

In this section, we develop two fundamental parameters that determine the 'size' of a projective space - *dimension* and *order*. In the course of doing so, we will introduce the concepts of subspaces, spanning and independence.

But first, let us define the projective space.

Definition 2.1.1. A **projective space** is a geometry of a set of *points* and a set of *lines*, with an *incidence* relation, such that the following holds:

i. Any two points lie exactly on a line.

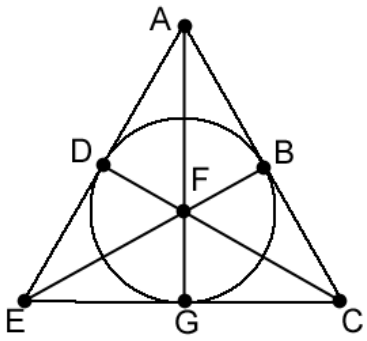
ii. *(Vebler-Young axiom)* Let A, B, C, D be four distinct points such that no three are collinear. If the lines AB and CD intersect each other, then the lines AD and BC also intersect each other.

iii. Any line has at least three points.

iv. There are at least two lines.

Remark 2.1.1. Axioms *(i),(iii),(iv)* are fairly simple to understand. However, axiom *(ii)* is a bit tricky. Another equivalent way of phrasing the Vebler-Young axiom is: *if two lines are in the same plane, then they will intersect at least one point*. Upon close examination, we will realise that this axiom does not hold in the affine space. Any pair of parallel lines is the counter example! They are indeed coplanar lines which do not intersect at all. Hence, an essential characteristic of projective geometry is that there are no parallel lines!

Example 2.1.1. A simple geometry (or the *smallest* one) that satisfies the above axioms is the following figure, better known as the *Fano Plane*. It consists of a plane triangle with its three cevians. The circle is considered as a line and only the indicated points exist. In the Fano Plane, there are seven points and seven lines, three points on each line and three lines passing through each point.



the Fano plane

By simple observation, we can verify that the axioms (i) to (iv) are satisfied.

2.2 Spanning, Independence, Dimension

Next, we shall introduce other terms and concepts so that we can better describe the projective space. We shall see familar terms such as spanning, independence and dimension. However, we emphasize that these terms are conceptually different from the 'same' terms in linear algebra. This is essentially due to the fact that they are defined differently.

Definition 2.2.1. Let $\mathbf{P}$ be an arbitrary projective space. A (linear) **subspace** of $\mathbf{P}$ is a set $\mathbf{U}$ of points $\subseteq \mathbf{P}$ such that for any two points X, Y in $\mathbf{U}$, any point on the line XY is contained in $\mathbf{U}$.

Clearly, any point, line and the whole space $\mathbf{P}$ is a subspace of $\mathbf{P}$. In addition, we note that most subspaces are themselves projective spaces (That is, provided there are at least two lines). From now on, all subspaces are denoted by uppercase letters in bold.

Definition 2.2.2. If $\mathcal{S}$ is a set of points in $\mathbf{P}$, the **span** of $\mathcal{S}$, $\langle S \rangle$, is defined to be the smallest subspace containing $\mathcal{S}$. We shall also say that $\mathcal{S}$ spans $\langle \mathcal{S} \rangle$ or $\langle \mathcal{S} \rangle$ is spanned by S.

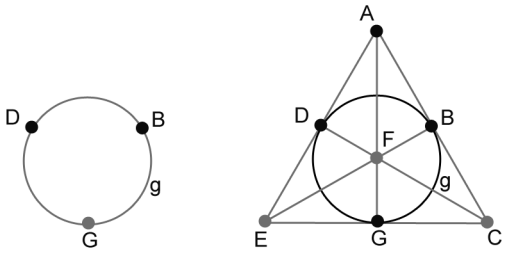
For instance, in the Fano plane, let $\mathcal{S} = \{A, B\}$. Then $\langle \mathcal{S} \rangle$ is the line AB. Hence, $C \in \langle \mathcal{S} \rangle$ too. In addition, we can replace the word 'points' with other elements of the projective space, such as lines. So, the Fano plane is spanned by either $\{A, B, D\}$ or $\{g, A\}$ (where g is the line containing B, D, G).

However, it is difficult to verify that a subspace is indeed the space spanned by a set of points. Or rather, it is not easy to check if the subspace is indeed the smallest one. Hence, we have the following theorem (stated without proof) which enables us to easily construct the span of a set of points.

Theorem 2.2.1. *Let* $\mathbf{U}$ *be a nonempty subspace of* $\mathbf{P}$*, and* X *be a point of* $\mathbf{P}$*. Then*

$$\langle \mathbf{U}, X \rangle = \bigcup \{\textit{points on the line } XY \mid Y \in \mathbf{U}\}$$

Example 2.2.1. Let us try to construct $\langle A, B, D \rangle$ using the theorem.



Constructing $\langle B, D \rangle$ and $\langle A, g \rangle$

First we note that $\langle B, D \rangle = g$. So we get an extra point G. Next to construct $\langle A, g \rangle$ we need to join A with the 3 points B, D, G. The line AB will contain another point C; line AD contains E; line AG contains F. Hence we obtain all the points on the Fano plane, which is indeed a linear subspace.

Definition 2.2.3. A set $\mathcal{S}$ of points is **independent** if $\forall X \in S$, $X \notin \langle S \backslash \{X\} \rangle$.

For instance, $\mathcal{S} = \{A, B, D\}$ is an independent set of points in the Fano plane. We check that $A \notin \langle B, D \rangle = \text{line } BDG$ and $B \notin \langle A, D \rangle = \text{line } ADE$ and $D \notin \langle A, B \rangle = \text{line } ABC$. Again, the word 'points' is substitutable. We can say both the sets $\{A, B, D\}$ and $\{A, g\}$ are independent.

However, we recall that the Fano plane (=$\mathbf{P}$) is spanned by $\{A, B, D\}$. We notice that $\mathbf{P} = \langle A, B, C, D \rangle$ too. But the set $\{A, B, C, D\}$ is not independent as C lies on the plane spanned by A, B and D. We realise that, if we wanted a set to span the entire space $\mathbf{P}$ efficiently, then point C is redundant as the set $\{A, B, D\}$ is sufficient. Hence we have the following theorem which exhibits the importance of independence.

Theorem 2.2.2. *Let $\mathcal{B}$ be a set of points. $\mathcal{B}$ is an independent set that spans $\mathbf{P}$ if and only if $\mathcal{B}$ is a minimal spanning set, that is, if $\mathcal{B}$ spans $\mathbf{P}$, no proper subset of $\mathcal{B}$ spans $\mathbf{P}$.*

Remark 2.2.1. There is a term for the set $\mathcal{B}$. The independent set $\mathcal{B}$ of points that spans $\mathbf{P}$ is called a **basis** of $\mathbf{P}$.

In addition, we note that for any fixed $\mathbf{P}$, a basis of $\mathbf{P}$ is not unique. For instance, $\{A, B, D\}$ and $\{C, E, F\}$ are both bases for the Fano Plane. However, we observe that both bases contain the same number of elements. In fact, this is always true, and we have the following theorem.

Theorem 2.2.3. *Let $\mathbf{P}$ be a* **finitely generated** *projective space (that is, there is a finite set of points that spans $\mathbf{P}$). Then any two bases of $\mathbf{P}$ have the same number of points.*

Hence, we obtain the first fundamental parameter.

Definition 2.2.4. Let $\mathbf{P}$ be a finitely generated space. If $d + 1$ denotes the number of points in the basis (which by 2.2.3 is constant), then we call d the dimension of $\mathbf{P}$, or $d = dim(\mathbf{P})$.

Therefore, the Fano plane has a dimension of 2 (there are $2 + 1$ points in any basis for the plane).

In any projective space $\mathbf{P}$, with dimension d, there are some subspaces that we are generally interested in. Hence, we give them specific names,

namely, the subspaces of dimension 2 are called **planes** and the subspaces of dimension $d-1$ are called **hyperplanes** of $\mathbf{P}$.

Lastly, we end our section with an important concept: **general position**. In the study of coding theory and cryptography, we are interested in generating points which are in general position. Hence, we define this term.

Definition 2.2.5. Let $\mathbf{P}$ be a finitely generated space. We say that a set $\mathcal{X}$ of at least $d+1$ points is (or the points are) in *general position* in $\mathbf{P}$ if any $d+1$ points in $\mathcal{X}$ form a basis for $\mathbf{P}$.

For instance, the set of points $= \{A, B, D, F\}$ is in general position in the Fano plane. We check that:$\{A, B, D\}$, $\{A, B, F\}$, $\{A, D, F\}$ and $\{B, D, F\}$ are all possible bases for the Fano plane.

Remark 2.2.2. We also emphasize the fact that the set of points is in general position *in the Fano plane*. That is, generally, when we say that a set of points are in general position, there must be a reference to the projective space they are in general position in. Illustrating this fact, we look at the points B, D, G in the Fano plane.

We can say that B, D, G are in general position *in the line* g. Simply because $\{B, D\}$, $\{B, G\}$, $\{D, G\}$ are all bases for the line g. But the points B, D, G are **not** in general position *in the Fano plane*. This is obvious because B, D, G do not even span the Fano plane.

Remark 2.2.3. There is a simple way of checking if a set of points is in general position in a projective space of dimension d. We need to ensure that no d of them lie in a hyperplane. Hence, in the case where $d = 1$, we need to ensure that no two points lie in the same point (or that the points are distinct); in the case where $d = 2$, we need to check that no three points are collinear.

2.3 Order

A projective space is called **finite** if its point set is a finite set. In this report, only finite spaces are dealt with. That is, we are only looking a finite set of points, which in turn leads to a finite set of lines and etc. Yet, the number of points on each line, or the number of hyperplanes in a projective space, is not as random as it seems. We have the following governing theorem.

Theorem 2.3.1. *Let g_1 and g_2 be two lines of a projective space* $\mathbf{P}$*. Then there exist a bijective map $f : (g_1) \longrightarrow (g_2)$ from the set (g_1) of points on g_1 to set (g_2) of points on g_2.*

In other words, the theorem states that any two lines have the same number of points. And by theorem 2.3.1, any two t-dimensional subspace have the same number of points, lines, and smaller subspaces. This suggests a great deal of symmetry in our projective spaces.

So we fix the second parameter.

Definition 2.3.1. Let $\mathbf{P}$ be a finite projective space. If $q+1$ denotes the number of points on a line, then we call q the **order** of $\mathbf{P}$.

Remark 2.3.1. However, not all positive integers q can be an order of a projective plane. We know of constructions for planes of order 2(the Fano plane), 3, 4 and 5. But mathmaticians also have shown that it is not possible for a plane of order 6. To date, mathematicians has shown the existence of projective planes of orders which are prime power. That is, $q = p^n$, where p is prime and n a positive integer. Yet, they have not shown the non-existence of planes with non-'prime power' order. In this report, we will assume q is a prime number.

Remark 2.3.2. We have come across two instances where the word 'finite' is used: a *finitely generated* space and a *finite* space. Indeed, they refer to the two parameters, dimension and order respectively. In this report, we will only deal with finite projective spaces of finite dimension d and order q.

Before we end this section, we note that the order q is important in aiding us in counting the number of t-dimensional subspaces in a particular projective space.

Theorem 2.3.2. *Let* $\mathbf{P}$ *be a projective space of dimension d and order q. Then*

i. The number of points in $\mathbf{P}$ *is*

$$\frac{q^{d+1}-1}{q-1}$$

ii. The number of t-dimensional subspaces in $\mathbf{P}$ *is*

$$\frac{(q^{d-t+1}-1)(q^{d-t+2}-1)\dots(q^{d+1}-1)}{(q-1)(q^2-1)\dots(q^{t+1}-1)}$$

iii. The number of t-dimensional subspaces containing a particular s-dimensional subspace is

$$\frac{(q^{t-s+1}-1)(q^{t-s+2}-1)\dots(q^{d-s}-1)}{(q-1)(q^2-1)\dots(q^{d-t}-1)}$$

Corollary 2.3.3. *In particular,*

i. The number of points on a line is $q+1$.

ii. The number of points on a hyperplane is $\frac{q^d-1}{q-1}$.

iii. The number of hyperplanes passing through a s-dimensional subspace is $\frac{q^{d-s}-1}{q-1}$.

2.4 Coordinatizing the Projective Space

In this section, we coordinatize the projective space by representing the points by vectors, and lines, planes, hyperplanes by subspaces in a vector space. Familar terms such as vectors and matrices in linear algebra will appear. As mentioned, q is prime in this report, and hence, we only work with vector spaces over finite fields with prime order. Again, all theorems here will be stated without proof. For a good reading of projective geometries over finite fields, please refer to [3].

Definition 2.4.1. Let V be a vector space of dimension $d+1$ over a finite field of order q. We define the geometry $\mathbf{P}(V)$ as follows:

- the points of $\mathbf{P}(V)$ are the 1-dimensional subspaces of V,
- the lines of $\mathbf{P}(V)$ are the 2-dimensional subspaces of V,
- a point X is incident with a line g if and only if the 1-dimensional subspace X is contained in the 2-dimensional subspace g.

Remark 2.4.1. We note that points are 0-dimensional objects in the projective space but they are represented by 1-dimensional subspaces of V. Similarly, 1-dimensional lines are represented by 2-dimensional subspaces of V. Generally, a n-dimensional subspace of a projective space is represented by a $n+1$-dimensional subspace of V.

Theorem 2.4.1. *Let V be a vector space of dimension $d+1$ over a finite field of order q. Then $\mathbf{P}(V)$ is a projective space of dimension d and order q. We denote $\mathbf{P}(V)$ to be $\mathbf{PG}(d,q)$.*

Example 2.4.1. Let us consider $V = F_2^3$. Then $\mathbf{P}(V)$ is in fact the Fano Plane. We can for instance let the points be the 1-dimensional subspaces,

$$A = \langle(0,0,1)\rangle$$
$$B = \langle(0,1,0)\rangle$$
$$C = \langle(0,1,1)\rangle$$
$$D = \langle(1,0,0)\rangle$$
$$E = \langle(1,0,1)\rangle$$
$$F = \langle(1,1,1)\rangle$$
$$G = \langle(1,1,0)\rangle$$

And the lines are 2-dimensional subspaces. So, the line $AB = \langle(0,0,1),(0,1,0)\rangle$. And of course, $C = \langle(0,1,1)\rangle \subseteq \langle(0,0,1),(0,1,0)\rangle = AB$, that is, C lies on the line AB.

From linear algebra, we know that any vector v can be represented uniquely by the **coordinates** $(a_0, a_1, \ldots, a_d)$, where $v = a_0v_0 + a_1v_1 + \ldots + a_dv_d, a_i \in F_q$, v_i form a basis for V. Hence, we have a representation for the points of $\mathbf{P}(V)$.

Definition 2.4.2. A point $\langle v\rangle$ of $\mathbf{P}(V)$ has the **homogenous coordinates** $(a_0, a_1, \ldots, a_d)$ if $\langle v\rangle = \langle a_0v_0 + a_1v_1 + \ldots a_dv_d\rangle$.

However, we observe that two different coordinates can represent the same point. For instance, in $\mathbf{PG}(2,3)$, $(1,1,1)$ and $(2,2,2)$ represent the same point as

$$\langle(1,0,0)+(0,1,0)+(0,0,1)\rangle = \langle 2(1,0,0)+2(0,1,0)+2(0,0,1)\rangle$$

where $\{(0,0,1),(0,1,0),(1,0,0)\}$ is a basis for the vector space.

In particular, two homogenous coordinates, $(a_0, a_1, \ldots, a_d)$ and $(b_0, b_1, \ldots, b_d)$, represent the same point if and only if there exists an element t in F_q such that $(a_0, a_1, \ldots, a_d) = t(b_0, b_1, \ldots, b_d)$. Without loss of generality, we will normalize the first(or last) non-zero coordinate to be 1.

Theorem 2.4.2. *Let V be the vector space F^{d+1}.*

i. Let M be a $(t+1)\times(d+1)$ matrix of rank $(t+1)$ and V' be the rowspace of M. Then $\mathbf{P}(V')$ is a t-dimensional subspace of $\mathbf{P}(V)$.

ii. Let $\mathbf{U}$ be a t-dimensional subspace of the projective space $\mathbf{P}(V)$. Then there exists a $(t+1)\times(d+1)$ matrix M of rank $(t+1)$ such that $\mathbf{U}=\mathbf{P}(V')$ where V' is the rowspace of M. We call M the **generator matrix** *for $\mathbf{P}(V')$*

Example 2.4.2. Again, we look at the representation of the Fano Plane.

Line AB can be represented by the matrix $\begin{pmatrix}0&0&1\\0&1&0\end{pmatrix}$.

We also observe a possible different generator matrix for line AB $\begin{pmatrix}0&1&1\\0&1&0\end{pmatrix}$.

We can have a unique representation if we choose the matrix to be of the Reduced Row Echelon Form.

So we represent AB by $\begin{pmatrix}0&1&0\\0&0&1\end{pmatrix}$.

Remark 2.4.2. As we see, points and subspaces may be represented by different vectors/coordinates and matrices respectively. For convenience, we adopt the following notations for the the point F

$$F=\langle(1,1,1)\rangle=(1,1,1)=t(1,1,1).$$

Similarly, the following all denote the line AB

$$AB=\langle(0,0,1),(0,1,0)\rangle=\begin{pmatrix}0&0&1\\0&1&0\end{pmatrix}=\begin{pmatrix}0&1&0\\0&0&1\end{pmatrix}.$$

Hence, we say two matrices are 'equal' iff they are row equivalent.

Theorem 2.4.3. *Let M be a $(t+1)\times(d+1)$ matrix of rank $(t+1)$ that represent a t-dimensional subspace $\mathbf{U}$ in $\mathbf{P}(V)$. There exists a matrix $(d-t)\times(d+1)$ matrix H such that a point $P(=\langle v\rangle)$ is a point of $\mathbf{U}$ if and only if $vH^T=\mathbf{0}$ We call H the* **dual matrix**.

Example 2.4.3. We continue from the previous example, and we see that the dual matrix for line AB is $H = (1, 0, 0)$ We can check

$$AH^T = (0, 0, 1)(1, 0, 0)^T = 0$$

$$BH^T = (0, 1, 0)(1, 0, 0)^T = 0$$

$$CH^T = (0, 1, 1)(1, 0, 0)^T = 0$$

So we have an easy way to check if a point is in a particular subspace.

Definition 2.4.3. Let **U** be a subspace of $\mathbf{P}(V)$ and let H be a $(d-t)\times(d+1)$ matrix defined as above. Then the rowspace of H will be called the **dual space** of **U**.

Theorem 2.4.4 (Principle of Duality). *For any projective space* $\mathbf{P} = \mathbf{PG}(d, q)$*, there is a dual space* $\mathbf{P}^*$*, whose points and hyperplanes are respectively the hyperplanes and points of* $\mathbf{P}$*. For any theorem true in* $\mathbf{P}$*, there is an equivalent theorem true in* $\mathbf{P}^*$*. Moreover, the dual of a* t*-dimensional subspace in a* $\mathbf{PG}(d, q)$ *is a* $(d - t + 1)$*-dimensional subspace.*

Remark 2.4.3. In particular, in $\mathbf{PG}(2, q)$, a point and a line are dual. Hence, if 'any two points lie exactly on one line' (*axiom (i)*), then 'any two lines intersect exactly in one point'.

Remark 2.4.4. The principle states that the words 'point' and 'hyperplane' can be used interchangably. In our report, as we shall describe in the following chapter, the 'secret' in our secret sharing schemes is often a point. However, in other reports, the 'secret' may be an entire hyperplane. Of course, these 'different' schemes are fundamentally the same, illustrating the principle of duality.

Chapter 3

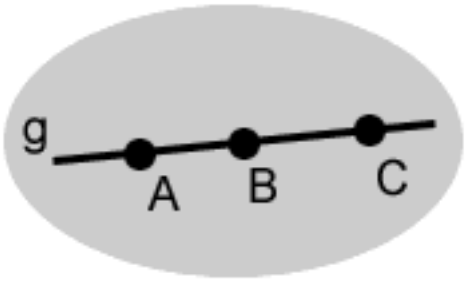
Threshold schemes

In the previous chapter, we have looked at concepts behind projective geometry. Although some properties may seem like mere figments of meaningless mathematical abstraction, the structures of classical projective geometry are surprisely ideally suited for modern communications. With its combinatorial connections, projective geometry have also induced many refreshing applications in the area of communications. Moreover, from our findings in 'analytic' geometry, we realise that projective spaces are easily constructed from vector spaces over finite fields. This realisation and with the advent of computers mean that we can implement such computationally complex mathematical schemes with ease.

In this report, we look into one cryptographic application – *secret sharing*. As the name implies, we study how to distribute secret information like authentication keys and encryption algorithms to a group of individuals.

A typical example is the following.

Example 3.0.4. In a bank, a boss wants to give three managers access to a bank vault. However, he does not trust any one manager to enter alone. He will only be comfortable if two managers are together to enter the bank vault. We propose a solution to this problem through the use of projective geometry. In a projective plane, we represent the secret to be a line g. To gain access to the bank vault, the managers must be able to construct the line g. We give each of the managers a point on the line distinct from the others. Then it is obvious that at least two managers must be together, so that the points can form the line g.



A simple example of secret sharing

Here is a formal defintion. A **secret sharing scheme** is a protocol to share a secret X among a set of participants in such a way that: participants in specified subsets are able to recover X by pooling their information; while participants in the other subsets are unable recover any information on X.

Hence, in the above example, the secret X is stored in the bank vault. The set of participants consists the three managers, while the subsets which are able to access the secret are the subsets containing at least two bankers.

In general, we can model secret sharing schemes in the bank vault example. We consider the secret to be locked in a bank vault. Then we divide the key (to the bank vault) into several parts for distribution amongst the participants. Only under some predetermined conditions, then the participants will be able to combine their parts to form a complete key to open the vault. Usually, there are many such subsets of participants which are able to fulfill the conditions. This is because we want the vault to able to be opened even if some part of the key is lost. However, the group of participants must be able to fulfill the conditions.

The most primitive form of secret sharing schemes are threshold schemes. They were independently introduced by Blakley and Shamir. While Shamir borrowed results from polynomial interpolation, Blakley used structures from classical projective geometry. In this chapter, we examine Blakley's scheme. In the following chapters, we make modifications to Blakley's simple scheme to give rise to some interesting properties.

3.1 Definition

But first, we define some terms which we will use to describe a secret sharing scheme.

In any secret sharing scheme, there are individuals who are interested in recreating the secret, and we call them **participants** and each participant is denoted by A_i. There is also the **dealer** D who will distribute information about the secret. The pieces of information are called **shares** or **shadows**, and the share given participant A_i is denoted by X_i. Secrets and shares can be any form, such as numbers, vectors, etc. However, in this report *secrets and shares are subspaces of a projective space*, and the *pooling of information involves finding the span of the shares.*

A group of participants pooling their pieces of information together is called a **constellation**. A secret sharing scheme as defined will restrict the access to the secret to only certain constellations. If a constellation of users can reconstruct the secret, then we call it a **legal** constellation, otherwise a illegal constellation. An **access structure** is then defined to be the family of all legal constellations.

A simple access structure is that of the **threshold schemes** and we have the following definition.

Definition 3.1.1. A t-**threshold scheme** is a secret sharing scheme with the following properties:

- At least t participants are required to reconstruct the secret.
- Any constellation of $t-1$ or fewer participants is illegal.

Remark 3.1.1. The number t is also known as a **quorum**. Hence, the quorum reflects the level of security that the scheme provides. The larger the t, the larger the number of participants required to reconstruct the secret, and hence, the higher the level of security.

Recalling our bank vault example, the key to bank vault is now divided into n (= the number of participants) parts and distributed. If there are t or more participants, they are able to combine their parts to reconstruct the key to access the vault. However, if there are $t-1$ or less parts, the key cannot be reconstructed.

3.2 Blakley's Scheme

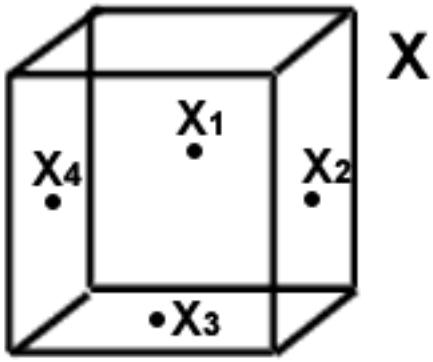
When Blakley solved the problem of sharing secrets, he gave a general construction of a threshold scheme using projective geometry.

Construction.

i. In $\mathbf{PG}(t, q)$, randomly select a hyperplane $\mathbf{X}$ to be the secret.

ii. Choose n points in the hyperplane that are in general position in $\mathbf{X}$. Hence, any t points form a basis for $\mathbf{X}$.

iii. To reconstruct the secret, we simple take the span $\mathbf{U}$ of the participating points and see if $\mathbf{U}$=$\mathbf{X}$.



Blakley's secret sharing scheme

It is obvious that the above construction satisifies the properties of a t-**threshold scheme**. We check that the set of $r \geq t$ points contains the basis for $\mathbf{X}$ and hence span $\mathbf{X}$. Also, if we have less than t points, they cannot form a basis for $\mathbf{X}$ and hence cannot span $\mathbf{X}$.

However, the above scheme is not 100% secure! (In fact, no scheme is!) Even with only one share X_i, an attack may attempt at randomly guessing the hyperplane. But since there are $\frac{q^t-1}{q-1}$ possible hyperplanes containing X_i, his chance of succeeding is $(\frac{q^t-1}{q-1})^{-1}$. This fraction, or the chance that an illegal set of participants can guess the secret correctly, is called the **probability of deception**.

For the Blakley's scheme, if there are $r \leq t-1$ participants cooperating to attack the scheme, the probability of deception is $(\frac{q^{t-r+1}-1}{q-1})^{-1}$ (there are $\frac{q^{t-r+1}-1}{q-1}$ hyperplanes containing the r points). We realise that as r increases, the probability of deception gets higher too. Hence there is an incentive for a illegal group of participants to cooperate. In perfect secret sharing schemes, we want to remove this advantage and we have the following definition.

Definition 3.2.1. A secret sharing scheme is called **perfect** if the probability of deception has the same value for all illegal constellations of participants.

Obviously, the Blakley's scheme is not perfect! Blakley observed this fact and made a modification to his original scheme.

3.3 Perfect Blakley's scheme

Consider this new construction.

Construction.

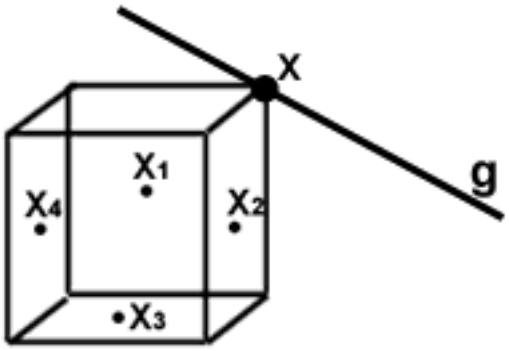
i. In $\mathbf{PG}(t, q)$, randomly select a **point** X to be the secret.

ii. Randomly select a public line g containing X. We call g a public line, as the dealer will announce to all participants that point X is on g.

iii. Select a hyperplane $\mathbf{H}$ such that $\mathbf{H} \cap g = X$.

iv. Choose n points $X_1, X_2, \ldots, X_n$ in $\mathbf{H}$ such that the points $X, X_1, X_2, \ldots, X_n$ are in general position in $\mathbf{H}$.

v. To reconstruct the secret, calculate the span $\mathbf{U}$ of the shares and find $\mathbf{U} \cap g$ and check $\mathbf{U} \cap g = X$.



a perfect Blakley's secret sharing scheme

The above construction indeeds leads to a perfect t-**threshold scheme**.

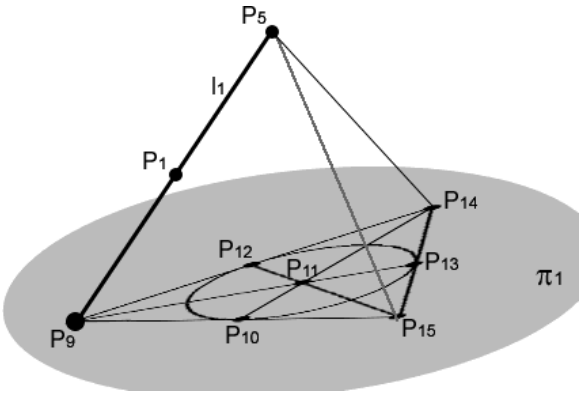
Given any $r \geq t$ shares, the set of r points contain the basis and hence the span $\mathbf{U}$ of the r points is $\mathbf{H}$. Therefore, we obtain the secret X when we intersect $\mathbf{U} = \mathbf{H}$ with g.

Given any $r \leq t-1$ shares, the set of r points cannot span $\mathbf{H}$. Moreover, X is not contained in the span of the r points as they are independent. Hence, the r participants only know that X is on the line g, and X can be any of the $q+1$ points. Therefore, probability of deception is always $(q+1)^{-1}$.

Remark 3.3.1. Let us look at the original scheme. The probability of deception is maximum when $t-1$ participants collude, and it is $(\frac{q^2-1}{q-1})^{-1} = (q+1)^{-1}$. This is equal to the probability of deception in the perfect scheme. This means that we have given the advantage of the group of $t-1$ participants to the each participant. In general, the use of the public line makes secret sharing schemes perfect.

3.4 Example

We look at a 3-**threshold scheme** in $\mathbf{PG}(3, 2)$. (Refer to appendix for $\mathbf{PG}(3, 2)$).



a 3-threshold scheme

We choose the plane π_1 as the secret. And π_1 contains the points P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}.

We choose P_9, P_{10}, P_{11} and P_{12} to be the shares. Note that no three points are collinear and that only three points are needed to construct the plane π_1.

Suppose we make an attack on the scheme without the knowledge of any points, then the chance of succeeding is $\frac{1}{15}$. However, if we know the points P_9 and P_{10}, then there are only three planes containing both P_9 and P_{10} (π_1, π_3, π_{13}). Hence, our chance of success is greatly increased to $\frac{1}{3}$.

Hence, this initial scheme is not perfect.

We make a modification by introducing the public line l_1 which contains P_1, P_5 and P_9 and letting the secret be the point P_9.

Hence, we have P_{10}, P_{11} and P_{12} as our shares. Any knowledge of any point will not be useful, as P_1, P_5 and P_9 are equally likely to be the secret. Hence, our scheme is perfect with the probability of deception to be a constant $\frac{1}{3}$.

3.5 Other schemes

Obviously, the threshold scheme is a very simple form of a secret sharing scheme. Certainly, it is not very realistic in the physical world. In the following chapters, we discuss about modified secret sharing schemes which have interesting properties:

- **compartment schemes** – the participants are divided into subgroups called **compartments**. To obtain the secret, a quorum of compartments is required. But for a compartment to participate in the quorum, *another* quorum of shares is required.
- **multi-level schemes** – the participants are divided into two ordered levels. To reconstruct the secret, a smaller quorum is required in the higher level. Also, each member of a 'higher' level can replace a member of the 'lower' level.
- **schemes with veto-capabilities** – to allow a qualified minority of participants to say 'no' and hence disallowing the quorum to obtain the secret.
- **schemes capable of identifying cheaters** – to allow individual participants to verify that the other participants are honest and are giving their true shares.

Chapter 4

Compartment Schemes

Let us return to the bank vault example. Each manager has a part of the key to the main vault. Suppose each manager keeps their part in a vault in their respective department (we call them department vault). Each manager then divides the key to the department vault into three parts and distribute one part each to an assistant manager. In the absence of the manager, any two assistant manager of the same department will able to reconstruct the key to the department vault, and hence access one part of the key to the main vault. So, if there two departments, each with two assistant manager participating, then the assistant managers are able to access the bank vault.

The above scheme is analagous to our compartment schemes. In general, in compartment schemes, the participants are divided into subgroups called **compartments**. To obtain the secret, a quorum of compartments is required. But for a compartment to participate in the quorum, *another* quorum of shares is required. Hence there are two quorums: 'quorum of compartments' and 'quorum of participants'. We have the formal definition.

4.1 Definition

A $(t, t_1, t_2, \ldots, t_n)$-**compartment scheme** is a secret sharing scheme with the following properties:

- There are n compartments $G_1, G_2, \ldots, G_n$, with G_i having n_i participants.

- For compartment G_i to participate, then t_i out of n_i the participants must take part.
- To reconstruct the secret, then t of the n compartments must participate.

But we construct our schemes to suit the requirements, we introduce the concept of **skew spaces**

4.2 Skew Spaces

Definition 4.2.1. Let $\mathbf{P}$ be a projective space of dimension d.

i. We call a set U of subspaces of $\mathbf{P}$ **skew** if no two distinct subspaces of U have a point in common. We call the subspaces in U **skew subspaces**.

ii. Let U be a set of skew subspaces. A line is called a **transversal** of U if it intersects each subspace in exactly one point.

Lemma 4.2.1. *Let* $\mathbf{P}$ *be a projective space. Let* g_1 *and* g_2 *be two skew lines and denote a point* X *outside* g_1 *and* g_2*. Then there is at most one transversal of* g_1 *and* g_2 *through* X*.*

Proof. Assume there are two transversals h_1,h_2 through X. Each of these transversals meet g_1 and g_2 at distinct points. So h_1 and h_2 span a plane which containes the skew lines g_1 and g_2. Contradiction. □

Theorem 4.2.2. *Let* $U = \{\mathbf{U_1}, \mathbf{U_2}, \ldots \mathbf{U_n}\}$ *be a set of* n *skew subspaces and denote a point* X *outside* U*. Then there is at most one transversal of* U *through* X*.*

Proof. Assume there are two transversals h_1 and h_2 through X. Then h_1 will intersect $\mathbf{U_1}$ and $\mathbf{U_2}$ at Y_1 and Y_2 respectively. Similarly, h_2 will intersect the subspaces at Z_1 and Z_2. But Y_1Z_1 and Y_2Z_2 are two skew lines contained in the plane spanned by h_1 and h_2. Contradiction. □

With this new concept, we look at a simple compartment scheme.

4.3 Basic Example

Let us look at the case where $t = t_1 = t_2 = \ldots = t_n = 2$.

Construction.

i. Randomly choose public line g in $\mathbf{PG}(n+2, q)$.

ii. Randomly choose a point on g to be the secret X.

iii. Pick another line $h \neq g$ such that $h \cap g = X$.

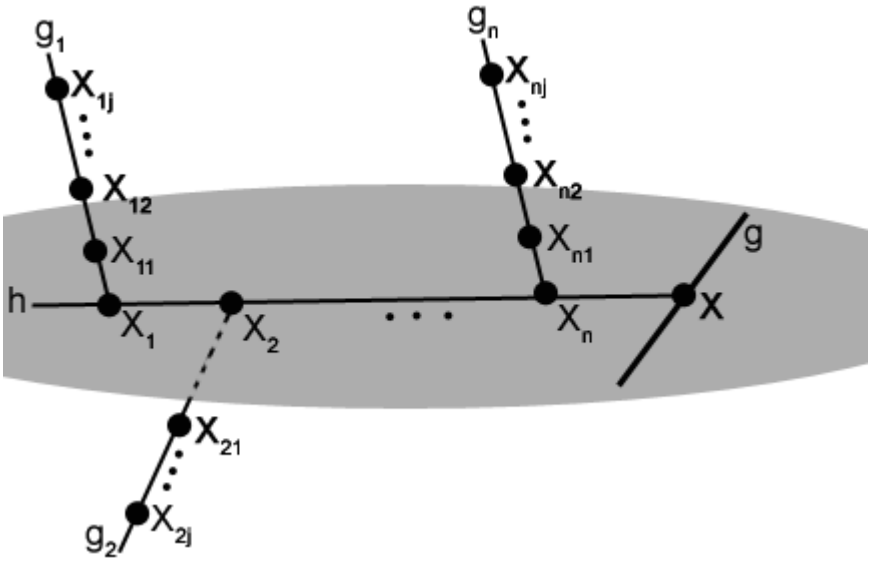
iv. Pick n points $X_1, X_2, \ldots X_n$ on h different from X.

v. Pick n lines $g_1, g_2, \ldots g_n$ in the following manner. For g_1, choose a point Y_1 outside the span of h and g and join X_1 and Y_1 to form g_1. Similarly, for g_i, choose a point Y_i outside $\langle h, g, g_1, \ldots, g_{i-1} \rangle$ and join X_i and Y_i to form g_i. Hence, $\{g, g_1, g_2, \ldots g_n\}$ is a set of independent and mutually skew lines.

vi. On line g_i pick n_i points $X_{i1}, X_{i2}, \ldots, X_{in_i}$ different from X_i.

vii. Point X_{ij} will be allocated as a share to the j-th participant in compartment G_i.

viii. To reconstruct the secret, simply calculate the span $\mathbf{U}$ of the participating shares (points) and compute $\mathbf{U} \cap g$.



Theorem 4.3.1. *The above scheme is indeed a* $(2, 2, 2, \ldots, 2)$**-compartment scheme**.

Proof. First, we show that: given a legal constellation of participants, we indeed get the unique point X by intersecting $\mathbf{U}$ with g.

WLOG, we assume the constellation of participants contribute the points $X_{11}, X_{12}, X_{21}, X_{22}$.

Recalling the definition of subspace, we know that all the points on a line PQ is contained in the subspace if P and Q are in the subspace.

Hence,

$$X_{11} \in \mathbf{U}, X_{12} \in \mathbf{U} \Rightarrow X_1 \in \mathbf{U}$$

$$X_{21} \in \mathbf{U}, X_{22} \in \mathbf{U} \Rightarrow X_2 \in \mathbf{U}$$

$$X_1 \in \mathbf{U}, X_2 \in \mathbf{U} \Rightarrow X \in \mathbf{U}$$

Therefore, since $X \in \mathbf{U}$ and $X \in g$, $X \in (\mathbf{U} \cap g)$.

However, we need to show that the $X = (\mathbf{U} \cap g)$. Assume that is another point $Y \in (\mathbf{U} \cap g)$. Then this implies that $g \subseteq \mathbf{U}$. This contradicts the assumption of the independence of the set $\{g, g_1, g_2\}$.

This proof is not complete. We need to show that an illegal constellation of participants is unable to obtain the secret point X.

From the construction of the scheme, we know the following:

Let $\mathbf{U}' = \langle X_{11}, X_{12}, X_{21}, X_{31}, \ldots, X_{(n-1)1} \rangle$. *Then* $\mathbf{U}'$ *is skew with the line* g_n.

Next, we assume the 'best' situation of an illegal constellation of participants: that is, two shares from the same compartment and one share from the rest of the compartments. WLOG, we assume they are the points:

$$X_{11}, X_{12}, X_{21}, X_{31}, \ldots, X_{n1}.$$

We will show that $X \notin \mathbf{U}'' = \langle X_{11}, X_{12}, X_{21}, X_{31}, \ldots, X_{n1} \rangle$ by contradiction.

Assume that $X \in \mathbf{U}''$. Then there exists a point $Z \in \mathbf{U}'$ such that X, X_{n1}, Z are collinear.

That is, $X_{n1}Z$ is transversal of the skew spaces, $\mathbf{U}'$ and g_n, which passes through X.

But h is another transversal that passes through X and $X_{n1}Z \neq h$. Therefore, contradicting the uniqueness of the transversal. So $X \notin \mathbf{U}''$.

For any 'worse' constellations, we can add shares to obtain the 'best' illegal constellation. It is obvious that the subspace spanned by the 'worse' constellations is a subspace of $\mathbf{U}''$. Hence, X will neither be contained in the 'worse' subspaces. □

Example 4.3.1. Here we show an example of a $(2, 2, \ldots, 2)$-**compartment scheme** with n compartments in $\mathbf{PG}(n+2, q)$.

First let e_i denote a unit vector with 1 at the i-th coordinate and 0 otherwise. That is,

$$e_i = (\underbrace{0, 0, \ldots, 0}_{(i-1)zeroes}, 1, 0, \ldots, 0)$$

Choose the public line $g = \langle e_{n+1}, e_{n+3} \rangle$ and point X as the secret where $X = \langle e_{n+3} \rangle$.

Let

$$h = \langle e_{n+2}, e_{n+3} \rangle$$

and

$$X_i = \langle e_{n+2} + i\, e_{n+3} \rangle$$

and

$$g_i = \langle e_i, e_{n+2} + i\, e_{n+3} \rangle$$

It is not difficult to check that $g, g_1, g_2, \ldots, g_n$ are mutually skew. Hence, let

$$X_{ij} = \langle j\, e_i + e_{n+2} + i\, e_{n+3} \rangle$$

Suppose that we have a legal constellation of shares, that is, the span of the points contain at least two lines, say g_r and g_s. It is easy to check that $X = \langle e_{n+3} \rangle \subseteq \langle g_r, g_s \rangle$.

$$\begin{aligned}\langle g_r, g_s\rangle &= \langle\, \langle e_r, e_{n+2} + r\, e_{n+3}\rangle, \langle e_s, e_{n+2} + s\, e_{n+3}\rangle\, \rangle \\ &= \langle e_r, e_{n+2} + r\, e_{n+3}, e_s, e_{n+2} + s\, e_{n+3}\rangle\end{aligned}$$

Hence, any vector is of the form,

$$\lambda_1\, e_r + \lambda_2\, (e_{n+2} + r\, e_{n+3}) + \lambda_3\, e_s + \lambda_4\, (e_{n+2} + s\, e_{n+3})$$

Let $\lambda_1 = \lambda_3 = 0,\ \lambda_2 = \lambda,\ \lambda_4 = -\lambda$.

Then $\langle g_r, g_s\rangle$ contains vectors of the form, $\lambda\, (r - s)\, e_{n+3}$.
That is, $X = \langle e_{n+3}\rangle$ belongs to span of g_r and g_s.

As above, let us check that $X \notin \mathbf{U}'' = \langle X_{11}, X_{12}, X_{21}, X_{31}, \ldots, X_{n1}\rangle$.

Observe

$$\mathbf{U}'' = \langle e_1,\ e_{n+2} + e_{n+3},\ e_2 + e_{n+2} + 2\, e_{n+3}, \ldots,\ e_n + e_{n+2} + n\, e_{n+3}\rangle$$

We see that the vectors of $\mathbf{U}''$ are of the form:

$$\lambda_1\, e_1 + \lambda_2\, (e_{n+2} + e_{n+3}) + \lambda_3\, (e_2 + e_{n+2} + 2\, e_{n+3}) + \ldots + \lambda_{n+1}\, (e_n + e_{n+2} + n\, e_{n+3}).$$

Since $X = \langle e_{n+3}\rangle$, then obviously

$$\lambda_1 = \lambda_3 = \ldots = \lambda_n = 0$$

hence,

$$\text{vectors are of the form: } \lambda_2\, (e_{n+2} + e_{n+3}) \notin \langle e_{n+3}\rangle$$

Therefore, $X \notin \mathbf{U}''$

4.4 General Construction

We have the following general construction for a $(t, t_1, t_2, \ldots, t_n)$-**compartment scheme**. The proof will be similar to that above and will not be shown.

Construction.

i. Randomly choose public line g in $\mathbf{PG}(t + t_1 + t_2 + \ldots + t_n - n, q)$.

ii. Randomly choose a point on g to be the secret X.

iii. Pick a $(t-1)$-dimensional subspace $\mathbf{H}$ such that $\mathbf{H} \cap g = X$.

iv. Pick n points $X_1, X_2, \ldots X_n$ in h such that the points in $\{X, X_1, X_2, \ldots, X_n\}$ are in general position in $\mathbf{H}$.

v. Pick n subspaces $\mathbf{G_1}, \mathbf{G_2}, \ldots \mathbf{G_n}$ such that $dim(G_i) = t_i - 1$ in the following manner. For $\mathbf{G_1}$, choose a set of $t_1 - 1$ points $\mathcal{Y}_\infty$ outside the span of $\mathbf{H}$ and g such that $\mathbf{G_1} = \langle \mathcal{Y}_1, X_1 \rangle$ forms a $t_1 - 1$-dimensional subspace. Similarly, for $\mathbf{G_i}$, choose a set of $t_i - 1$ points $\mathcal{Y}_i$ outside $\langle g, \mathbf{H}, \mathbf{G_1}, \mathbf{G_2}, \ldots, \mathbf{G_{i-1}} \rangle$ such that $\mathbf{G_i} = \langle \mathcal{Y}_i, X_i \rangle$ forms a $t_i - 1$-dimensional subspace. Hence, $\{g, \mathbf{G_1}, \mathbf{G_2}, \ldots, \mathbf{G_{i-1}}\}$ is a set of independent and mutually skew lines.

vi. In the subspace $\mathbf{G_i}$ pick s_i points $X_{i1}, X_{i1}, \ldots, X_{is_i}$ such that the points in $\{X_i, X_{i1}, X_{i1}, \ldots, X_{is_i}\}$ are in general position in $\mathbf{G_i}$.

vii. Point X_{ij} will be allocated as a share to the j-th participant in compartment G_i.

viii. To reconstruct the secret, calculate the span $\mathbf{U}$ of the participating shares (points) and compute $\mathbf{U} \cap g$.

Chapter 5

Multi-level Schemes

In the previous chapter, although the bank company is divided into departments, there are no hierachies. In this new scheme, called multi-level scheme, we divide the participants into two groups, or rather, two ordered levels. Naturally, to reconstruct the secret, a smaller quorum is required in the higher level. Also, each member of a 'higher' level can replace a member of the 'lower' level. In the bank example, the company is now divided into two levels, one 'senior' and one 'executive' . The parts of the key are distributed in a manner such that: 2 members from the senior level can construct the key, while 3 members from the executive level are needed to reconstruct the key. We can imagine the senior management as getting bigger parts of the key. This also implies that 1 member from the senior level and 2 from the executive level can construct the key.

We define multi-level schemes formally.

5.1 Definition

A (s, t)-**multi-level scheme**$(s < t)$ is a secret sharing scheme with the following properties:

- There are two disjoint sets of participants, $\mathcal{A}$ and $\mathcal{B}$, with n_1 and n_2 participants respectively.
- At least s shares from $\mathcal{A}$ are required to reconstruct the secret.

- At least t shares from $\mathcal{B}$ are required to reconstruct the secret.
- Let $r < s$. r shares from $\mathcal{A}$ and at least $t-r$ shares from $\mathcal{B}$ are required to reconstruct the secret.

5.2 Basic example

Let us consider $s = 2$.

Construction.

i. Randomly choose public line g in $\mathbf{PG}(t, q)$.

ii. Randomly choose a point on g to be the secret X.

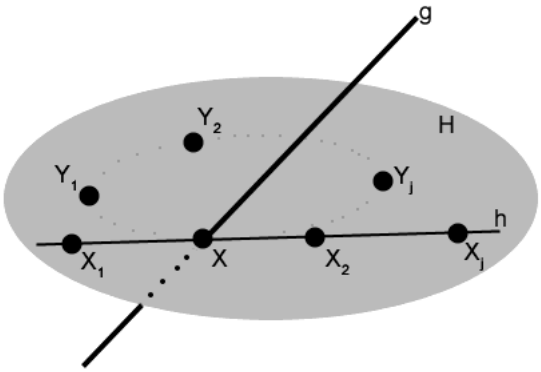
iii. Pick another line $h \neq g$ such that $h \cap g = X$.

iv. Pick a hyperplane $\mathbf{H}$ containing h such that $\mathbf{H} \cap g = X$.

v. Pick n_2 points $Y_1, Y_2, \ldots Y_{n_2}$ on $\mathbf{H}$ such that $X, Y_1, Y_2, \ldots Y_{n_2}$ are points in general position in $\mathbf{H}$. They will be allocated as shares to participants in $\mathcal{B}$.

vi. Pick n_1 points $X_1, X_2, \ldots, X_{n_1}$ on h such that $X_i, X, Y_1, Y_2, \ldots Y_{n_2}$ $(i = 1, 2, \ldots, n_1)$ are points in general position in $\mathbf{H}$. They will be allocated as shares to participants in $\mathcal{A}$.

vii. To reconstruct the secret, simply calculate the span $\mathbf{U}$ of the participating shares (points) and compute $\mathbf{U} \cap g$.



Theorem 5.2.1. *The construction leads to a* $(2,t)$-**multi-level scheme**.

Proof. If the constellation is legal, we have the following cases:

Case 1. At least 2 shares from set $\mathcal{A}$. These points will span h and hence, $h \cap g = X$. Therefore, we obtain the secret.

Case 2. At least t shares from set $\mathcal{B}$. There exist t points that will span $\mathbf{H}$ and $\mathbf{H} \cap g = X$. Therefore, we obtain the secret.

Case 3. $(t-1)$ shares from $\mathcal{B}$ and 1 share X_j from $\mathcal{A}$. These t points are contained $\{X_j, X, Y_1, Y_2, \ldots Y_{n_2}\}$. Hence, the t shares span $\mathbf{H}$ and we obtain $X = \mathbf{H} \cap g$.

If the constellation is illegal, we have the following two cases:

Case 4. 1 share X_j from $\mathcal{A}$ and at most $(t-2)$ shares in $\mathcal{B}$. Let the span of the shares be $\mathbf{U}$. If $X \in \mathbf{U}$, then this contradicts the independence of $\{X_j, X, Y_1, Y_2, \ldots Y_{n_2}\}$.

Case 5. At most $(t-1)$ shares from $\mathcal{B}$. Similarly, X is not contained in the span, otherwise, we contradict the independence of $\{X, Y_1, Y_2, \ldots Y_{n_2}\}$. □

Example 5.2.1. Here we show an example of a $(2,3)$-**multi-level scheme** in $\mathbf{PG}(3,11)$.

We select the public line $g = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $X = (0,0,1,0)$ to be the secret.

Allocate the participants from $\mathcal{A}$ the shares:

$X_1 = (0,1,0,0) \quad X_2 = (0,1,1,0) \quad X_3 = (0,1,2,0) \quad X_4 = (0,1,10,0)$

Allocate the participants from $\mathcal{B}$ the shares:

$Y_1 = (1,1,1,0) \quad Y_2 = (1,2,4,0) \quad Y_3 = (1,3,9,0) \quad Y_4 = (1,4,5,0) \quad Y_5 = (1,5,3,0)$

Let us check:

If we have 2 participants, X_1,X_2, from $\mathcal{A}$, then

$$X_1X_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

We check that $X_1X_2 \cap g = (0, 0, 1, 0) = X$.

If we have 3 participants, Y_1,Y_2,Y_3, from $\mathcal{B}$, then

$$\langle Y_1, Y_2, Y_3\rangle = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 4 & 0 \\ 1 & 3 & 9 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

We check that $\langle Y_1, Y_2, Y_3\rangle \cap g = (0, 0, 1, 0) = X$.

If we have 1 participants, X_3, from $\mathcal{A}$, and 2 participants, Y_4,Y_5, from $\mathcal{B}$, then

$$\langle X_3, Y_4, Y_5\rangle = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 4 & 5 & 0 \\ 1 & 5 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Also, $\langle X_3, Y_4, Y_5\rangle \cap g = (0, 0, 1, 0) = X$.

5.3 General Construction

Construction.

i. Randomly choose public line g in $\mathbf{PG}(t, q)$.

ii. Randomly choose a point on g to be the secret X.

iii. Pick a $(s-1)$-dimensional subspace $\mathbf{H_A}$ such that $\mathbf{H_A} \cap g = X$.

iv. Pick a hyperplane $\mathbf{H_B}$ such that $\mathbf{H_A} \subseteq \mathbf{H_B}$ and $\mathbf{H_B} \cap g = X$.

v. Pick the set $\mathcal{B}$ of n_1 points(shares) $Y_1, Y_2, \ldots Y_{n_2}$ in $\mathbf{H}\backslash\mathbf{H_A}$ such that $\{X\} \cup \mathcal{B}$ are points in general position in $\mathbf{H_B}$.

vi. Pick the set $\mathcal{A}$of n_2 points $X_1, X_2, \ldots, X_{n_1}$ on h such that $\{X\} \cup \mathcal{A}$ are points in general position. In addition, for any subset $\mathcal{A}'$ of $(s-1)$ elements in $\mathcal{A}$, $\{X\} \cup \mathcal{A}' \cup \mathcal{B}$ are points in general position in $\mathbf{H_B}$.

vii. To reconstruct the secret, simply calculate the span $\mathbf{U}$ of the participating shares (points) and compute $\mathbf{U} \cap g$.

It is not difficult to check that the above scheme satisfies the properties of a (s, t)-**multi-level scheme**.

Chapter 6

Veto Capabilities

In the conventional t-**threshold scheme**, if a certain t number of participants decide to say 'yes', then they are able to retrieve the secret. However, in many practical situation, it may be more advisable to allow a qualified minority of participants to say 'no' and hence disallowing the t participants to obtain the secret. The ability to say 'no' can be described as the right to veto.

Consider the bank company. The boss may have a special key and divide into three parts and distribute one part each to the three most senior members in the company. Any two of the parts can be reconstructed to form the special key, while this special key can overwrite the normal key and lock the vault. Therefore, even if all the employers pool their keys together and reconstruct a key, they are unable to access the vault. Hence, the boss rely on the three senior members to keep things in check. The special key of the three senior members hence represents their right to veto.

6.1 Definition

A (s, t)-**veto scheme** is a secret sharing with the following properties:

- There are two disjoint sets of shares, $\mathcal{X}$ and $\mathcal{Y}$.
- If there are at least s shares from $\mathcal{X}$ and at most $t-1$ shares from $\mathcal{Y}$, the secret can be reconstructed.

- If there are at most $s-1$ shares from $\mathcal{X}$, the secret cannot be reconstructed.
- If there are at least t shares from $\mathcal{Y}$, the secret cannot be reconstructed.

The shares from $\mathcal{X}$ can be thought of as the the shares saying 'yes', and the shares from $\mathcal{Y}$ as those shares saying 'no'.

6.2 Basic Example

Let us consider $s = t = 2$.

Construction.

i. Randomly choose public line g in $\mathbf{PG}(3, q)$

ii. Randomly choose a point on g to the secret X.

iii. Pick another line $h \neq g$ such that $h \cap g = X$.

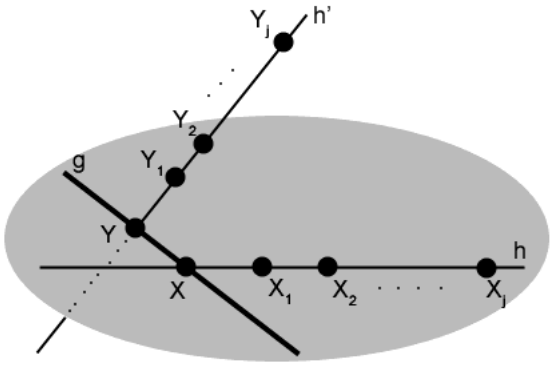
iv. Choose distinct points $X_1, X_2, \ldots$ on h and allocate them as shares in $\mathcal{X}$.

v. Pick another point $Y \neq X$ on g.

vi. Pick a line h' not contained in the plane $\langle g, h \rangle$ and skew to h such that $h' \cap g = Y$.

vii. Choose distinct points $Y_1, Y_2, \ldots$ on h' and allocate them as shares in $\mathcal{Y}$.

viii. To reconstruct the secret, calculate the span $\mathbf{U}$ of the participating points and compute $\mathbf{U} \cap g$.



a $(2, 2)$-veto scheme

Theorem 6.2.1. *The construction leads to a* $(2, 2)$-**veto scheme**.

Proof. Looking at the possible cases:

Case 1. If there are at least 2 shares from $\mathcal{X}$ and 0 share from $\mathcal{Y}$, then $\mathbf{U} = h$ and $h \cap g = X$.

Case 2. If there are at least 2 shares from $\mathcal{X}$ and 1 share P from $\mathcal{Y}$, then $\mathbf{U} = \langle h, P \rangle$ and hence $X \in \mathbf{U}$. But Y is not contained $\mathbf{U}$, otherwise, YP and h are two skew lines contained in the same plane. Therefore, $\mathbf{U}$ intersect g at X only.

Case 3. If there are at least 2 shares from $\mathcal{X}$ and at least 2 shares from $\mathcal{Y}$, then $\mathbf{U}$ contains both skew lines h and h'. Hence, $\mathbf{U}$ is the whole space and $\mathbf{U} \cap g = g$, and the participants cannot get the secret.

Case 4. If there are at most 1 share from $\mathcal{X}$ and at least 2 shares from $\mathcal{Y}$, then by similar arguments in Case 1 and Case 2, $\mathbf{U} \cap g = Y \neq X$. This means that they reconstruct another point which is not the secret.

Case 5. If there are at most 1 share from $\mathcal{X}$ and at most 1 share P from $\mathcal{Y}$, it is obvious that there will be no intersection between $\mathbf{U}$ and g. □

6.3 General Construction

Construction.

i. Randomly choose public line g in $\mathbf{PG}(s+t-1, q)$

ii. Randomly choose a point on g to the secret X.

iii. Pick a $(s-1)$-dimensional subspace $\mathbf{H_X}$ not containing g such that $\mathbf{H_X} \cap g = X$.

iv. Choose distinct points $X_1, X_2, \ldots$ in $\mathbf{H_X}$ such that $X, X_1, X_2, \ldots$ are in general position in $\mathbf{H_X}$. Allocate points $X_1, X_2, \ldots$ as shares in $\mathcal{X}$.

v. Pick another point $Y \neq X$ on g.

vi. Pick a $(t-1)$-dimensional subspace $\mathbf{H_Y}$ not containing g and skew to $\mathbf{H_X}$ such that $\mathbf{H_Y} \cap g = Y$.

vii. Choose distinct points $Y_1, Y_2, \ldots$ on $\mathbf{H_Y}$ such that $Y, Y_1, Y_2, \ldots$ are in general position in $\mathbf{H_Y}$. Allocate points $Y_1, Y_2, \ldots$ as shares in $\mathcal{Y}$.

viii. To reconstruct the secret, calculate the span $\mathbf{U}$ of the participating points and compute $\mathbf{U} \cap g$.

Theorem 6.3.1. *The construction leads to a* (s,t)-**veto scheme**.

Proof. First, we note the following:

- points in $\mathcal{X} \cup \{X\}$ are in general position in $\mathbf{H_X}$. This implies that any s points span $\mathbf{H_X}$ and X is not in the span of $k < s$ other points.
- points in $\mathcal{Y} \cup \{Y\}$ are in general position in $\mathbf{H_Y}$. This implies that any t points span $\mathbf{H_Y}$ and Y is not in the span of $k < t$ other points.
- points in $\mathcal{Y} \cup \mathcal{X} \cup \{X, Y\}$ are in general position in $\mathbf{PG}(s+t-1, q)$. This implies that any $s+t$ points span $\mathbf{PG}(s+t-1, q)$, and any point is not in the span of $k < s+t$ other points.

Let us divide into cases.

Case 1. If there are at most $s-1$ shares from $\mathcal{X}$, then clearly, X is not contained in the span $\mathbf{U}$. Hence, the secret cannot be reconstructed.

Case 2. If there are at least t shares from $\mathcal{Y}$, then $\mathbf{H_Y}$ is contained in $\mathbf{U}$. Therefore, $Y \in \mathbf{U}$ which means that either we reconstruct the incorrect secret Y or we obtained the public line g.

Case 3. If there are at least s shares from $\mathcal{X}$ and at most $(t-1)$ shares from $\mathcal{Y}$, then $X \in \mathbf{H_X} \subseteq \mathbf{U}$. g is not contained in $\mathbf{U}$, or otherwise $Y \in \mathbf{U}$ contradicts the fact that $\mathcal{Y} \cup \mathcal{X} \cup \{X, Y\}$ are in general position in $\mathbf{PG}(s+t-1, q)$. Therefore, we reconstruct the unique intersection point X. □

Example 6.3.1. Here we show an example of a (s,t)-**veto scheme**.

We adopt the following notation: I_k to be a $k \times k$ indentity matrix and O to be the zero matrix.

Let

$$X = (\underbrace{1, 1, \ldots, 1}_{s \text{ one's}}, 0, \ldots, 0) \quad \text{and} \quad Y = (0, 0, \ldots, 0, \underbrace{1, 1, \ldots, 1}_{t \text{ one's}})$$

Hence the public line $g = \begin{pmatrix} 1 & 1 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 1 & 1 & \ldots & 1 \end{pmatrix}$.

We choose $\mathbf{H_X}$ and $\mathbf{H_Y}$ to be the following skew subspaces:

$$\mathbf{H_X} = (I_s, O) \quad \mathbf{H_Y} = (O, I_t)$$

Let the points $X_1, X_2, \ldots$ in $\mathcal{X}$ be distinct points(distinct from X) on the normal rational curve in $\mathbf{H_X}$. That is, X_i is of the form

$$X_i = (1, \lambda_i, \lambda_i^2, \ldots, \lambda_i^{(s-1)}, 0, \ldots, 0) \text{ where } \lambda_i \in F_q \text{ and } \lambda_i \neq 1.$$

Similarly, we let the points $Y_1, Y_2, \ldots$ in $\mathcal{Y}$ to be the distinct points Y_i to be of the form:

$$Y_i = (0, \ldots, 0, 1, \mu_i, \mu_i^2, \ldots, \mu_i^{(t-1)}) \text{ where } \mu_i \in F_q \text{ and } \mu_i \neq 1.$$

Consider the case when there are s participants saying 'yes' and $k(< t)$ participants saying 'no'. WLOG, let the participants be $X_1, X_2, \ldots, X_s$ and $Y_1, Y_2, \ldots, Y_k$.

First,

$$\langle X_1, X_2, \ldots, X_s \rangle = \begin{pmatrix} 1 & \lambda_1^2 & \ldots & \lambda_1^{s-1} & 0 & 0 & \ldots & 0 \\ 1 & \lambda_2^2 & \ldots & \lambda_2^{s-1} & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_s^2 & \ldots & \lambda_s^{s-1} & 0 & 0 & \ldots & 0 \end{pmatrix} = (I_s, O)$$

We note the second equality follows from the fact that the $Vandermonde$ determinant of $\begin{pmatrix} 1 & \lambda_1^2 & \ldots & \lambda_1^{s-1} \\ 1 & \lambda_2^2 & \ldots & \lambda_2^{s-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_s^2 & \ldots & \lambda_s^{s-1} \end{pmatrix}$ is non-zero and hence we can reduce $\begin{pmatrix} 1 & \lambda_1^2 & \ldots & \lambda_1^{s-1} \\ 1 & \lambda_2^2 & \ldots & \lambda_2^{s-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_s^2 & \ldots & \lambda_s^{s-1} \end{pmatrix}$ to the identity matrix.

However,

$$\langle Y_1, Y_2, \ldots, Y_k \rangle = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 & \mu_1^2 & \ldots & \mu_1^{t-1} \\ 0 & 0 & \ldots & 0 & 1 & \mu_2^2 & \ldots & \mu_2^{t-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 1 & \mu_k^2 & \ldots & \mu_k^{t-1} \end{pmatrix} = (O, A)$$

We note the following: if we add rows representing $Y, Y_{k+1}, \ldots, Y_{t-1}$ to (O,A), we get a $t \times (s+t)$ matrix (O,A'). Furthermore, A' has a non-zero $Vandermonde$ determinant. Hence the rows of A' or (O,A') are linearly independent. This means that $Y \notin \langle Y_1, Y_2, \ldots, Y_k \rangle$ or $(\underbrace{1, 1, \ldots, 1}_{t}) \notin A$.

Hence,

$$\mathbf{U} = \langle X_1, X_2, \ldots, X_s, Y_1, Y_2, \ldots, Y_k \rangle = \begin{pmatrix} I_s & O \\ O & A \end{pmatrix}$$

Now any point on the line g is either the point $Y = (0, 0, \ldots, 0, \underbrace{1, 1, \ldots, 1}_{t \text{ one's}})$, or of the form $(\underbrace{1, 1, \ldots, 1}_{s}, \underbrace{\nu, \nu, \ldots, \nu}_{t})$.

We consider the last t coordinates. From above, we know that $(\underbrace{1, 1, \ldots, 1}_{t})$, or equivalently $(\underbrace{\nu, \nu, \ldots, \nu}_{t})$, cannot be formed by any linear combination of

the rows in A. Therefore the last t coordinates of the intersection of g and $\mathbf{U}$ are zero.

Hence, the only possible intersection is the point $X = (1, 1, \ldots, 1, 0, 0, \ldots, 0)$.

If we have s participants $X_1, X_2, \ldots, X_s$ saying 'yes' and t participants $Y_1, Y_2, \ldots, Y_t$ saying 'no', then

$$\langle X_1, X_2, \ldots, X_s \rangle = \begin{pmatrix} 1 & \lambda_1^2 & \ldots & \lambda_1^{s-1} & 0 & 0 & \ldots & 0 \\ 1 & \lambda_2^2 & \ldots & \lambda_2^{s-1} & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \lambda_s^2 & \ldots & \lambda_s^{s-1} & 0 & 0 & \ldots & 0 \end{pmatrix} = (I_s, O)$$

and

$$\langle Y_1, Y_2, \ldots, Y_t \rangle = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 & \mu_1^2 & \ldots & \mu_1^{t-1} \\ 0 & 0 & \ldots & 0 & 1 & \mu_2^2 & \ldots & \mu_2^{t-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 1 & \mu_k^2 & \ldots & \mu_t^{t-1} \end{pmatrix} = (O, I_t).$$

So,

$$\mathbf{U} = \langle X_1, X_2, \ldots, X_s, Y_1, Y_2, \ldots, Y_t \rangle = \begin{pmatrix} I_s & O \\ O & I_t \end{pmatrix} = I_{s+t}$$

which is the whole space! Hence the intersection of g with $\mathbf{U}$ is the entire line g. That is, the secret is any of the $q + 1$ points on g.

Using the same methods, we also notice that if there are $k(k < s)$ participants saying 'yes' and t participants saying 'no' then we obtain the intersection point Y. Hence, the secret can be any of the $q(= q + 1 - 1)$ points.

We observe something ironic. Suppose there are s participants who wants to obtain the secret X but they know that they would face opposition from t other members. Then it would be better for less of the s 'yes' members to take part, since $q^{-1} > (q+1)^{-1}$! That is, they can eliminate the point Y as a possible secret. But we can avoid the problem by choosing a large q so that there is no significant difference between the two values.

6.4 Problem of Privacy

We return to the simplest form, a $(2, 2)$-**veto scheme** with only two members A and B. We give the shares X_1,Y_1 to A and X_2,Y_2 to B. Hence, both participants have the power to vote 'for' or 'against' to access the secret.

Consider the following cases:

Case 1. A and B wants the secret. Then the intersection $X_1X_2 \cap g = X$.

Case 2. A and B do not want the secret. Then the intersection $Y_1Y_2 \cap g = Y$.

Case 3. A wants the secret but B does not. Then the intersection $X_1Y_2 \cap g = \emptyset$.

Hence, by looking at the final computation result (whether the intersection is X or Y or neither), both A and B are now aware of each other's intentions.

We can compare with our threshold scheme. In 2-**threshold scheme**, we give shares X_1 to A and X_2 to B.

Similarly, consider the following:

Case 1. A and B wants the secret. Then the intersection $X_1X_2 \cap g = X$.

Case 2. A and B do not want the secret. Then the intersection $\emptyset \cap g = \emptyset$.

Case 3. A wants the secret but B does not. Then the intersection $X_1 \cap g = \emptyset$.

Here, we see no difference between the computation results of case 2 and case 3. That is, if there are no intersection of the shares with g, A and B will not be aware of each other's intention.

There is yet another simple protocol which keeps the decisions of both A and B private.

If A wants the secret, he will feed '1' to computer. Otherwise, he will feed '0'. Let a be the value A inputted. Similar for B and let b be the value B inputted. Now the computer computes $a \times b$ and shows the results.

We do a similar analysis:

Case 1. A and B wants the secret. Then the result is $1 \times 1 = 1$.

Case 2. A and B do not want the secret. Then the the result is $0 \times 0 = 0$.

Case 3. A wants the secret but B does not. Then the the result is $1 \times 0 = 0$.

We cannot differentiate between the last two cases, and hence we have respected the privacy of both A and B decisions.

Chapter 7

Identifying Cheaters

In the previous chapters, we have always assumed that the vault is only accessible by the constructed key. However, in the real world, there are other illegal means to open the vault (for example, getting engineers). So is there any guarantee that the vault cannot via illegal means? Of course not. However, one way to deter illegal entry is to create redundant vaults which contain false information. So even if the intruder breaks open all the vaults, he is unable to infer which information is true.

Let us look at this method in the light of a t-**threshold** scheme. We know that each of the $q+1$ points on the public line is equally possible to be the secret point. That is, there are $q+1$ possible keys $K_0, K_1, \ldots, K_q$ which can be constructed. We hence create $q+1$ vaults (of which q are redundant) $V_0, V_1, \ldots, V_q$ such that K_i $(0 \leq i \leq q)$ only opens V_i.

Suppose V_X is the vault containing the secret and K_X is the corresponding key. Assuming all t participants are honest, then the computed $\mathbf{U} \cap g$ will yield the corresponding key K_X to open V_X to obtain the secret.

What if one participant is dishonest and lies about his point? Suppose the new computed $\mathbf{U} \cap g$ yields the corresponding key K_Y $(Y \neq X)$. Then the honest participants will open V_Y and believe that the information behind the vault to be true. This means that by having the redundant vaults, we have allowed the dishonest participants to deceive the rest.

The essential difference between the the two schemes is that there exists a verifying mechanism in the former. In the usual t-**threshold** scheme, the computer will verify if $\mathbf{U} \cap g = X$, or the participants can test the key by

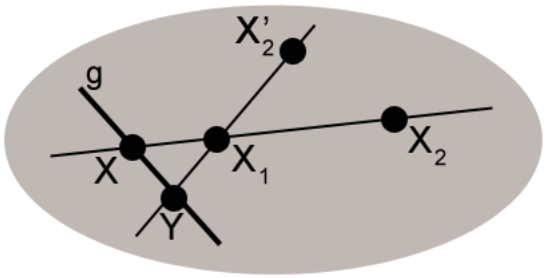
attempting to open the one vault. In the second scheme, the participants are unable to do so. Any key can be used to open one corresponding door.

Let us illustrate this again.

Consider a simple 2-**threshold scheme** with only 2 participants, A and B. We give the points/shares X_1 to A and X_2 to B.

If A and B are honest and provide each other the correct information, then $\mathbf{U} = X_1X_2$ intersects g at X and they obtain the secret.

Suppose B is not interested in the secret and wants A to believe that another point is the secret. If B gives A the point X', then $\mathbf{U} = X_1X_2'$ and the intersection point is Y. Then A will hence believe that Y is the actual secret and B has sucessfully deceived A.



B cheats in a 2-threshold scheme

In [8], Brickell and Stimson presents a modification of Blakley's threshold scheme which gives honest participants the ability to *identify* cheaters. The scheme was proposed in an affine setting. In this report, the author has modified the scheme for the projective setting. The basic concept is to include another verifying mechanism. This mechanism will enable participants to check the honesty of each other.

7.1 Basic Example

First, we will look at a 2-**threshold scheme** with the ability to identify cheaters.

Construction.

i. In $\mathbf{PG}(2, q)$, randomly select a **point** X to be the secret.

ii. Randomly select a public line g containing X.

iii. Select a line h such that $h \cap g = X$.

iv. Choose n distinct points $X_1, X_2, \ldots, X_n$ on h.

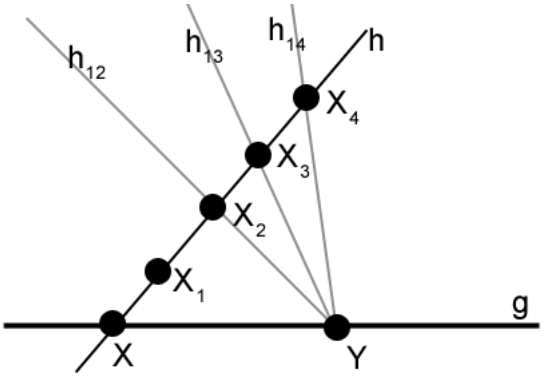
v. Choose n (not necessarily distinct) points $Y_1, Y_2, \ldots, Y_n$ on g.

vi. Let the lines h_{ij} (where $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$ and $i \neq j$) be the lines $Y_i X_j$.

vii. Give participant A_i, his share X_i and the supershares $h_{i1}, h_{i2}, \ldots, h_{in}$ $(i \neq j)$.

viii. To reconstruct the secret, calculate the span $\mathbf{U}$ of the shares and find $\mathbf{U} \cap g$.

ix. To check the 'honesty' of another participant A_j, A_i checks if the point(share) given by A_j is on the line h_{ij}.



2-threshold scheme capable of identifying cheaters

We verify that the above scheme is still a 2-**threshold scheme** even with the inclusion of the supershares. Indeed, from the above disgram, any one participant A_i is unable to infer any other share other than his own share X_i. He only know that the shares lie on the supershares h_{ij} given to him. However, A_i knows that the point Y_i on g cannot be the secret X. Therefore, he eliminates one possibility and we see that the scheme is not *perfect* anymore.

Next, we observe that the new scheme is not 100% cheater–proof. If A_2 decides to cheat A_1 and tells A_1 that the former's share is a point which (incidentally) lie on h_{12}, then A_1 will be deceived. Hence, there is a need for us to find the chance of such an occurence.

WLOG, we assume $A_2, A_3, \ldots, A_{m+1}$ attempt to cheat A_1.

Consider the case $m \geq 2$. We observe that since $m \geq 2$ the m cheaters are able to obtain the points X and X_1. Specifically, $X = X_2X_3 \cap g$ and $X_1 = h_{21} \cap h_{31}$.

If A_2 tries to cheat A_1, he will not choose any point on g (obviously), nor any point on the line h (since the point is to not let A_1 obtain X). Therefore, A_2 has $q^2 - q$ $(= (q^2 + q + 1) - (q + 1) - (q + 1) + 1)$ points to choose from.

Let A_2 choose the point X_2'.

Then A_2 succeeds in deceiving A_1 iff $X_2'X_2 = h_{12}$.

There are $q + 1$ lines passing through X_2 but h is not part of the choice. The remaining q lines each contains $q - 1$ possible cheating points.

Therefore, the chance of A_2 successfully cheating A_1 is $\frac{1}{q}$.

Now, alternatively, let Y_{12}' be the intersection of $X_2'X_2$ with g. We see that A_2 successfully deceives iff $Y_{12}' = Y_1$. There are q choices of Y_{12}' on g (excluding point X) and hence the probability is $\frac{1}{q}$.

Let us consider the coalition of m cheaters. Suppose A_2 attempts to deceive A_1 and chooses the point X_2'. Let $Y_{12}' = X_2'X_2 \cap g$. If A_2 fails at deceiving A_1, then $Y_{12}' \neq Y_1$. Then when A_3 attempts to deceive A_1, he will NOT choose any point on $Y_{12}'X_3$. Instead, he will choose a point X_3' such that $Y_{13}' = X_3'X_3 \cap g \neq Y_{12}'$.

Hence, let us similarly define the point $Y'_{1j} = X'_j X_j \cap g$ where X'_j is the point A_j chooses to cheat. To maximise their collective chance of successfully cheating A_1, the m cheaters would choose $Y'_{12}, Y'_{13}, \ldots, Y'_{1(m+1)}$ to be m distinct points on g. Hence, their chance of succeeding by cooperating is $\frac{m}{q}$.

Consider the case $m = 1$. Then A_2 is unable to obtain the point X and hence has to choose any of the $q + 1$ points on g to be Y'_{12}. Therefore the chance of succeeding is reduced to $\frac{1}{q+1}$.

We observe that the chances of succeeding are either $\frac{m}{q}$ or $\frac{1}{q+1}$. By using a large q, the chance of success is made as small as required.

7.2 General Position

Before generalising our method to any t-**threshold schemes**, let us examine the notion of *general position*.

We recall that:

In a projective space $\mathbf{P}$ of dimension d, a set $\mathcal{U}$ of at least $d + 1$ points is in *general position* if any $d + 1$ points of $\mathcal{U}$ form a basis for $\mathbf{P}$. This implies that we have no $d + 1$ points lie in the same hyperplane.

One important property of $\mathcal{U}$ is that: for any n $(0 \leq n \leq d)$, any $n + 1$ points of $\mathcal{U}$ span a projective space of dimension n.

Consider the dual of this definition (replacing 'points' with 'hyperplanes'). It is:

In a projective space $\mathbf{P}$ of dimension d, a set $\mathcal{U}'$ of at least $d+1$ hyperplanes is in *general position* if any $d + 1$ hyperplanes of $\mathcal{U}'$ have no common point of intersection.

Moreover, for any n $(0 \leq n \leq d)$, any $n + 1$ hyperplanes of $\mathcal{U}'$ intersect in a projective subspace of dimension $d - n - 1$.

In general, it is simple to derive from a set $\mathcal{U}$ of points in general position a set $\mathcal{U}'$ of hyperplanes which are also in general position. Indeed, for each point X_i in $\mathcal{U}$, we find the dual space (or hyperplane) H_i. Then the set $\{H_i \mid 1 \leq i \leq n\}$ is indeed $\mathcal{U}'$. The proof can be easily derived by the reader.

7.3 General Construction

Hence, with the concept of *general position* extended to hyperplanes, we now look at the construction of the a t-**threshold scheme** with the capability to identify cheaters.

Construction.

i. In $\mathbf{PG}(t, q)$, randomly select a **point** X to be the secret.

ii. Randomly select a public line g containing X.

iii. Select a hyperplane $\mathbf{H}$ such that $\mathbf{H} \cap g = X$.

iv. Choose n points $X_1, X_2, \ldots, X_n$ in $\mathbf{H}$ such that $X, X_1, X_2, \ldots, X_n$ are in general position in $\mathbf{H}$.

v. Choose another hyperplane $\mathbf{H}'$ such that $\mathbf{H}'$ contains g but not the points $X_1, X_2, \ldots, X_n$.

vi. Let $\mathbf{K} = \mathbf{H} \cap \mathbf{H}'$.

vii. In $\mathbf{H}'$, choose n $(t-2)$-dimensional subspaces $\mathbf{K_1}, \mathbf{K_2}, \ldots, \mathbf{K_n}$ such that $\mathbf{K}, \mathbf{K_1}, \mathbf{K_2}, \ldots, \mathbf{K_n}$ are in general position in $\mathbf{H}'$ and no one of these subspaces contains the line g.

viii. Hence, each $\mathbf{K_i}$ intersect g at a unique point Y_i (Note that Y_i's are not necessarily distinct).

ix. For $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, n$ and $i \neq j$, let the hyperplanes $\mathbf{H_{ij}} = \langle K_i, X_j \rangle$.

x. Give participant A_i, his share X_i and the supershares $\mathbf{H_{i1}}, \mathbf{H_{i2}}, \ldots, \mathbf{H_{in}}$ $(i \neq j)$.

xi. To reconstruct the secret, calculate the span $\mathbf{U}$ of the shares and find $\mathbf{U} \cap g$.

xii. To check the 'honesty' of another participant A_j, A_i checks if the point(share) given by A_j is on the hyperplane $\mathbf{H_{ij}}$.

Remark 7.3.1. When $t = 2$, the subspaces $\mathbf{K_i}$ are in fact reduced to the points Y_i on g.

We observe one characteristic of the above construction: For a fixed j, $1 \leq j \leq n$, let $\mathcal{H}_j = \{\mathbf{H}, \mathbf{H_{1j}}, \mathbf{H_{2j}}, \ldots, \mathbf{H_{nj}}\}$. Then the intersection of any s hyperplanes in $\mathcal{H}_j$ is a subspace of dimension $t - s$.

First, we show that the knowledge of the supershares does not enable any $t-1$ participants to determine the secret X. Suppose the participants $A_1, A_2, \ldots, A_{t-1}$ attempt to obtain the secret. For any point(share) X_j, $t \leq j \leq n$, the participants know that X_j is contained in the $t-1$ hyperplanes $\mathbf{H_{1j}}, \mathbf{H_{2j}}, \ldots, \mathbf{H_{(t-1)j}}$. From the above characteristic, we know the intersection of these hyperplanes is a 1-dimensional subspace or a line. Let this line be l_j. That is, they are unable to determine the point X_j.

The participants also know that $\mathbf{U} = \langle X_1, X_2, \ldots, X_{t-1} \rangle$ is contained in $\mathbf{H}$. The participants are aware that $X \notin \mathbf{U}$ as $X, X_1, X_2, \ldots, X_{t-1}$ are independent points. Hence, there is no intersection between $\mathbf{U}$ and g.

Since $\mathbf{U}$ cannot intersect g and the participants are aware that X_j lies on l_j, then the best option for the participants to use the span of l_j and $\mathbf{U}$ to intersect with g. Now, suppose $\langle l_j, \mathbf{U} \rangle$ is contained in some hyperplane $\mathbf{F}$. Then the points $X_1, X_2, \ldots, X_{t-1}$ (from $\mathbf{U}$) and X_j (from l_j) are contained in $\mathbf{F}$, or, $\mathbf{F}$=$\mathbf{H}$. Now, $l_j \subseteq \mathbf{H}$ and $l_j = \mathbf{H_{1j}} \cap \mathbf{H_{2j}} \cap \ldots \cap \mathbf{H_{(t-1)j}}$, which means l_j is contained in the intersection of t hyperplanes in $\mathcal{H}_j$. Contradiction.

Hence, $\langle l_j, \mathbf{U} \rangle$ is not contained in any hyperplane, or $\langle l_j, \mathbf{U} \rangle$ spans the entire projective space. This means that the intersection of $\langle l_j, \mathbf{U} \rangle$ with g is g itself.

We conclude that there is no way for $t-1$ participants to locate point X. However, these $t-1$ participants can eliminate the $t-1$ points $Y_1, Y_2, \ldots, Y_{(t-1)}$ as possible secrets (Recall: $\mathbf{H_{ij}} \cap g = Y_i$ and that some of them may coincide with each other). Hence, we see that our scheme is no longer perfect.

As above, we attempt to estimate the probability of successful deception. Let us consider the 'best' scenario for the cheaters: $A_2, A_3, \ldots, A_n$ attempt to cheat A_1. The best option for them is to $A_2, A_3, \ldots, A_{t-1}$ to be honest, while the rest attempt to cheat.

Consider the following strategy. For A_t to successfully deceive A_1, he only needs to guess correctly the $(t-2)$-dimensional subspace $\mathbf{K_1}$. In fact, any point in $\mathbf{K_1}$ is sufficient and A_t focuses his effort at finding the point Y_1 on g in particular. Hence A_t just guesses any point on g, say Y_t'. Then A_t will claim that his share is a X_t' such that X_t' lies on $X_3 Y_t'$. Of course, A_t

will be successful iff $Y_t' = Y_1$. Now, there is only q choices for Y_t' (since X is obviously not a choice). Therefore, the chances of A_t succeeding is $\frac{1}{q}$.

If A_t guesses incorrectly, then A_{t+1} has one less choice for his guess Y_{t+1}'. Hence he is more likely to deceive A_1 and the probability of success is $\frac{1}{q-1}$. Inductively, the probability of successful deception for A_j is $\frac{1}{q-j+t}$. Therefore, collectively the probability of success for the $n-1$ cheaters is $\frac{n-t+1}{q}$. In fact, we can show that this is in fact the best strategy.

Example 7.3.1. Let us put the above scheme into a better perspective by looking at a 3-**threshold scheme** in $\mathbf{PG}(3, 11)$.

First, we choose the secret $X = (0, 0, 0, 1)$ on the public line $g = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

We choose $\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Let the shares be (we can check them to be in general position in $\mathbf{H}$)

$$X_1 = (1, 1, 0, 1) \quad X_2 = (1, 2, 0, 4) \quad X_3 = (1, 3, 0, 9) \quad X_4 = (1, 4, 0, 5) \quad X_5 = (1, 5, 0, 3).$$

Next we choose $\mathbf{H}' = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ (observe that $X_1, X_2, \ldots, X_5$ are not in $\mathbf{H}'$).

Hence, $\mathbf{K} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

We choose now choose the $\mathbf{K_i}$'s such that $\mathbf{K_i}$'s and $\mathbf{K}$ are are in general position in $\mathbf{H}'$ (we can verify this fact easily).

$$\mathbf{K_1} = \begin{pmatrix} 0 & 1 & 0 & 10 \\ 0 & 0 & 1 & 10 \end{pmatrix}$$

$$\mathbf{K_2} = \begin{pmatrix} 0 & 1 & 0 & 9 \\ 0 & 0 & 1 & 7 \end{pmatrix}$$

$$\mathbf{K_3} = \begin{pmatrix} 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$$\mathbf{K_4} = \begin{pmatrix} 0 & 1 & 0 & 7 \\ 0 & 0 & 1 & 6 \end{pmatrix}$$

$$\mathbf{K_5} = \begin{pmatrix} 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 8 \end{pmatrix}$$

For $i = 1, 2, \ldots, 5$, $j = 1, 2, \ldots, 5$ and $i \neq j$, we define the hyperplanes $\mathbf{H_{ij}} = \langle K_i, X_j \rangle$.

We first check that the scheme is still a 3-**threshold scheme**. Consider the situation when A_1 and A_2 cooperate to find the secret X. The two participants know that X_3 (A_3's share) lies on the line,

$$l_3 = \mathbf{H_{13}} \cap \mathbf{H_{23}} = \begin{pmatrix} 1 & 3 & 0 & 9 \\ 0 & 1 & 0 & 10 \\ 0 & 0 & 1 & 10 \end{pmatrix} \cap \begin{pmatrix} 1 & 3 & 0 & 9 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 1 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 0 & 9 \\ 0 & 1 & 7 & 3 \end{pmatrix}.$$

Since A_1 and A_2 are unable to determine the exact location of X_3, they instead try their luck by using the span of X_1, X_2 and l_3 to intersect with g. However,

$$\langle X_1, X_2, l_3 \rangle = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 2 & 0 & 4 \\ 1 & 3 & 0 & 9 \\ 0 & 1 & 7 & 3 \end{pmatrix} = I_4.$$

Hence, the span is the entire space and the intersection of this span with g is g itself. With a similar analysis for X_4 and X_5. We find that A_1 and A_2 have no way to determine secret X. However, they eliminate two possible points, namely $(0, 0, 1, 10)$ and $(0, 0, 1, 7)$.

Similarly, we can check that any pair of participants cannot obtain the secret despite the fact that they have gained partial information.

Next, we consider the scenario where A_2, A_3, A_4, A_5 attempts to cheat A_1.

Now, the 4 (> 3) participants can find out the secret X. Specifically,

$$
\begin{aligned}
X &= \mathbf{U} \cap g \\
&= \langle X_2, X_3, X_4, X_5 \rangle \cap g \\
&= \begin{pmatrix} 1 & 2 & 0 & 4 \\ 1 & 3 & 0 & 9 \\ 1 & 4 & 0 & 5 \\ 1 & 5 & 0 & 3 \end{pmatrix} \cap \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= \cdots \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cap \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= (0, 0, 0, 1)
\end{aligned}
$$

To maximise their chances of cheating successfully, the cheaters decide to let A_2 pretend to be 'honest' .

Suppose they adopt the strategy of guessing the point $Y_1 = (0, 0, 1, 10)$ (which A_2, A_3, A_4, A_5 do not know).

A_3 has $12-1 = 11$ choices for his guess of Y_1 (X is definitely not a choice) and so his chance of succeeding is $\frac{1}{11}$.

Suppose A_3 guesses the point $Y_3' = (0, 0, 1, 2)$. Then A_3 will choose a point on the line $X_3Y_3' = \begin{pmatrix} 1 & 3 & 0 & 9 \\ 0 & 0 & 1 & 2 \end{pmatrix}$. Let this point be $X_3' = (1, 3, 1, 0)$. We and A_1 can then easily check that $X_3' \notin \mathbf{H_{13}} = \begin{pmatrix} 1 & 3 & 0 & 9 \\ 0 & 1 & 0 & 10 \\ 0 & 0 & 1 & 10 \end{pmatrix}$. Hence, A_3 realises that he had failed.

Now, when A_4 attempts to guess the point Y_1, he obviously will not choose $(0, 0, 1, 10)$. So he has one less choice and his chance of success is improved to $\frac{1}{10}$. Similarly, if A_4 guesses incorrectly, A_5 can eliminate one more choice and his chance improves to $\frac{1}{9}$.

Hence, the chance of A_2, A_3, A_4, A_5 collectively succeeding (remember: A_2 does not use a false share) is $(\frac{1}{11}) + (\frac{10}{11})(\frac{1}{10}) + (\frac{10}{11})(\frac{9}{10})(\frac{1}{9}) = \frac{3}{11}$.

7.4 Problem of Anonymity

As with the scheme with veto capability, when we modify the Blakley's scheme to include new features, we also lose some characteristics of the original scheme. Here we discuss the problem of anonymity.

This characteristic is clearly lost in the cheater-identifying scheme. To verify if any participant is 'honest' , there is a need to see the share of the participant so that we can check if the point lies on the supershare (which contains the point). Hence, we are conscious of which shares belong to which participants. So even if the participants are unable to access the secrets, they gain the knowledge of the shares of the other participants.

Compare this with the Blakley's threshold scheme. There is no need for the participants to see each other's shares. They can just feed them into a machine, and this machine need not take note which share belongs to whom. Moreover, if there is no access to the secret, there is no method to figure out the shares which was inputted.

Chapter 8

Conclusion

To end this report, it is apt that we summarize the essential features of our secret sharing schemes constructed using geometry.

Honest dealer

In this report, we have assumed that the dealer is honest. That is, the dealer will distribute the shares, such that the secret can be reconstructed. There are cases where the dealer cheats and hence rendering certain users inaccessible to the secret. Nevertheless, there are protocols where the participants are able to verify the honesty of the dealer. There are also secret sharing schemes, known as *verifiable secret sharing schemes*, which exhibit such a characteristic.

Machine is trustworthy

We have also assumed that our machine not only sees all the inputted shares, but also it keeps them secret to the participants. Such a restriction is essential especially in the case of veto.

Consider a $(2, 2)$-**veto scheme**. If there are 2 shares X_1, X_2 from $\mathcal{X}$ and 2 shares Y_1, Y_2 from $\mathcal{Y}$, then the computed result is the entire public line. But to an attacker, this result implies that there are 2 shares from $\mathcal{X}$. Hence, the attacker randomly chooses a pair of points from the 4 points X_1, X_2, Y_1, Y_2, and use the pair to attack the system. The chance of the attacker succeeding is now increased to $\frac{1}{6}$!

Provable security

Unlike many public-key cryptosystems, secret sharing schemes do not rely on known NP-complete problems. Hence, while improvements in computer technology by intruders can affect the relative security of public-key systems, they have no effect on Blakley's scheme. As we have shown and proven, the probability of deception is computable and we can fix the security level at any arbituary level.

Comfortable Participant Management

Indeed, one can add users to a secret sharing scheme without altering the shares of the other participants. This is provided that the projective space is big enough to accommodate the points. In a projective space of order q, we can have at least $q + 1$ points to be in general position in this space. That is, we can have at least $q + 1$ shares. Hence, a large q will solve our problem.

Although adding users is simple, the removal is rather complicated. However, there are nevertheless schemes which are constructed for such purposes. They are called *disenrollment schemes*. Basically, when a user withdraws from the scheme, the dealer will alter the secret and subsequently the shares. Then the dealer will announce publicly the transformation which maps the old share to the new share. Hence, the scheme is convenient as the participants need not 'meet up' to get the shares. Moreover, it is safe to broadcast the transformation as it provides no information of the original shares. But there is a limit to how many times a disenrollment schemes can disenrol a member.

Repeated Usage

Now, as one realises, once the secret is revealed to the participants, it is not possible to reuse the secret or the scheme. Therefore, the scheme has to be restructured and the shares redistributed. Such a process will be costly. Interested readers can research into this area.

Other Secret Sharing Schemes

To complete this report, the author mentions a few other possible secret sharing schemes which the reader can study about.

Some interesting classes of secret sharing schemes:

- **disenrollment schemes**– as described above, these schemes which allow easy departure of users.
- **verifiable secret sharing schemes** – as described above, these schemes allow the users to check on the dealer.
- **democratic schemes** – in such a scheme, the participants are able to construct the secret and distribute the shares amongst themselves. Hence, we can omit the presence of the dealer.

Some interesting mathematical structures for constructing secret sharing schemes:

- **polynomial interpolation** – Shamir uses the fact that there is an unique polynomial of degree at most $t-1$ that passes through t points. Shamir's system is usually perfect.
- **error correcting codes** – first introduced by McEliece and Sarwate to allow for the identification of cheaters. They used the fact that errors are identifiable in an invalid codeword. So, we are able to identify the cheaters.
- **Chinese remainder theorem**
- **block designs**

Appendix

Projective spaces of small order and dimensions

This appendix describes the incidence structure of points, lines and planes in smaller dimension and order. In each space, we give label the points, lines and planes using arabic numerals. Then, we assign the points to some coordinates and list down the points incident to a certain line or plane.

$\mathbf{PG}(2, 2)$

Point	Coordinates
1	(1,0,0)
2	(1,0,1)
3	(1,1,0)
4	(1,1,1)
5	(0,1,0)
6	(0,1,1)
7	(0,0,1)

Line	Points		
1	5	6	7
2	2	4	5
3	3	4	7
4	2	3	6
5	1	2	7
6	1	4	6
7	1	3	5

$\mathbf{PG}(2,3)$

Point	Coordinates
1	(1,0,0)
2	(1,0,1)
3	(1,0,2)
4	(1,1,0)
5	(1,1,1)
6	(1,1,2)
7	(1,2,0)
8	(1,2,1)
9	(1,2,2)
10	(0,1,0)
11	(0,1,1)
12	(0,1,2)
13	(0,0,1)

Line	Points			
1	10	11	12	13
2	3	6	9	10
3	2	5	8	10
4	7	8	9	13
5	3	5	7	12
6	2	6	7	11
7	4	5	6	13
8	3	4	8	11
9	2	4	9	12
10	1	2	3	13
11	1	6	8	12
12	1	5	9	11
13	1	4	7	10

$\mathbf{PG}(3, 2)$

Point	Coordinates
1	(1,0,0,0)
2	(1,0,0,1)
3	(1,0,1,0)
4	(1,0,1,1)
5	(1,1,0,0)
6	(1,1,0,1)
7	(1,1,1,0)
8	(1,1,1,1)
9	(0,1,0,0)
10	(0,1,0,1)
11	(0,1,1,0)
12	(0,1,1,1)
13	(0,0,1,0)
14	(0,0,1,1)
15	(0,0,0,1)

Line	Points		
1	1	5	9
2	1	6	10
3	2	6	9
4	2	5	10
5	1	7	11
6	1	8	12
7	2	8	11
8	2	7	12
9	3	7	9
10	3	8	10
11	4	8	9
12	4	7	10
13	3	5	11
14	3	6	12
15	4	6	11
16	4	5	12
17	1	3	13
18	1	4	14
19	2	4	13
20	2	3	14
21	5	7	13
22	5	8	14
23	6	8	13
24	6	7	14
25	1	2	15
26	3	4	15
27	5	6	15
28	7	8	15
29	9	11	13
30	9	12	14
31	10	12	13
32	10	11	14
33	9	10	15
34	11	12	15
35	13	14	15

Plane	Points						
1	9	10	11	12	13	14	15
2	2	4	6	8	9	11	13
3	3	4	7	8	9	10	15
4	2	3	6	7	9	12	14
5	5	6	7	8	13	14	15
6	2	4	5	7	10	12	13
7	3	4	5	6	11	12	15
8	2	3	5	8	10	11	14
9	1	2	3	4	13	14	15
10	1	3	6	8	10	12	13
11	1	2	7	8	11	12	15
12	1	4	6	7	10	11	14
13	1	2	5	6	9	10	15
14	1	4	5	8	9	12	14
15	1	3	5	7	9	11	13

References

1. Dahila Malkhi, *An advanced course in computer and network security, Secret Sharing Lecture Notes,* http://www.cs.huji.ac.il/∼ ns/SS.doc

2. Austin J Maher, *Survey of Secret Sharing from 1979 to 1998 using Cryptographic Primitives,* http://www.cs.stevens-tech.edu/∼swetzel/CS693/papers/Secret_ Sharing.pdf

3. A. Beutelspacher, U. Rosenbaum, *Projective Geometry: from foundations to applications,* Cambridge University Press 1998

4. J.W.P. Hirschfield, *Projective geometries over finite fields,* Oxford University Press 1979

5. edited by Charles J Colbourn, Jeffrey H. Dinitz, *CRC Handbook of combinatorial designs,* CRC Press c1996

6. Gustavus J. Simmons, *Prepositioned shared secret and/or shared control schemes,* Eurocrypt 89

7. A. Beutelspacher, *How to say 'No' ,* Eurocrypt 89

8. E.F. Brickell, D.R. Stimson, *The Detection of Cheaters in Threshold schemes*, Crypto 88