Threshold Schemes with Hierarchical Information

by

Doreen Lynn Erickson

Tech Report # 9323

A thesis
presented to the University of Waterloo in 1990
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada 1993

Abstract

Consider the problem of n trustees, any k of which are needed to be in agreement to make an action x. In addition, if only $k-1$ are in agreement, we would like to ensure that the action can not be made. Solutions to this type of problem have been independently proposed by Shamir [Sha79] and Blakley [Bla79]. The solution is commonly referred to as a threshold scheme.

Numerous uses for threshold schemes are presented. These uses range from protecting encryption keys to preventing military and management actions without proper authority. Several general methods for implementing such schemes are examined in the literature. In this thesis we look at methods based on polynomial interpolation, on the intersection properties in finite geometries, and, more generally, Steiner systems, on those utilizing error correcting codes, and on those employing the Chinese Remainder Theorem.

Some of the threshold schemes in the literature present variations to the general scheme including the detection and the prevention of cheating. Others explore the implementation of threshold schemes that permit a hierarchy of authority for the participants in the scheme. The aim of this thesis is to present and explore variations and expansions of existing methods for threshold schemes to accommodate hierarchical information. Some of the proposed schemes not only provide hierarchical information but also implement hierarchical authority.

Acknowledgements

First and foremost, I wish to express my gratitude to my supervisor, Charlie Colbourn. Thank you for having faith in me, taking me in, pointing out several interesting possible topics , your help in finding ghost references, the idea of hierarchical information, and in general finding time to help me when time didn't exist.

I also wish to thank my readers, Ron Mullin and Gordon Agnew. Their help in locating ghost references as well as their comments were invaluable.

I also wish to acknowledge the Rotary Foundation, the math faculty, the computer science department, and the Institute for Computer Research for all the emotional and financial support.

I also would like to express my sincerest gratitude to the computer Science professors at Eckerd College. First, my undergraduate mentor, Mark Fishman, who sparked my interest in computer science and encouraged me to continue in that direction. Thank you for all the support, advice, and inspiration, from my first experience, "Oh no, there is a zillion errors flying across the screen !!!" through to my acceptance to a fantastic graduate school. I only hope someday I can do the same for a student of mine as you have done for me. A huge Thanks!! Secondly, a big thanks to Professor Gallizzi for all the advice, support, believing in me and strongly encouraging me to work in the area of computer science. The third Eckerd College professor to whom I would like to express my gratitude is George Lofquist. Thank you for all the advice as to pursuing a mathematical area as well as to what math courses would be most beneficial. I couldn't have even attempted a thesis on this topic without all the background I learned from you.

I would also like to acknowledge Bart Domzy. Thank you for showing me the ropes, letting me bounce things off you when your time was already tight, and finally, thanks for help in figuring out what those silly zeds are supposed to be!

Last but not least, I would like to thank Sue Thompson, Nadia BenHassine, all the SIGsporters, and the Minotians for all your help in making it through the past year!!

Dedication

This thesis is dedicated to my parents. Thanks for all the love and support through out my life. Thanks for always being there... even when I am 1500 miles away. Thanks for everything!

Love,

Doreen

Contents

1 Introduction **1**

1.1 Possible Uses of Threshold Schemes 2

1.2 Framework for A General Model 3

1.3 Variations to the General Method 6

1.4 Hierarchical Information Schemes 8

1.5 Overview 9

2 Polynomial Interpolation **11**

2.1 The method 11

2.2 Detection of Cheaters 14

2.3 Hierarchical Authority 15

2.4 Hierarchical Information 16

3 Finite Geometries **21**

3.1 The Method 21

3.2 Hierarchical Authority 25

3.3 An Imperfect Scheme That Detects Cheaters 26
3.4 Yes-No Threshold Scheme 28
3.5 Hierarchical Information 30

4 Steiner Systems **34**
4.1 The Method 34
4.2 Hierarchical Information 39

5 Error Correcting Codes **41**
5.1 The Method 42
5.2 Hierarchical Authority 44
5.3 Hierarchical Information 46

6 Chinese Remainder Theorem **48**
6.1 The Method 48
6.2 Validating Shadows 51
6.3 Hierarchical Information 52

7 Conclusion **58**

A Terms **64**

Bibliography **67**

List of Tables

2.1 Partial keys for Hierarchical Information 19

4.1 Upper Bounds on $M(3,3,v)$ 36

4.2 Known Values and Bounds for $M(3,3,v)$ $v \leq 30$ 37

4.3 Bounds on$M(4,4,v)$ 37

4.4 Bounds on Threshold Schemes with Invalid Partial Keys 38

4.5 Master keys for a $(3,3,9;7)$-threshold scheme 38

5.1 Possible systems based on Reed-Solomon codes 45

5.2 Hierarchical Authority Levels and Weights 45

6.1 Partial Keys for Hierarchical Information 54

6.2 Partial Keys for Alternate Hierarchical Information Scheme 56

7.1 Hierarchical Information Schemes Presented 60

7.2 Hierarchical Information Schemes evaluated by Criteria 61

List of Figures

3.1 Compartmental Scheme [Sim88] 25

3.2 Ultimate Hierarchical Authority Scheme [BV87] 29

3.3 Scheme with honest participants [BS89] 29

3.4 Scheme with cheaters [BS89] 29

Chapter 1

Introduction

Consider the problem of n trustees, any k of which are needed to be in agreement to make an action x. In addition, if only $k-1$ are in agreement, we would like to ensure that the action can not be made. Solutions to this type of problem have been independently proposed by Shamir [Sha79] and Blakley [Bla79]. Shamir, as well as other authors who built on Shamir's work, refer to the solution as a k-out-of-n secret sharing scheme. In these works, the partial keys given to the n trustees are referred to as shares. In contrast, these partial keys are referred to as shadows and the scheme is known as a (k, n) threshold scheme [1] by other authors whose work was primarily based on that of Blakley. In this thesis, we survey research on these secret sharing/threshold schemes as well as suggest a variation to protect hierarchical information.

[1] Such schemes have also been referred to as key safeguarding schemes and key sharing schemes. As well, Blakely and Swanson [BS81] have called their system an information protection scheme. In that paper, they also sought to standardize the terminology in the area but later papers in the area have not followed their suggestions.

1.1 Possible Uses of Threshold Schemes

Various uses for threshold schemes have been proposed. Karnin et. II. [KGH83] examine the situation in which a legitimate owner of a file loses the key used to enciphered it. One possible solution is to make multiple copies of the key. If one key is stolen, the secret is compromised. If a threshold scheme were to be utilized, the security is only compromised if k keys are stolen. The access is compromised only if more than $n - k$ keys are lost.

A similar situation was proposed by Blakely [Bla79]. He describes four events that one needs to protect against when using a key in an RSA (Rivest, Shamir and Adleman) or DES (Data Encryption Standard) cryptosystem. They are:

- Destruction by accident,
- Degradation - for example, if a person loses the key and makes one up,
- Defection - when a trustee gives the key to the opposition but not to the organization that entrusted the trustee, and
- Dereliction - when a trustee gives the key to the opposition as well as those who entrusted the trustee.

A threshold scheme could then be used to protect against any expected number of the aforementioned events. If an organization predicts that at most $k - 1$ of these events would occur, then a (k, n) threshold scheme could be utilized to protect the safety of their cryptosystem key (for $n \geq 2k - 1$).

Asmuth and Blakley [AB82] present the scenario in which one is sending a large message over parallel channels where at most $k-1$ channels are possibly inoperative. If

the message can be encoded using a (k, n)-threshold scheme, the message is decodable as long as k of the n channels are operative. In addition, as long as an opponent could not obtain access to k or more of the channels, the message is secure. Harari [Har83] mentions that financial terminals as well as access to remote computer equipment could be implemented using a secret sharing scheme.

Simmons [Sim90] [Sim89] [Sim88] suggests many military applications for secret sharing schemes. This area alone presents endless examples of applications. One of the more obvious amongst these is that "pushing the button" should certainly be controlled by a threshold scheme. This would prevent any one person from making such a decision without the consent of the minimum threshold. This is also true of making any potentially destructive and critical decisions in both military and administrative capacities.

It remains an open question as to whether any of the schemes that exist today could be utilized for all of the proposed uses.

1.2 Framework for A General Model

While there are several methods for implementing threshold schemes, it is convenient to describe a general model within which all methods can be described. The following describes a $(k, n)-$threshold scheme, also referred to as simply a $k-$threshold scheme.

In a threshold scheme there exist partial keys, $s_1, \ldots s_n$ where n is the number of participants. These partial keys are given to each of the n participants or trustees by the distributor. Given these partial keys, one can construct a larger object, the master key. The master key, S, may be the information that is being protected, or it may itself be a key that permits access to the information or permits an action to

occur. This master key is constructible whenever k, the threshold, or more of the partial keys are submitted to the master key constructor. The master key constructor is the algorithm that transforms the partial keys into the master key. The contents of the partial key, as well as the algorithm of the master key constructor, is dependent on the method used.

While describing the schemes within this framework, we also qualitatively evaluate the various methods by the following criteria.

criterion 1. The size of the partial key.

The size may be in terms of the information being protected or in terms of the number of participants.

criterion 2. The master key construction time.

If the master key requires days or even several hours to construct it may be impractical for many applications.

criterion 3. Storage requirements for the partial keys and the master key.

This criterion also affects the criterion of master key construction time.

criterion 4. Security of the scheme which consists of two points:

criterion 4a. The amount of information revealed about the master key by fewer than k partial keys[2] and

criterion 4b. The independence of the partial key to the amount of authority it permits (suggested by Simmons [Sim89] [Sim88]).

An *extrinsic scheme* is one in which the value of the partial keys is independent of the key and is determined by the master key constructor's

[2]A perfectly secure scheme is one in which $k-1$ partial keys pooled together have no more information about the master key than a complete outsider [SS89] [SV88a] and [BS89].

handling of the key. In addition, all partial keys are the same size despite possible difference in authoritative power [Sim88]. An *intrinsic scheme* in one in which the partial key's value is contained within the key and not in the master key constructor's handling of the key [Sim88]. Currently, all threshold schemes appear to be intrinsic.

criterion 5. Variety of known schemes of this type.

If there are insufficient schemes of this type that exist or that are known to exist, it may be impractical to use this scheme. In addition, the method may be impractical if the methods known to construct or verify that the scheme is valid require more time than is available to set up the scheme.

As one would suspect, some of the criteria may be more objectively applied than others. Many of the criteria are interdependent. This interdependence is discussed within the specific methods when relevant.

An example to illustrate the various aspects of a threshold scheme follows. The secret being protected is S. Let k, the number of partial keys needed to reconstruct the master key, equal 3. Let n, the number of participants holding partial keys, equal 5. Let the n partial keys equal $(s_1, s_2, s_3, s_4, s_5)$ where participant p_i is given partial key s_i and s_i is chosen from a set, C, of possible partial keys. Let the size of each s_i equal the size of S, the master key. The master key constructor algorithm is the function ϕ, a mapping from any subset of C to a subset of a set M of possible master keys such that $\phi(s_i, s_j, s_k) = S$ (where $i \neq j \neq k; 1 \leq i, j, k \leq 5$). Furthermore, let $\phi(s_i, s_j) = M$ and let $\phi(s_i) = M$. In other words, ϕ applied to any i partial keys, $i < k$, defines M, the entire set of possible master keys. Suppose that ϕ is a polynomial time computable function.

Evaluating this scheme by **criterion 1**, the size of the key is equivalent to the

size of the secret being protected. The construction time for the master key should be relatively low since the function is said to take polynomial time in terms of the parameters. By **criterion 3**, the storage requirements for the partial keys equals five times the storage requirements for the secret itself since each of the five keys are as large as the secret itself. **Criterion 4** reveals that the scheme is perfectly secure since 2 partial keys reveal nothing about the specific master key. **Criterion 5** is irrelevant in this general example.

1.3 Variations to the General Method

This section introduces variations and extensions to the general problem of secret sharing.

The first variation to the general model is that of preventing and detecting cheaters. The forms of cheating that have been discussed in the literature include:

- collaboration of the partial key holders,
- deliverance of an illegitimate key by the distributor,
- the presentation of an illegitimate key by a trustee (also see [Fel87] [CCD88].),
- illegitimate take over of the key distributor,
- deliverance of information about the identity of the partial keys themselves [Ben86],
- the take over of the partial key distributor [Mea88],
- the take over of the master key constructor [Mea88], and

- the tapping one of two communication channels by an outsider [Yam89].

Research by Blakely and Dixon [BD86] reveals that one cannot detect tampering in a secret sharing system which is perfectly secure, and in which the size of the key is less than or equal to the size of the secret (i. e. which does not involve expansion for those methods in which the master key is the protected information). Simmons [Sim90] notes that if the information contained in the partial keys includes the secret itself, then the system can not be perfect (since insiders have more information than outsiders). This seems to be a driving motivation behind work on the second variation of the general model, imperfect schemes. The goal is to maintain a high level of security but to keep the computational and other communication complexities low. For example, users of a system may not mind that 3 keys out of a very large set of possible keys can be eliminated. Addition information on imperfect threshold schemes can be found in [BM85] and [Yam86].

A third variation to the general model is a type of threshold scheme that allows a hierarchy of authority; these are *multilevel schemes.* The hierarchy may involve two or more levels of authority. This variation generally allows certain partial keys to be weighted. An example would be giving a president a partial key which is equivalent to two partial keys of a vice-president. Sometimes, this weighting essentially involves giving multiple keys to partial key holders with more authority.

Another type of hierarchical authority may be a compartmented scheme [Sim89] [Sim90] [BV89]. In this type of scheme the partial keys for the master keys are themselves constructed by partial keys. Thus, there is a threshold for each group or compartment. There then must be enough of the groups to submit their keys to reach the threshold for the master key.

A conditional multilevel scheme is also proposed in [Sim90]. This is useful when

one desires a multilevel system for use under emergency (or non-normal) circumstances. In such circumstances, conditions would render communicating the whole scheme to be difficult. Simmons considers an approach which can be considered a special form of key distribution. In this approach each set of sub-keys form a 56 bit key for a DES system (for example). The sub key holders have no information about the secret until it is activated, i.e. until a message is encrypted and sent. Then, and only then, is the key useful. This allows the separation of the private sub-keys from the actual secret they conceal.

Recent work by Beutelspacher [Beu89] permits yes-no partial keys. Each trustee is given yes-partial key and no-partial keys. There is a threshold for yes keys, k and a threshold for no keys, s. If there are more than s no-partial keys, regardless of the number of yes keys, no action can occur.

1.4 Hierarchical Information Schemes

The aim of this thesis is to present and explore variations and expansions of existing methods for threshold schemes to accommodate hierarchical information. In this section, we expand the general method to accommodate hierarchical information or information which may be divided into two or more layers.

In a hierarchical information scheme, the information may be separated into several levels which may be viewed as security levels. These higher levels may be accessed in the following three manners:

- participation of more partial key holders,
- participation of a partial key holder with more authority, and

- participation of more partial key holders with more authority.

The latter two not only provide hierarchical information but also require hierarchical authority. In addition, the lower levels may be separate and not necessarily hierarchical themselves.

When attempting to provide hierarchical information in a threshold scheme, one needs to identify some sort of hierarchy in the master key. If there is a natural hierarchy in the structure of the master key, the scheme is genuine. In other cases, the hierarchy may be developed by building a larger scheme on top of the existing scheme. In this situation, one is actually superimposing one threshold scheme on another. If the hierarchical scheme is the "union" of simpler schemes each participant needs several keys. This could be termed the "janitor problem". Of course, many partial keys could be encoded to form a single more complex key, alleviating the "janitor" problem. This is not a satisfactory solution, however, if the resulting key is large, requiring significant storage.

The hierarchical information schemes are presented in the last sections of chapters 2 through 6.

1.5 Overview

The various methods surveyed and described in terms of the general model include those based on linear interpolation in Chapter 2, finite geometries in Chapter 3, the more general Steiner systems in Chapter 4, those based on error correcting codes in Chapter 5, and finally, those based on the Chinese Remainder Theorem in Chapter 6. Chapter 7 presents the conclusion of the research conducted. Appendix A contains

the glossary of the major terms used throughout the thesis (indicated throughout the thesis by*).

Chapter 2

Polynomial Interpolation

The first method is based on polynomial interpolation. It was first proposed by Shamir [Sha79].

2.1 The method

The secret is assumed to be representable as a number, S. The information is then divided into pieces s_i, $i = 1, \ldots n$. A random $k-1$st degree polynomial, $q(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ is chosen with the constraint that a_0 is set to equal S. The remaining coefficients are chosen randomly, uniformly, and independently from a finite field such as $GF(p^\alpha)$, the Galois field of order p^α. The prime, p, is chosen such that it is greater than n, the number of participants, and S, the secret. The partial keys, s_1 to s_n are then: $s_1 = (x_1, y_i \equiv q(1) \bmod p), \ldots, s_i = (x_i, y_i \equiv q(i) \bmod p), \ldots, s_n = (x_n, y_n \equiv q(n) \bmod p)$.

Thus, the points that represent the partial keys are (x_i, y_i). Any k points $(x_i, y_i), \ldots, (x_k, y_k)$ with $x_i \neq x_j, 1 \leq i \leq j; 1 \leq j \leq i, i \neq j$, suffice to determine

the coefficients of $q(x)$, a polynomial of degree $k-1$. This polynomial, $q(x)$, is defined to be $a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ where $q(x_i) = y_i$ for all i. An additional advantage by **criterion 4a** is that $q(x)$ is unique and any $(k-1)$ keys have as good a chance of reconstructing the polynomial $q(x)$ as random guessing. Shamir [Sha79] points out that the size of each partial key does not exceed the size of the original data(**criterion 1**), although Denning [Den82] remarks that there might be some expansion in $GF(p)$ since p must be larger than k, the threshold. The master key is a_0. In addition, algorithms for the master key constructor exist that have a running time of $O(n \log^2 n)$ where n is the total number of partial keys [AHU74] [Knu69] (**criterion 2**).

The following is an example for a (3,5) threshold scheme implemented in $GF(p)$ where $p = 17, S = 13$, and $q(x) = 6x^2 + 7x + 13 (n = 5, k = 3)$. $q(x)$ for $x = 1$ to 5 is

$$y_1 = q(1) = 16 \bmod 17 = 16$$
$$y_2 = q(2) = 41 \bmod 17 = 7$$
$$y_3 = q(3) = 78 \bmod 17 = 10$$
$$y_4 = q(4) = 129 \bmod 17 = 8$$
$$y_5 = q(5) = 188 \bmod 17 = 1$$

Thus, the partial keys are $(1,16), (2,7), (3,10), (4,8),$ and $(5,1)$. Determining the master key is accomplished using the Lagrange Polynomial.

$$q'(x) = \sum_{c=1}^{k} \frac{s_c(x-x_1)(x-x_2)\ldots(x-x_k)}{(x_c-x_1)(x_c-x_2)\ldots(x_c-x_k)}.$$

If three partial key holders entered their keys, $s(1), s(3)$, and $s(5)$

$$q'(x) = \{16\frac{(x-3)(x-5)}{(1-3)(1-5)} + 10\frac{(x-1)(x-5)}{(3-1)(3-5)} + 1\frac{(x-1)(x-3)}{(5-1)(5-3)}\} \bmod 17$$

$$= (\frac{-3}{8}x^2 - \frac{3}{2}x + \frac{143}{8}) \bmod 17$$
$$= 2x^2 + 10x + 13 = q(x).$$

Expanding the example for four partial keys, $s(1), s(2), s(3)$, and $s(5)$

$$q'(x) = (16\frac{(x-2)(x-3)(x-5)}{(1-2)(1-3)(1-5)} + 7\frac{(x-1)(x-3)(x-5)}{(2-1)(2-3)(2-5)}$$
$$+10\frac{(x-1)(x-2)(x-5)}{(3-1)(3-2)(3-5)} + 1\frac{(x-1)(x-2)(x-3)}{(5-1)(5-2)(5-3)}) \bmod 17$$

$$= (\frac{-17}{8}x^3 + \frac{75}{4}x^2 - \frac{403}{8}x + \frac{199}{4}) \bmod 17$$

$$= 2x^2 + 10x + 13 = q(x).$$

Once again expanding the example for five partial keys, $s(1), s(2), s(3), s(4)$, and $s(5)$:

$$q'(x) = (16\frac{(x-2)(x-3)(x-4)(x-5)}{(1-2)(1-3)(1-4)(1-5)} + 7\frac{(x-1)(x-3)(x-4)(x-5)}{(2-1)(2-3)(2-4)(2-5)}$$
$$+10\frac{(x-1)(x-2)(x-4)(x-5)}{(3-1)(3-2)(3-4)(3-5)} + 8\frac{(x-1)(x-2)(x-3)(x-5)}{(4-1)(4-2)(4-3)(4-5)}$$
$$+1\frac{(x-1)(x-2)(x-3)(x-4)}{(5-1)(5-2)(5-3)(5-4)}) \bmod 17$$

$$= (\frac{17}{24}x^4 - \frac{119}{12}x^3 + \frac{1147}{24}x^2 - \frac{1123}{12}x + 71) \bmod 17$$

$$= 2x^2 + 10x + 13 = q(x).$$

Thus, once the threshold is reached or surpassed, the master key can still be constructed.

2.2 Detection of Cheaters

Tompa and Woll [TW86] added security to Shamir's scheme proposed in [Sha79]. Their scheme allows the additional property that there is a small probability $\epsilon > 0$ that any $k-1$ participants $i_1 \ldots i_{k-1}$ can fabricate new shares $S\prime_{i1}, S\prime_{i2} \ldots S\prime_{ik-1}$ that deceive a k^{th} participant. In other words, they desire that the reconstruction of a legal but incorrect secret occurs with probability $\epsilon > 0$. This can be accomplished by having the distributor sign each share with an unforgable signature. The advantages of this approach according to Tompa and Woll, include:

1. It does not rely on the hypothesis of the intractability of integer factorization (this is also true of Shamir's scheme [Sha79]), and
2. It is as easily implemented as Shamir's Scheme (polynomial in terms of k, n, log s, and log $(1/\epsilon)$).

This approach assumes the distributor is honest. The implementation of this scheme is as follows:

1. Choose any prime $p > max(s/\epsilon + k, n)$
2. Choose $a_1, a_2, \ldots a_{k-1} \in \mathcal{Z}_p$ randomly, uniformly, and independently
3. Let $q(x) = S + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$
4. Choose $(x_1, x_2, \ldots, x_n)$ uniformly and randomly from all permutations of n distinct elements from $1, 2, \ldots p-1$.Let $S_i = (x_i, s_i)$ where $s_i = q(x_i)$[1].

[1]This scheme differs from Shamir's scheme in this requirement. Shamir's scheme can be described as above except that this step would be replaced by : Let $S_i = q(i) \forall i \ 1 \leq i \leq n$ where the evaluation of q(i) is over $\mathcal{Z}_p$.

Tompa and Woll sketch a proof showing that participant i_k deceives with probability $\epsilon > (s-1)(k-1)/(p-k)$. They also note that while the cheaters are detected, they often obtain the secret while the other members don't. An outline to a solution to this problem is also examined. Briefly summarized, one chooses a dummy legal value s, that is never used. The secret S is then encoded as $S^1, S^2, \ldots S^t$ where $S^i = s$ for all $j \neq i$ and $S^i = S$ for some i chosen randomly. Each element of the sequence is divided into shares using the aforementioned scheme. Thus, the probability of cheating while going undetected at possible previous cheats is less than $(1-\epsilon)^{-1}t^{-1}$.

2.3 Hierarchical Authority

The idea of hierarchical authority in this method is presented in Shamir's original paper [Sha79]. He suggests that tuples of polynomial values be given to higher levels in the hierarchy. Thus, the weighting is accomplished by those with more authority carrying more keys.

Adapting the example presented in section 2.1, one key holder is given more authority by holding the partial key s_1, and s_2. The (3,5)-threshold scheme would now be a (3,4)-threshold scheme with one partial key holder possessing more authority. In this situation, any three members may enter their partial keys to obtain the master key, or the more authoritative partial key may be entered along with any of the other three remaining partial keys. Thus, the threshold scheme implemented in $GF(p)$ where $p = 17, S = 13$, and $q(x) = 6x^2 + 7x + 13 (n = 5, k = 3)$. $q(x)$ for $x = 1$ to 5 is

$$y_1 = q(1) = 16 \bmod 17 = 16$$
$$y_2 = q(2) = 41 \bmod 17 = 7$$

$$y_3 = q(3) = 78 \bmod 17 = 10$$
$$y_4 = q(4) = 129 \bmod 17 = 8$$
$$y_5 = q(5) = 188 \bmod 17 = 1$$

The partial keys are $[(1,16),(2,7)], (3,10), (4,8),$ and $(5,1)$. The Lagrange Polynomial

$$q'(x) = \sum_{c=1}^{k} \frac{s_c(x-x_1)(x-x_2)\ldots(x-x_k)}{(x_c-x_1)(x_c-x_2)\ldots(x_c-x_k)}$$

is still used.

The following is an example if two partial key holders entered their keys which included the more authoritative member. Using the partial keys of $s_{[1,2]}$ and s_5

$$q'(x) = \{16\frac{(x-2)(x-5)}{(1-2)(1-5)} + 7\frac{(x-1)(x-5)}{(2-1)(2-5)} + 1\frac{(x-1)(x-2)}{(5-1)(5-2)}\} \bmod 17$$

$$= (\frac{7}{4}x^2 - \frac{54}{4}x + \frac{57}{2}) \bmod 17$$

$$= 2x^2 + 10x + 13 = q(x).$$

2.4 Hierarchical Information

The first natural extension would be to have the higher levels of information accessible by more partial key holders. Thus, more partial key holders could interpolate a polynomial of higher degree. Since hierarchical authority was implemented through the issuance of multiple tuples, this scheme could implement hierarchical authority and information. In order to avoid the maintaining of large keys, it would be best if the partial key holders were able to utilize exactly the same key when attempting to access the different security levels of information.

Without loss of generality, we look at the case in which there are two security levels and show that this cannot be accomplished using this method.

Let $q(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$, the polynomial for the lower level of information. Let $p(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1}$, the polynomial for the higher security level information where $k < m$. Choose p, the prime such that $k < m < p$. If $q(x) \neq p(x)$ then, without loss of generality, there exists a point (x, y) on $q(x)$ that is not on $p(x)$. However, in order for the partial key holders to use exactly the same key for each level, $q(x_i) = p(x_i)$ for all i where i is an element of $GF(p)$. Thus, there is a contradiction of our assumption that $q(x_i) = p(x_i)$ for all i and the polynomials are the same. In addition, $a_0 = b_0$ which is the secret the schemes are protecting.

A possible solution to attempt to accommodate hierarchical information is to give the partial key holders an additional s_i for each level they are allowed to access. The index, i may be the same thus allowing the partial key to be half has large as the original partial key for each access level permitted. Hierarchical authority may also be imposed by simply not giving a partial key to participants who are not authorized to access that level. If one wishes to restrict the higher security levels to more people with higher authority, then the polynomial for the higher levels is chosen such that it requires more partial keys to interpolate it.

Evaluating this scheme by **criterion 1**, if the size of the partial key for one level is 2γ, a partial key for L levels would be $\gamma + L\gamma$. This is assuming that the partial key requires γ storage space for the x coordinate and γ storage space for the y coordinate. Thus, by maintaining the same x coordinate for hierarchical information schemes $2L\gamma - (\gamma + L\gamma) = \gamma(L - 1)$ less storage space is utilized.

Let the various thresholds for m levels of authority be represented as $k_1, \ldots k_m$ where $1 < \cdots < m$. The partial keys would still be points as in the general method. They would be chosen from $GF(p)$ where p is greater than k_m, n (the number of

participants) as well as all the secrets. Once the index value which serves as the x coordinate is chosen for a particular partial key holder for one scheme, it remains the same. These values may be chosen uniformly and randomly from all permutations of distinct elements from $1, 2, \ldots p-1$ as recommended by Tompa and Woll [TW86] in order to detect tampering. The threshold scheme for each level would be the same as the general method. Specifically, for level k_α, any k_α points $(x_i, y_i), \ldots (x_{k_\alpha}, y_{k_\alpha})$ with $x_i \neq x_j, 1 \leq i \leq j;\ 1 \leq j \leq i,\ i \neq j$, suffice to determine the coefficients of $q_\alpha(x)$, the polynomial of degree k_α. The secret at level α would be y-intercept for the polynomial interpolated at that level. As in the general method, $q_\alpha(x)$ is defined and unique. Furthermore, any $k_\alpha - 1$ keys have as good of a chance of reconstructing the polynomial as random guessing.

The following is an example of a hierarchical information threshold scheme implemented in $GF(p)$ where $p = 11$. The lowest level secret is not hierarchical itself and consists of two (2,3)-threshold schemes. Level 2 requires a higher threshold than level 1 and is a (3,6)-threshold scheme. Level three is a (3,4)-threshold scheme with all participants not receiving partial keys. Thus, at this level there is a hierarchy of authority as well as a hierarchy of information. The polynomials used for the various levels are as follows:

Level 3 $\boxed{q_3(x) = 10x^2 + 3x + 2}$

Level 2 $\boxed{q_2(x) = 6x^2 + 7x + 3}$

Level 1 $\boxed{q_{1a}(x) = 9x + 5}$ $\boxed{q_{1b}(x) = 2x + 10}$

The secret for level 1a is 5, for 1b is 10, for level 2 is 3, and for the highest level is 2.

The partial keys are computed in $GF(11)$; s_i denotes the i^{th} partial key. Y_j denotes the Y coordinate portion of the partial key for level j. An asterisk denotes a key not distributed.

	x_i	Y_{1a}	Y_{1b}	Y_2	Y_3
s_1	4	8	$*$	6	$*$
s_2	9	9	$*$	2	3
s_3	2	1	$*$	8	4
s_4	8	$*$	4	3	6
s_5	7	$*$	2	5	7
s_6	3	$*$	5	1	$*$

Table 2.1: Partial keys for Hierarchical Information

For level 1a access, if partial keys s_2 and s_3 are used,

$$q'_{1a}(x) = (9\frac{(x-2)}{(9-2)} + 1\frac{(x-9)}{(2-9)}) \bmod 11$$

$$= (\frac{8}{7}x - \frac{9}{7}) \bmod 11$$

$$= 9x + 5 = q_{1a}(x).$$

For level 1b access, if partial keys s_4 and s_6 are used,

$$q'_{1b}(x) = (4\frac{(x-3)}{(8-3)} + 1\frac{(x-8)}{(3-8)}) \bmod 11$$

$$= (\frac{-1}{5}x + \frac{28}{5}) \bmod 11$$

$$= 2x + 10 = q'_{1b}(x).$$

For level 2 access with partial keys s_1, s_3, and s_4, the secret is revealed as follows.

$$q'_2(x) = (6\frac{(x-2)(x-8)}{(4-2)(4-8)} + 8\frac{(x-4)(x-8)}{(2-4)(2-8)} + 3\frac{(x-4)(x-2)}{(8-4)(8-2)}) \bmod 11$$

$$= (\frac{1}{24}x^2 - \frac{5}{4}x + \frac{31}{3}) \bmod 11$$

$$= 6x^2 + 7x + 3 = q_2(x)$$

The final example is for the top level using the partial keys of s_2, s_3 and s_4.

$$q'_3(x) = (3\frac{(x-2)(x-8)}{(9-2)(9-8)} + 4\frac{(x-9)(x-8)}{(2-4)(2-8)} + 6\frac{(x-9)(x-2)}{(8-9)(8-2)}) \bmod 11$$

$$= (-\frac{10}{21}x^2 + \frac{107}{21}x - \frac{30}{7}) \bmod 11$$

$$= 10x^2 + 3x + 2 = q_3(x)$$

Chapter 3

Finite Geometries

The second implementation strategy is based on intersection properties of finite geometries. A finite geometry is defined in terms of a system of axioms and undefined terms which limits the set of elements(such as points and lines) in the geometry to a finite number [Tul67]. For example, a finite geometry could consist of a finite set of points, a finite set of lines, and an incidence relation between the points and the lines, where the axioms constrain this incidence relation.

3.1 The Method

The general idea behind geometric threshold schemes is that one chooses a block* or line[1], b, to be the master key. The partial keys are n points chosen on that block such that any k of the n points uniquely determines the block. In addition, any $k-1$ points identify numerous blocks [BV87] [Beu88].

[1]A line in a finite geometry is assumed to have more than one, but only a finite number of points [Sma88].

For the master key constructor, Beutelspacher and Vedder point out that one could store k points [BV87] [Beu88]. The master key constructor would then, upon receiving $u \geq k$ points, attempt to construct a block. If no such block exists or more than one blocks exists, then the master key constructor terminates. Otherwise, the constructor checks if the secretly stored k points lie on the block constructed by the u points entered. An alternative method improves the scheme's rating by **criterion 3**. A set, S of points is chosen such that they intersect the block in a unique point X; then the master key constructor only needs to store S and X. If u partial keys are entered and define a unique block c, the constructor then computes $c \cap S$. If $c \cap S = X$, the threshold is met.

Various schemes described in [Beu88] [BV87] include a 5-threshold scheme (i. e. $k = 5$) utilizing the fact that through any 5 points in the Euclidean plane, there is a unique conic. A conic is a set of points that are intersections of corresponding lines in two projectively related pencils of lines in the same plane. Pencils of lines are the set of lines through a fixed point which is collinear with pairs of corresponding points on two lines [Sma88]. Some of the more familiar conics include the ellipse and the circle. The number n of partial keys distributed is only restricted by the fact that no three partial keys or points are collinear. The master key constructor could store two points which define a tangent to the conic as S. A tangent is a line that has one point, X, in common with the conic. If additional security it needed, they recommend choosing a secant to the conic. A secant is a line which has two points in common with the conic. Thus, in this situation, X is a set of two points. Similarly, a 3-threshold scheme involving a circle could be constructed. The generalization presented is that any k points determine a "rational normal curve" in $k-3$-dimensional projective space. In addition, there exists a unique rational normal curve through any k points, no $k-2$ of which may lie on a common hyperplane*.

A method for using flats, or subspaces is also presented by Beutelspacher and Vedder [Beu88] [BV87]. If G represents an affine or projective geometry of dimension d, a block is a $(k-1)$-dimensional subspace of G. The partial keys are points in the subspace chosen such that any k of them span the block. Once again, the master key constructor only needs to store S. In this scheme, S is a $(d-k+1)$-dimensional subspace which intersects the block only in the point, X. It is also required that every $(k-1)$-dimensional subspace of G intersect S.

An additional contribution made by Beutelspacher and Vedder is a scheme that uses Desarguesian projective planes*, specifically those arising from the Galois Field $GF(p^\alpha)$ where p is a prime [BV87]. Blakely [Bla80] states that threshold schemes in $GF(2^\alpha)$ are preferred to those in GF(p^α) where p is an odd prime as the implementation on a computer can be accelerated. This is due to the ability to use the exclusive-or (XOR), a natural operator in this field. However, the author has not indicated how secure this type of system would be from the opponents' viewpoint.

De Soete and Vedder [DSV88] present t-threshold schemes for $t = 2$ and 3 based on generalized quadrangles*. A finite *generalized quadrangle* (GQ) of order (σ, τ) is an incidence structure*[2] which satisfies the following axioms:

1. Each point is incident with exactly $1 + \tau$ lines ($\tau \geq 1$) and two distinct points are incident with at most one line.

2. Each line is incident with exactly $1 + \sigma$ points ($\sigma \geq 1$) and two distinct lines are incident with at most one point.

3. For any line L and any point x not on L, there exists a unique line which is incident with both x and a (unique) point on L. (In other words, only one of

[2]An incidence structure, I, is a subset of $p \times b$ where p is a set of points and b is a set of blocks [DSV88]. Another threshold scheme based on incidence structures is presented by Ecker [Eck].

the τ lines through x intersects the line L.) [DSV88]

The scheme uses the span of pointsets. The span of 2 distinct points consists of all points which are collinear with every point in the trace of x and y. More formally, let $x^{\perp}$ be the set of all points collinear with x, a point. The span of x and y is defined as : $sp(x,y) = \{x,y\}^{\perp\perp} = \{u \in P | u \in Z^{\perp} \text{ for all } Z \in tr(x,y)\}$ where $tr(x,y)$, also denoted $\{x,y\}^{\perp}$ is the trace of a pair (x,y) = set $x^{\perp} \cap y^{\perp}$. A threshold scheme for $k = 2$ is described in which the partial keys are the points of $sp(x,y)$ where x and y are two non-collinear points of G, a generalized quadrangle of order (σ, τ) with $\sigma, \tau > 1$. The master key is the span of x and y.

De Soete and Vedder [DSV88] state that the probability of obtaining the master key when one valid partial key and some other invalid point is entered equals

$$\frac{n-1}{\sigma^2\tau + \sigma\tau + \sigma} \leq \frac{\tau}{\sigma^2\tau + \sigma\tau + \sigma}.$$

If the partial key holder knows some finite geometry and knows the lines through his point, the probability increases since $\sigma\tau + \sigma$ points are collinear with the partial key. The resulting probability is

$$\frac{n-1}{\sigma^2\tau + \sigma\tau + \sigma - (\sigma\tau + \sigma)} = \frac{n-1}{\sigma^2\tau} \leq \frac{1}{\sigma^2}.$$

An unanimous concurrence scheme with a geometrical base is presented in [IS90]. This type of scheme is one in which the master key is created by all participants, no one person of which knows the master key. This scheme does not have a distributor. In this scheme, the inputs are privately made by each of the participants and each contribution is equally influential in determining the secret. The example presented in the paper is as follows. If one desires that 2 out of 3 Vice Presidents should be able to open the vault then each President chooses a plane, the point of intersection

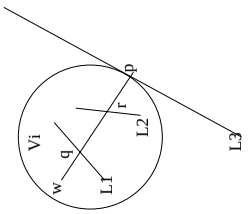

Figure 3.1: Compartmental Scheme [Sim88]

of which is the master key. Each President then proceeds to give each of the other 2 Vice-Presidents 2 distinct lines that define his/her plane. The partial keys for each Vice-President consist of their plane and a line from each of the other two Vice-Presidents.

3.2 Hierarchical Authority

A compartmented threshold scheme is presented by Simmons [Sim88]. Each compartment's threshold is 2 in the example presented. Furthermore, there are two compartments which make up the master-threshold. Each compartment's partial key is a line. The partial keys within the compartments are points. Thus, the participants receive a point contained on their line. Any two participants of a compartment may define their line. The two lines, L_1 and L_2 are skew and thus do not intersect. The master key constructor has a third line, L_3 known as the domain variety, skew to both L_1 and L_2 that is not contained in the 3-flat they determine. In addition, the master key constructor has a third, unique line, w which intersects the lines L_1, L_2, and L_3 at points q, r, and p respectively. (See Figure 3.1 [Sim88].) Thus, when the two compartmental thresholds are met, a 3-flat, V_i, is defined. The master key constructor then calculates $V \cap L_3 = p$, a unique point that serves as the master key.

Restrictions on the points given as partial keys for each compartment includes that they may not lie on L_3 nor w nor may they equal p. In this scheme, it is assumed that p is not itself the secret but that the master key constructor, with knowledge of p, can determine the secret with p as a reference point. The function that determines the secret may use the distance of p from some reference point, one of its coordinates, or some other information provided by knowledge of p. Possibilities for generalization and incorporation of additional features for this type of scheme may be found in [Sim88] [Sim89] [Sim90].

A multilevel scheme in which one level, such as computer programs, can never obtain ultimate authority for a decision over another level of users such as humans is presented in [BV87] and [Beu88] . To implement this scheme, a $(k-1)$-dimensional subspace, B, is utilized for choosing the partial keys to be utilized by humans. The human partial keys are in general position (i.e. any k of them span B). The computer partial keys are chosen in general position from a $(k-1-i)$-dimensional subspace of B, B^+ where i is the minimal number of human participants required for the threshold. The human partial keys are contained in B but are outside of B^+. Thus, the human user's consent is necessary in order to identify the master key, B but the humans may obtain the threshold without the consent of the programs. (See Figure 3.2 [BV87].)

3.3 An Imperfect Scheme That Detects Cheaters

A nearly perfect threshold scheme in Galois Field (q) in which any single cheater is identified with probability $1 - \frac{1}{q-1}$ is presented by [BS89]. If there is only one honest participant, then the probability of cheating successfully is $\frac{n-k+1}{q-1}$ where n is the number of participants and k trustees are needed to access. The scheme is nearly

perfect in that $k-1$ participants can eliminate at most 2 keys. The partial key distributor is assumed to be honest.

The implementation is a modification of Blakely's threshold scheme [Bla79] which is described below.

1. The distributor fixes a line L in V, a k-dimensional vector space over $GF(q)$ where $q = p^{\alpha}, p$ a prime.
2. This line is made known to all participants.
3. The distributor constructs a random $(k-1)$-dimensional subspace H that meets L in a point.
4. The distributor then constructs the hyperplane $H_p = H + p$.
5. The distributor then chooses n random points on H_p, h_i, $1 \leq i \leq n$ such that no k of them lie in a flat of dimension $k-2$.
6. The master key constructor upon receiving k points can uniquely determine H_p and thus obtain p by calculating $H_p \cap L = p$ which is true by construction.

Brickell and Stinson's modification is explained in terms of a threshold scheme where $k = 2$. The random subspace constructed by the distributor is 1-dimensional and the hyperplane H_p is a line. The distributor then constructs w random 1-dimensional subspaces, h_i, $1 \leq i \leq n$. These subspaces are distinct from H_p but not necessarily distinct from each other. The distributor then gives each participant the parallel lines $H_{ji} = h_j + s_i$ where s_i is a point on H_p. Thus, extra information is being distributed to the participants (**criterion 1**). For security purposes, the order of the Galois Field, q, should be large relative to n. Figure 3.3 shows the scheme when all participants are honest and use the correct partial keys.

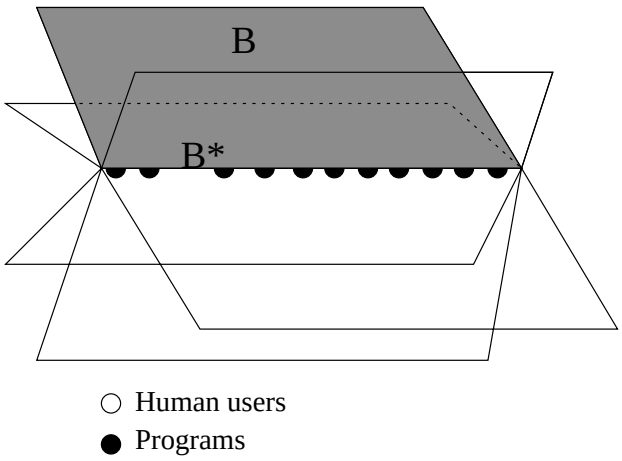

Figure 3.2: Ultimate Hierarchical Authority Scheme [BV87]

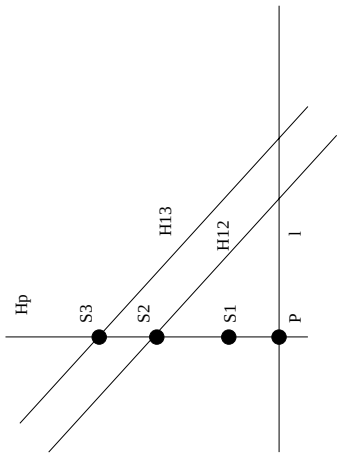

Figure 3.3: Scheme with honest participants [BS89]

Figure 3.4 displays the result of the partial key holder of s_2 giving $s_{2'}$. The authors explain that the cheater would not choose a point on L, nor any point on a line through the other participants line parallel to L since these points would reveal the lie. In addition, the cheater would not choose a point on H_p since this would reveal the secret. Thus, through any of the remaining possibilities there is a unique line which contains the actual and the fake point. An example of such a line is H_{12} in figure 3.4 [BS89]. There are $q-1$ possible lines such as H_{12} in $GF(q)$.

3.4 Yes-No Threshold Scheme

Finally, Beutelspacher [Beu89] presents an imperfect scheme that allows the additional feature of yes/no partial keys and thus effects the size of each partial key (**criterion 1**). Each key holder possess a yes-partial key and a no-partial key. If k yes-partial keys are given to the master key constructor, the master key is constructed subject to the existence of fewer than s no-partial keys. This scheme is referred to as a $(k;s)$-threshold scheme. Thus, if there are fewer than k yes-partial keys the master key cannot be constructed. If there are at least k yes-partial keys and fewer than s no-partial keys, the master key can be uniquely determined. Finally, if there are k or more yes-partial keys and more than s no-partial keys, there is too much information. The probability of guessing the correct master key in the last case is $\frac{1}{q+1}$ where q is the order of the underlying projective space.

The implementation is similar to the schemes described in [BV87] and in section 1 and 2 of this chapter. The yes-partial keys belong to the set P of points in K, a $(k-1)$-dimensional subspace. The no-partial keys belong to the set N of points in S, a $(s-1)$-dimensional subspace which is skew to K. A line L is fixed such that it intersects K in a unique point X and is skew to S. L is spanned by the points X and

Y. The partial keys are chosen such that $P \cup N \cup \{X, Y\}$ is an arc. This constraint allows any $k+s$ points to span the whole space. Thus, if U partial keys are presented to the master key constructor:

- If U contains $k-1$ yes-partial keys (points of P), then X is not an element of $< U >$ and the secret cannot be reconstructed.
- If U contains at most $s-1$ no-partial keys (points of N), then Y is not an element of $< U >$, and thus the secret may be retrieved if there are enough yes-partial keys.
- If U contains at least s no-partial keys (points of N), and at least k yes-partial keys (points of P), then $< X, Y > \subseteq U$ and the secret may not be retrieved.

A generalization utilizing a geometry consisting of subspaces is also presented.

3.5 Hierarchical Information

The first approach to hierarchical information based on the intersection properties of finite geometries is an adaptation of the compartmented scheme proposed by Simmons [Sim88] and presented in section 3.2. Specifically, the example presented may be extended to a hierarchical information scheme with two levels of information. The lower level has two separate groups of partial keys, one for each group of participants. The partial keys for group 1 are points on L_1. A threshold amongst this group permits access to information level $1a$. The partial keys for group 2 are points on L_2, a line skew to L_1. Access to level $1b$ is permitted when a threshold of users in group 2 is met. The master key constructor once again possesses a third line, L_3 which is skew to both L_1 and L_2 and a unique line w which intersects L_1, L_2 and L_3 at points

q, r, and p respectively. If there is a threshold amongst the participants in group 1 and group 2, access is permitted to information in level 2.

The adaptation of Simmons' scheme simply involves the master key constructor. If the partial keys presented identify L_1, the master key constructor is able to identify the point q as described in section 3.2, it permits access to information in level $1a$. If the partial keys submitted allow the identification of point r, level $1b$ access is granted. Furthermore, if the point p is identifiable thus signifying a threshold amongst partial key holders in group 1 and group 2, then the higher level information in level 2 is accessible. In conclusion,this scheme is still essentially a compartmented hierarchical scheme with a small adaptation to the master key constructor to allow access when a threshold in each compartment is reached.

Assuming the master key constructor previously stored line w as well as q, r, and p, the storage requirements for hierarchical information are the same for the master key (**criterion 3**). This is also true for the size of the partial keys since they have gone unchanged in this scheme (**criterion 1**).

A generalization based of a compartmented scheme presented in [Beu] is used as a basis for a generalization of this type of hierarchical information scheme. Let $G_1, \ldots G_n$ represent n groups each of which is allowed access to information in level $1i$. Let k_i represent the threshold for group G_i. For every group, G_i, there is a linear subspace, U_i of dimension $k_i - 1$ of a projective space p. The U_i subspaces are chosen such that:

- They generate a space of dimension $(\sum_{i=1}^{n} k_i) - 1$. (In other words, they are in general position and the dimension is one less than the sum of the thresholds for each level.)
- The U_i's generate a space of dimension $(\sum_{i=1}^{n} k_i) - 1$.

- They intersect a subspace U_∞ of dimension $k_\infty - 1$ in the points $X_1, \ldots X_n$ respectively.

Once again, there is a unique line, S, which intersects U_∞ in a unique point X. If the master key constructor is able to construct X_i, then access to information in level 1_i is permitted. If each of the thresholds in group G_i for i equals 1 to n, then the master key constructor can construct X and thus permit access to the higher level secret in level 2.

The second approach to hierarchical information is based on the ultimate authority multilevel scheme presented in [Beu89] [BV87] and in section 3.2. This hierarchical information scheme also provide a hierarchy of authority. The following is an adaptation and provides access to two levels of information and provides two levels of authority. The lower authority partial key holders may only access the higher level information if i higher authority partial keys are presented to the master key constructor. The higher authority partial key holders may access either level of information with the presentation of k partial keys.

To implement this scheme, a $(k-1)$-dimensional subspace, B, is utilized for choosing the partial keys for the higher authority partial key holders. These partial keys are to be chosen in general position (i.e. any k of them span B). The lower authority partial keys are chosen in general position from a $(k-1-i)$-dimensional subspace of B, B^+. The number of partial keys distributed is limited only by the above constraints. The higher authority partial keys are contained in B but are outside of B^+. Thus, the higher authority partial keys must be presented in order to identify the master key, B for the higher level information. By defining B, they also define any subspace of B and thus the master key constructor will permit access to any threshold permitted by a subspace as in the scheme by Beutelspacher and Vedder [Beu] [BV87]. The higher authority users may obtain the threshold for either level of

information without the consent of the lower authority users. The lower level partial key holders could never define B without i higher authority partial keys. Furthermore, the lower level partial key holders may define B^+ subspace with a threshold of $k-2-i$ and thus obtain access to the lower level information.

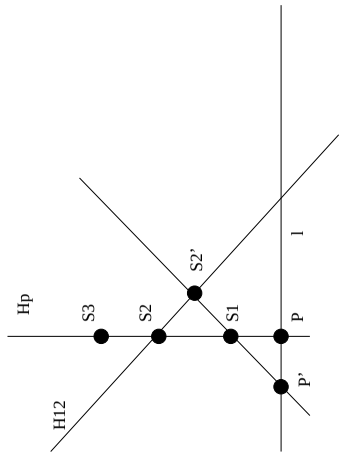

Figure 3.4: Scheme with cheaters [BS89]

Chapter 4

Steiner Systems

More generally, geometrical threshold schemes may be based on Steiner systems*. A Steiner system $\mathcal{S}(k, n, v)$[1] is a simple n-uniform hypergraph on v points such that every k-subset of points define a unique block*.

4.1 The Method

The partial keys in this method are the v points. From the v points, n are chosen as partial keys and given to the n participants. The master key constructor, with k partial keys, can calculate any one of a set of m master keys, $\{S_1, \ldots S_m\}$ [2]. These m master keys are the unique blocks defined by every k-subset of unordered points. The representation for threshold scheme based on Steiner systems is a $(k, n, v; m)$-threshold scheme.

[1]The usual notation for a Steiner system is $\mathcal{S}(t, k, v)$. The notation is changed here in an effort to maintain consistent notation for k and n within the thesis.

[2]Additional schemes which consist of a set of master keys, referred to as access structures, can be found in [ISN87] [BS90]

Stinson and Vanstone [SV88b] [SV88a] show that there exists a perfect $(k, n, v; m)$ threshold scheme if and only if there exists m mutually k-compatible* n-uniform hypergraphs on v points. Two hypergraphs, A_1 and A_2, are considered to be k-compatible if $A_1(k-1) = A_2(k-1)$ and $A_1(k) \cap A_2(k) = \emptyset$ where $A(k)$ equal the set of all subsets of vertices of order k. They also show that $M(k, n, v) = \frac{(v-k+1)}{(n-k+1)}$ if and only if a $\mathcal{S}(k, n, v)$ Steiner system can be partitioned into $\mathcal{S}(k-1, n, v)$ Steiner systems. ($M(k, n, v)$ is the maximum possible value for m, the number of master keys in a $(k, n, v; m)$ threshold scheme.) The general upper bounds for $M(3, 3, v)$ as well as the exact value, when known, for $M(3, 3, v)$ for $v \leq 30$ presented by [SS89] and [CS89] are displayed in Table 4.1 and Table 4.2 respectively. When the exact value for $v \leq 30$ is not known, the upper and lower bounds known are presented. Table 4.1 has been updated to reflect recent work by Teirlinck [3] [Tei89]. Table 4.3 displays one upper and three lower bounds on $M(4, 4, v)$ as presented by [SS89]

The schemes presented are for a $(k, n, v; m)$-threshold scheme where $k = 3$ and $n = 3$ and $(v; m) = (9; 7), (12; 8), (14; 10), (16; 10), (17; 13), (23; 19)$ and for a $(3, 3, v; m)$ threshold scheme that meets the upper bound on m. Also presented in their paper are some combinatorial designs for imperfect schemes.

General bounds for reconstructing keys are presented in [Mer83]. They are reportedly proven in Merritt's thesis (See Table 4.4). These bounds involve the relationship between the number of participants n, and the number of people holding invalid par-

[3] The original work was by J.X. Lu whose death left his proofs for the existence of certain partitions of Steiner systems incomplete. Prior to the work by Teirlinck, six cases were left unsettled.

Value of v	Value of $M(3,3,v)$
$v = 1$ *or* $3 \bmod 6, v > 1$	$M(3,3,v) \leq v-2$
$v = 0,2$ *or* $5 \bmod 6, v > 2$	$M(3,3,v) \leq v-4$
$v = 4 \bmod 6, v > 4$	$M(3,3,v) \leq v-6$
$v = 1,3 \bmod 6, v \neq 1,7$	$M(3,3,v) = v-2$
$v = 2$ *or* $6 \bmod 12, v/2 \neq 1,7$	$M(3,3,v) = v-4$
$v = 4$ *or* $12 \bmod 24, v/4 \neq 7$	$M(3,3,v) \geq v-8$
$v = 5 \bmod 30, v/5 \neq 7$	$M(3,3,v) \geq v-10$

Table 4.1: Upper Bounds on $M(3,3,v)$

tial keys b, in a k-threshold scheme.

Evaluating the scheme by the criteria, the size of the partial key, γ is determined by the implementor when choosing the partial keys. The master key constructor needs to store at least $\gamma * k * m$ since the master key is a set of m master keys, each of which is defined by a minimum of 1 set of k partial keys the size of γ.

An example of a perfect (3,3,9;7)-threshold scheme presented by Chen and Stinson [CS89] follows. The 9 partial keys are $\{0,1,2,3,4,5,6,7,8\}$. The 7 master keys are represented as $S_1, S_2, \ldots S_7$ and are presented in table 4.5.

If the partial keys $\{4,2,5\}$ were presented to the master key constructor, the unique master key S_7 would be identified since $\{2,4,5\}$ is contained in S_7.

Other examples presented in [CS89] include those for a $(k,n,v;m)$-threshold scheme where $k = 3$ and $n = 3$ and $(v;m) = (9;7),(12;8),(14;10),(16;10),(17;13),(23;19)$

v	$M(3,3,v)$	v	$M(3,3,v)$
6	2	19	15
7	3	20	$8 \leq M(3,3,20) \leq 16$
8	4	21	19
9	7	22	$14 \leq M(3,3,22) \leq 16$
10	4	23	19
11	7	24	20
12	8	25	23
13	11	26	22
14	10	27	25
15	13	28	$20 \leq M(3,3,28) \leq 22$
16	10	29	$M(3,3,29) \leq 25$
17	13	30	26
18	14		

Table 4.2: Known Values and Bounds for $M(3,3,v)$ $v \leq 30$

Values for v	Bounds on $M(4,4,v)$
all v (upper bound)	$M(4,4,v) \leq v-3$
$v = 8$ *or* 16 mod 24	$M(4,4,v) \geq 3v/4$
$v = 0$ *or* 6 mod 12	$M(4,4,v) \geq v/3$
$v = 4$ *or* 20 mod 24, $v/4$ a prime power	$M(4,4,v) \geq v/4$

Table 4.3: Bounds on$M(4,4,v)$

restrictions on (n, b, k)	upper bounds	lower bounds
k even	$b+2$	$b+1$
k odd	$b+1$	b
$b = 1$	$b+1$	$b+1$
$(7, 4, 3)$	b	b
$(6, 2, 4)$	$b+2$	$b+2$ conjectured

Table 4.4: Bounds on Threshold Schemes with Invalid Partial Keys

S_1	S_2	S_3	S_4	S_5	S_6	S_7
{7,8,0 }	{7,8,1 }	{7,8,2 }	{7,8,3 }	{7,8,4 }	{7,8,5 }	{7,8,6 }
{0,1,6 }	{1,2,0 }	{2,3,1 }	{3,4,2 }	{4,5,3 }	{1,6,4 }	{6,0,5 }
{0,2,5 }	{1,3,6 }	{2,4,0 }	{3,5,1 }	{4,6,2 }	{1,0,3 }	{6,1,4 }
{0,3,4 }	{1,4,5 }	{2,5,6 }	{3,6,0 }	{4,0,1 }	{1,1,2 }	{6,2,3 }
{1,2,4 }	{2,3,5 }	{3,4,6 }	{4,5,0 }	{5,6,1 }	{2,0,2 }	{0,1,3 }
{3,5,6 }	{4,6,0 }	{5,0,1 }	{6,1,2 }	{0,2,3 }	{4,3,4 }	{2,4,5 }
{7,1,5 }	{7,2,6 }	{7,3,0 }	{7,4,1 }	{7,5,2 }	{7,6,3 }	{7,0,4 }
{7,2,3 }	{7,3,4 }	{7,4,5 }	{7,5,6 }	{7,6,0 }	{7,0,1 }	{7,1,2 }
{7,4,6 }	{7,5,0 }	{7,6,1 }	{7,0,2 }	{7,1,3 }	{7,2,4 }	{7,3,5 }
{8,3,1 }	{8,4,2 }	{8,5,3 }	{8,6,4 }	{8,0,5 }	{8,1,6 }	{8,2,0 }
{8,6,2 }	{8,0,3 }	{8,1,4 }	{8,2,5 }	{8,3,6 }	{8,4,0 }	{8,5,1 }
{8,5,4 }	{8,6,5 }	{8,0,6 }	{8,1,0 }	{8,2,1 }	{8,3,2 }	{8,4,3 }

Table 4.5: Master keys for a $(3, 3, 9; 7)$-threshold scheme

and for a $(3, 3, v; m)$ threshold scheme that meets the upper bound on m. Imperfect schemes are also presented in their paper. Additional examples and information on threshold scheme based on Steiner systems may be found in [SS89], [CvO89], [SV88a], [SV88b], [DSV88] and [BV87].

4.2 Hierarchical Information

The hierarchical information threshold scheme based on a Steiner system, $\mathcal{S}(k, n, v)$, allows access to higher levels based on a greater number of participants. Let $k_1, \ldots k_j$ represent the thresholds for levels $1 \ldots j$. Level j is implemented using a $\mathcal{S}(k_j, n, v)$ Steiner system. Assume $\mathcal{S}(k_j, n, v)$ is partitionable into $\mathcal{S}(k_j - 1, n, v)$ which is also partitionable. Assume $\mathcal{S}(k_j - 1, n, v)$ is partitionable into $\mathcal{S}(k_j - 2, n, v)$ which is also partitionable and so on. Then, we eventually have $\mathcal{S}(k_j, n, v)$ which is partitionable into a $\mathcal{S}(k_{j-1}, n, v)$. In addition, $\mathcal{S}(k_{j-1}, n, v)$ is partitionable into $\mathcal{S}(k_{j-3}, n, v) \ldots \mathcal{S}(k_2, n, v)$, and $\mathcal{S}(k_1, n, v)$. Then, whenever k_1 partial keys are submitted to the master key constructor, a block in $\mathcal{S}(k_1, n, v)$ is identified and access to level 1 information is granted. When k_2 partial keys are submitted to the master key constructor, a block in $\mathcal{S}(k_1, n, v)$ as well as a larger block in $\mathcal{S}(k_2, n, v)$ is identified. Thus, those who submitted the k_2 partial keys are granted access to level 1 and to level 2. In general, when k_i partial keys are submitted, access is granted to level i information as well as to all levels below level i.

Evaluating the scheme by the criteria, the partial keys being distributed are not changed from the single level information threshold scheme. The master key constructor may have to store additional information in order to be able to identify all the partitioned blocks. However, Chen and Stinson [CS89], point out that if $v = n$, then each block of a $\mathcal{S}(k, n, v)$ is itself an $\mathcal{S}(k - 1, n, n)$. In this situation, the master

key constructor would be able to identify the various partitions by identifying the partial block defined by the partial keys. Thus, if block (x, y, z) where defined the access would not be as great as those would could define block (x, y) since (x, y, z) is only a portion of block (x, y). The major problem with this scheme is revealed when evaluating it by **criterion 5**. As pointed out by Chen and Stinson [CS89], little successful investigation has been accomplished in the area of solving the problem of decomposing Steiner systems. Furthermore, only a few Steiner systems are known for $k = 4$ and $k = 5$ and none are known for $k > 5$ [BV87].

Chapter 5

Error Correcting Codes

Methods for threshold schemes involving error correcting codes have also been presented. An error correcting code consists of a set of codewords also referred to as vectors and blocks. Assuming a binary code, the elements of the vectors belong to the set $\{0, 1\}$, the alphabet of the code. A generator matrix for an (a, b)-code is a $b \times a$ matrix whose rows are a vector space basis for the code where a-tuples of bits are embedded into b tuples to provide redundancy to allow the detection and correction of errors. The distance between two codewords, also known as the Hamming distance*, is the number of bits in which the two codewords differ. The Hamming distance of the code is the minimum distance between any two codewords. An error correcting code with distance d where $d \geq 2t + 1$ can correct t errors. The Hamming weight* of a vector is the number of non-zero coordinates or bits in the vector, denoted $w(s)$ for an error vector s. The Hamming weight for the error vectors $s_1, \ldots s_k$ is

$$W(\oplus \sum_{i=1}^{k} S_i) = t$$

where $\oplus$ is the bit by bit exclusive OR of the vectors [VvO89].

5.1 The Method

One approach is presented by Davida, DeMillo, and Lipton [DDL80]. The secret is assumed to be representable as $I * b$ information bits which are contained in a vector S of length L consisting of b blocks (groups of bits). The partial keys are also vectors of length L, represented as $s_1, \ldots s_n$. Each code vector or partial key differs from all other partial keys in at least d bits where $d \geq 2t + 1$, the distance of the code. The master key constructor is an (L, I, d) error correcting code algorithm. The partial keys are chosen such that the Hamming weight* of any k error vectors is t. Furthermore, the Hamming weight of any $k - 1$ vectors is $t + e$ where e is some residual error which forbids the correction by the master key constructor. Thus, the presentation of any k error vectors has a Hamming weight of t and is correctable. The master key constructor constructs $S \oplus S'$ where $S' = \oplus \sum_{i=1}^{n} s_i$. Then, it exclusive ORs this with the exclusive OR of the partial keys presented. If the threshold is met, an error correction algorithm obtains S.

McEliece and Sarwate [MS81] show that extensions and generalizations of Shamir's method [Sha79] can be obtained by the decoding algorithms used for Reed-Solomon codes* [1]. A Reed-Solomon code is the code generated by $g(x)$ where $g(x) = (x - \beta^{1+\alpha})(x - \beta^{2+\alpha}) \cdots (x - \beta^{\delta-1+\alpha})$ and $\beta \in F = GF(q), |\beta| = n$ (i.e. $\beta^n = 1$ but $\beta^s \neq 1$ for an positive $s < n$) and where $\delta \geq 2$ and $a \geq 0$ [VvO89]. In one form of the Reed-Solomon code, an information word or vector is $a = (a_0, a_1, \ldots a_{k-1})$ where the a_i's are elements of a finite field of order r, $F = \alpha_0, \alpha_1, \ldots \alpha_{r-1}$. The information word a is encoded into the codeword $S' = (s_1, s_2, \ldots s_r)$. The partial keys are $s_i = \sum_{j=0}^{k-1} a_j \alpha_i^j$. As in Shamir's scheme, the secret $S = a_0$. In this scheme, $a_0 = -\sum_{i=1}^{r-1} s_i$. If u $(k \leq u \leq n)$ partial keys are presented, t of which are in error, applying an error-

[1] Additional generalizations of Shamir's method may be found in [Ben86] [Kot85] [Mea88] [BL88].

and-erasure decoding algorithm reveals the master key provided that $k \leq u - 2t$ as in the previous error correcting based scheme. McEliece and Sarwate point out that Shamir's scheme [Sha79] is a special case in which the order of the field is prime and $t = 0$.

Evaluating the scheme by the criteria, the partial keys are of the same length as the master key. According to McEliece and Sarwate, standard algorithms exist for the master key constructor that require $O(n^2)$ as well as an efficient $O(n \log^2 n)$ algorithm [MS81].

Denes and Keedwell [DK90] show the connection of the above schemes to Golomb-Posner codes. This is achieved through the generator matrix for the extended Reed-Solomon code corresponding to a threshold scheme. If there are only two rows in this matrix, a minor substitution reveals it to be the codeword obtained by Golomb-Posner in [GP64]. Let α be the primitive element of $GF(q)$. The matrix in which k partial keys are need for a threshold is:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{q-2} \\ 0 & 0 & 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(q-2)} \\ . & . & . & . & . & \dots & . \\ 0 & 1 & 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \dots & \alpha^{(k-1)(q-2)} \end{pmatrix}.$$

If there are only two rows, the second row contains all the elements of the field. The resulting matrix is

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{q-2} \end{pmatrix}.$$

Denes and Keedwell proceed to show that if $\alpha_0 = 0$ and $\alpha_1 = 1$, then the codeword, obtained by adding α_i times row 1 to α_j times row 2 is

$$(\alpha_i, \alpha_j, \alpha_i + \alpha_1\alpha_j, \alpha_i + \alpha_2\alpha_j, \dots, \alpha_i + \alpha_{q-1}\alpha_j).$$

This is the codeword obtained in the Golumb-Posner [GP64] construction using the entries of the ith row and the jth column of the members of the complete set of $q-1$ mutually orthogonal Latin squares* in $GF(q)$ [DK90]. A Latin square of order n is a $n \times n$ matrix in which each row and column is a permutation of its row or column elements. Two Latin squares are mutually orthogonal if the superimposition determines another Latin square in which all the entries are distinct. The construction of the extended Reed-Solomon code generator matrix from Latin squares is shown in Wu [Wu85]. Denes and Keedwell point out that when Latin squares are used, the threshold is always 2 (i.e. $k = 2$) due to the above connection [DK90].

An alternative method involving error correcting codes is presented by Harari [Har83]. The partial keys that are given out consist of multiple tuples of a bit (assuming binary representation of the secret) and bit location. When k partial keys are submitted, the undefined locations are arbitrarily set to 0. If enough partial keys are submitted, the decoding algorithm of the master key is able to correct the arbitrary bit to the correct value, correct the vector and thus reveal the secret. Table 5.1, from [Har83], shows examples of possible threshold schemes based on Reed-Solomon codes in terms of the maximum number of participants, minimum threshold, the length of the secret vector, and the number of bits each partial keys. The values are related to the maximum distance of each code. Additional details are available in Harari [Har83].

5.2 Hierarchical Authority

A hierarchical authority threshold scheme is proposed by Davida, DeMillo and Lipton [DDL80]. This is accomplished by giving users at different levels different keys such that if level i requires k_i partial keys for the threshold, the the partial keys for level i

Number of bits in the Secret	Number of bits per partial key	Maximum value of n	Minimum value of k
47	9	4	2
101	10	10	4
149	10	18	11
197	8	24	15
293	8	35	19

Table 5.1: Possible systems based on Reed-Solomon codes

are such that the the Hamming weight of any k_i of them equals t. Furthermore, the Hamming weight of any $k_i - 1$ of them is $t + e_i$. This can best be summarized by Table 5.2.

Authority Level	Threshold	Weight of k_i partial keys
1	k_1	$W(\oplus \sum_{j=1}^{k_1} s_j) = t$
2	k_2	$W(\oplus \sum_{j=1}^{k_2} s_j) = t$
3	k_3	$W(\oplus \sum_{j=1}^{k_3} s_j) = t$
.	.	.
L	k_L	$W(\oplus \sum_{j=1}^{k_L} s_j) = t$

Table 5.2: Hierarchical Authority Levels and Weights

The authors also state that collusion of users at different levels may take place or may be prohibited by selecting vectors that add to the error if members from different levels work together. No details on the construction of vectors for the allowance or prohibition of users of different levels are provided in the paper.

5.3 Hierarchical Information

The hierarchical information threshold scheme is based on the scheme proposed by Harari [Har83]. This is a hierarchical authority and hierarchical information scheme. Thus, participants with more authority are required in order for a higher level information. As in the scheme proposed by Harari, the partial keys consist of multiple tuples of bits (assuming binary representation of the secret) and bit locations. The restriction on the partial keys is that for a participant who only has access to level i, the locations of all of their bits are between location 1 and location $|S_i|$ where $|S_i|$ is the size of the vector for S_i, the secret for level i. If a participant has authority for level j, $j > i$, then the locations of all of their bits are between location 1 and location $|S_j|$. Since $j > i$, the first $|S_i|$ bits of $S_j = S_i$. This permits those of higher authority to also access the lower levels. As in Harari's scheme, when k_i partial keys with authority for at least level i are submitted, the undefined locations are arbitrarily set to 0 (where k_i is the threshold for level i). If enough partial keys are submitted, the decoding algorithm of the master key is able to correct the arbitrary bits and thus correct the vector and reveal S_i by correcting the secret for the bits 1 through $|S_i|$. When k_j partial keys of authority for at least level j are presented, the master key constructor once again arbitrarily sets the undefined bits to 0. A decoding algorithm is able to correct the code for bits 1 though $|S_j|$. Thus, secrets S_i and S_j as well as all $S_\alpha, \alpha < j$ are revealed. One restriction to the scheme is that $|S_i| + d < |S_{i+1}|$. If there are not at least d bits separating the size of one level of the scheme to the next, then if all participants of level i entered their partial keys, the decoding algorithm may be able to correct the next level secret as well since only d bits, the distance of the code, are undefined and the vector is correctable for level S_{i+1}.

The partial key for the higher levels must have the minimum number of bits for

each level below its maximum level and thus the partial key is larger.

Chapter 6

Chinese Remainder Theorem

The final method is based on the Chinese Remainder Theorem*. The Chinese Remainder Theorem is as follows: Let $n_1, n_2, \ldots, n_k$ be positive integers such that $gcd\{n_i, n_j\} = 1$ for $i \neq j$. If $n = n_1 n_2 \cdots n_k$ and a, $b_1, b_2, \ldots, b_k$ are integers, then there exists a unique integer b such that $a \leq b \leq a + n$ and $b \equiv b_i \bmod n_i$ for $i = 1, \ldots, k$. [Fis77]

6.1 The Method

The first method is presented by Asmuth and Blakley [AB82]. The secret is once again to be representable as a number, S. A prime p is chosen. The partial keys in this scheme are congruence classes of a number associated with S. The n partial keys are s_1 to s_n such that $s_i \equiv S' \bmod d_i$, where d_1 through d_n are chosen with the following constraints:

- $d_i < d_{i+1} \quad \forall i \neq j$

- $gcd(d_i, d_j) = 1 \ \ \forall i \neq j$ (pairwise relatively prime)
- $gcd(p, d_i) = 1 \ \ \forall i$
- Let $M = \prod_{i=1}^{k} m_i$ such that $M > p \prod_{i=1}^{k-1} m_{n-i+1}$

The master key is $S' = S + Ap$ where A is an arbitrarily chosen integer subject to the condition that $0 \leq S' < M$ (i.e. A is in the range [0, (M/p)-1]. The master key is also assumed to be less then p and greater than or equal to 0.

The master key S', can be constructed when k partial keys, $s_1, \ldots, s_k$ (without loss of generality), are presented. Specifically, by the Chinese remainder theorem, $S' \equiv (s_1 z_1 + s_2 z_2 + \cdots + s_k z_k) \bmod w$ where $w = \prod_{i=1}^{k} d_i$ and $z_i = \frac{w}{d_i} * y_i$ where y_i = the inverse of $\frac{n_i}{d_i}$ and d_i (i.e. y_i satisfies $((\frac{n_i}{d_i} * y_i) \bmod d_i \equiv 1$. This is solved by extended Euclidean algorithm.) The secret is then $S = S' - Ap$.

Evaluating the scheme by **criterion 1**, the partial keys, s_i, are given modulus the secret, S (since $s_i \equiv S \bmod d_i, s_i < S$), however, the s_i's and d_i's must both be stored . Thus, the partial keys are twice the size of the master key. The master key in this scheme requires the storage of the secret, as well as A, p and S'. Thus, assuming A, p and S' require as much storage as the secret, the master key constructor for the secret requires four times the storage as the secret itself. With respect to **criterion 2**, Asmuth and Blakely state that the master key construction algorithm is $O(k)$.

The following example is presented in Denning [Den82]. The secret equals 3, n or the number of partial key holders equals 3, the threshold k equals 2. The random prime chosen, p, is 5 and the random integer, A equals 9. Thus $S' = S + Ap = 3 + (9 * 5) = 48$. The d_i's chosen and the related partial keys, s_i are as follows:

$$d_1 = 7 \qquad s_1 = 48 \bmod 7 \equiv 6$$
$$d_2 = 9 \qquad s_2 = 48 \bmod 9 \equiv 3$$

$$d_3 = 11 \qquad s_3 = 48 \bmod 11 \equiv 4$$

The master key can be calculated using any two partial keys since k equals 2. Choosing s_1 and s_3, $w_1 = d_1 * d_3 = 7 * 11 = 77$. Using the extended Euclidean algorithm to find y_i and y_2 where y_1 satisfies $\frac{77}{7} * y_1 \bmod 7 \equiv 1$; y_2 =satisfies $\frac{77}{11} * y_2 \bmod 11 \equiv 1$; thus $y_1 = 2; y_2 = 8$. It follows that $z_1 = 11 * 2 = 22$ and $z_2 = 7 * 8 = 56$. Thus, the master key,

$$S' \equiv [22 * 6 + 56 * 4] \bmod 77$$

$$\equiv 356 \bmod 77 \equiv 48 = S'.$$

The secret

$$S = 48 - (9 * 5) = 3$$

as required.

Extending the example for three partial keys, we choose s_1, s_2, and s_3. We find $w = 693, y_1 = 1, y_2 = 2, y_3 = 7$, and $z_1 = 99, z_2 = 154$, and $z_3 = 441$. Thus

$$S' \equiv (6 * 99 + 3 * 154 + 4 * 441) \bmod 693 \equiv 48 = S'$$

As expected, the secret

$$S = 48 - (9 * 5) = 3.$$

The second scheme based on the Chinese remainder theorem is presented by Mignotte [Mig83]. This scheme can be described as follows. Let A be the ring of integers, $\mathcal{Z}$, and let I be an ideal* of A. Also, let $I_j = d_j\mathcal{Z}$ and $1 \leq j \leq n$ and $d_1, \ldots d_n$ are coprime in pairs. The master key or the secret, S, is then an element of $\mathcal{Z}$, where $a \leq S \leq b$; $a, b \in \mathcal{Z}$. The partial keys are represented as s_j where $s_j \equiv S \bmod d_j$ where $1 \leq j \leq n$. Once again, $d_1, \ldots, d_n$ are chosen such that the

product of any k of the d_j is greater than b and that the product of $(k-1)$ of the d_j is less than a. Then, the secret S is equivalent to $s_1 z_1 + \cdots + s_k z_k \bmod d_1 \ldots d_k$. The z_i's are once again obtained using the extended Euclidean algorithm.

Mignotte states that if only $k-1$ partial keys are used, then there exists at least $\frac{b-a}{d_1 d_2 \cdots d_{k-1}}$ values which satisfy $S \equiv (s_1 z_1 + \cdots + s_{k-1} z_{k-1}) \bmod d_1 \cdots d_{k-1}$ in the interval $[a, b]$ (**criterion 4a**). Thus, this scheme is not perfect. Evaluating the scheme by **criterion 1**, the partial keys are given modulus the secret as in the previous scheme and require the same storage space. However, the master key in this scheme requires only the storage of the secret.

The previous example can be adapted to show this scheme. Let the secret, S, equal 48, n equal 3, and k equal 2. Let a, the upper bound on the product of any $k-1$ partial keys equal 6. Let b, the lower bound on the product of any k partial keys equal 62. d_1 through d_5 and s_1 through s_5, where $s_i \equiv S \bmod d_i$ could be as follows:

$$\begin{aligned} d_1 &= 7 & s_1 &= 48 \bmod 7 \equiv 6 \\ d_2 &= 9 & s_2 &= 48 \bmod 9 \equiv 3 \\ d_3 &= 11 & s_1 &= 48 \bmod 11 \equiv 4 \end{aligned}$$

Once again choosing s_1 and s_3, the y_i's and z_i's are the same as the previous example and thus,

$$S \equiv (22 * 6 + 56 * 4) \bmod 77 \equiv 356 \bmod 77 = 48 = S$$

6.2 Validating Shadows

Asmuth and Bloom [AB83] state that there is an extremely small probability that two distinct sets of k partial keys would yield the same, but incorrect master key.

In a (20,30)-threshold scheme with six partial keys being in error, the probability of this happening is $\frac{\binom{24}{30}}{\binom{30}{20}} < \frac{1}{2800}$. An alteration to the scheme presented in section 1 eliminates partial keys found to be incorrect prior to distribution.

The constraints for choosing d_1 through d_n are changed slightly to the following constraints:

- $d_i < d_{i+1} \quad \forall i \neq j$
- $gcd(d_i, d_j) = q_{i,j} \quad \forall i \neq j$
- $gcd(p, d_i) = 1 \quad \forall i$
- $lcm(\text{any } k \text{ of the } d_i) > p * lcm(\text{any } k-1 \text{ of the } d_i)$

Thus, by changing the second constraint and thus not requiring all the d_i's to be relatively prime, one may validate the partial keys. The validation occurs since if $q_{i,j}$ is known, then $s_i \equiv s_j \bmod q_{i,j}$. Asmuth and Bloom state that the congruence class of most if not all of the $q_{i,j}$ would change if there was a random error in s_i.

To construct the d_i's to aid in defeating tampering, choose $\binom{n}{r}$ pairwise relatively prime integers. A set of r of these integers is represented as $\{i_1, i_2, \ldots, i_r\}$ the product of which corresponds to the integer $q_{i_1,\ldots i_r}$. The modulus, d_j, is defined as: $d_j = \prod_{j \in \{i_1,\ldots i_r\}} q_{i_1,\ldots i_r}$.

6.3 Hierarchical Information

The following hierarchical threshold scheme, based on the Chinese Remainder Theorem, is an extension to the system proposed by [Mig83]. To get a $(k_1, k_2, \ldots k_m, n)$ threshold scheme where $(k_1, k_2, \ldots k_m)$ are various access levels, the partial keys for

level i are s_{i_j} where $1 \leq j \leq n$ and $s_{i_j} \equiv S_i \bmod d_j$. The secrets are $S_1, S_2, \ldots S_m$ where $c_1 \leq S_1 \leq c_2$ and $c_3 \leq S_2 \leq c_3 \cdots c_{2m-1} \leq S_m \leq c_{2m}$ and where $c_1, c_2, \ldots c_{2m}$ are integers, $0 \leq c_1 \leq c_2 \cdots \leq c_{2m}$. The d_i's, $d_1, \ldots, d_m$ are taken such that

- the product of any $k_1 - 1$ of the d_j are less than c_1,
- the product of any k_1 of the d_j are greater than c_2,
- the product of any $k_2 - 1$ of the d_j are less than c_3,
- the product of any k_2 of the d_j are greater than c_4,

$\bullet$

$\bullet$

$\bullet$

- the product of any $k_{m-1} - 1$ of the d_j are less than c_{2m-3},
- the product of any k_{m-1} of the d_j are greater than c_{2m-2},
- the product of any $k_m - 1$ of the d_j are less than c_{2m-1},
- the product of any k_m of the d_j are greater than c_{2m}.

When $k_i, 1 \leq i \leq m$, of the s_j are known, then

$$S_\alpha \equiv s_{\alpha_1} z_1 + \cdots + s_{\alpha,k_i} z_{k_i} \bmod d_1 d_2 \ldots d_{k_i}$$

where $s_{\alpha,i}$ denotes the portion of the partial key, s_i, for security level α. And the z's are found using the extended Euclidean algorithm. The s_i's are dependent on the secret of each level and thus if the storage requirements for the partial keys for a single

level of information are γ, for m levels, they are $m * \gamma$. Hierarchical authority may be also be implemented with the hierarchical information by simply not distributing a partial key for the level that the participant shouldn't be able to access.

An example for three levels of information, five participants with level one requiring a (2,5)-threshold scheme, level two requiring a (3,5)-threshold scheme and level three requiring a (4,5)-threshold scheme follows. Let the secrets, $S_1 = 47, S_2 = 356$, and $S_3 = 3999$. The following d_i's may be used and the corresponding s_i are listed.

d_i	$s_{1,i} \equiv 47 \bmod d_i$	$s_{2,i} \equiv 356 \bmod d_i$	$s_{3,i} \equiv 3999 \bmod d_i$
$d_1 = 7$	5	6	2
$d_2 = 9$	2	5	3
$d_3 = 11$	3	4	6
$d_4 = 13$	8	5	8
$d_5 = 17$	13	16	4

Table 6.1: Partial Keys for Hierarchical Information

The c_i's used are $c_1 = 6, c_2 = 62, c_3 = 222, c_4 = 692, c_5 = 2432$, and $c_6 = 9008$.

For level one, using partial keys $s_{1,1}$ and $s_{1,5}$, the y_i's must first be determined as described in section 1. y_1 satisfies $\frac{119}{7} * y_1 \bmod 7 \equiv 1$ and y_5 satisfies $\frac{119}{17} * y_5 \bmod 17 \equiv 1$. Using the extended Euclidean algorithm, $y_1 = 5.$ and $y_5 = 5$. The z_i's are

$$z_1 = \frac{119}{7} * 5 = 85$$

$$z_5 = \frac{119}{17} * 5 = 35.$$

The secret for level 1,

$$S_1 = (5 * 85 + 35 * 13) \bmod 119 \equiv 47 = S_1.$$

For level two, using partial keys $s_{2,2}, s_{2,3}$, and $s_{2,4}; w = 9 * 11 * 13 = 1287$, the y_i's are determined to be $y_2 = 8, y_3 = 8$, and $y_4 = 5$. The z_i's are

$$z_2 = \frac{1287}{9} * 5 = 1144$$

$$z_3 = \frac{1287}{11} * 4 = 936,$$

$$z_4 = \frac{1287}{13} * 5 = 495.$$

Thus the secret

$$\equiv (5 * 1144 + 4 * 936 + 495 * 5) \bmod 1287 \equiv 356 = S_2.$$

For the top level using partial keys $s_{3,1}, s_{3,2}, s_{3,3}$, and $s_{3,4}; w = 7*9*11*13 = 9009$, the y_i's are determined to be

$$y_1 = 6, y_2 = 5, y_3 = 9, y_4 = 10.$$

The z_i's where $z_i = \frac{w}{d_i} * y_i$ are:

$$z_1 = 7722, z_2 = 5005, z_3 = 7371, z_4 = 6930.$$

As expected,

$$S = (2 * 7722 + 3 * 5005 + 6 * 7371 + 8 * 6930) \bmod 9009 \equiv 3999 = S.$$

An alternate hierarchical threshold scheme using the Chinese Remainder Theorem utilizes the same s_i's for all levels of the hierarchy. In order to implement their system with a hierarchy of authority as well, each s_i is given modulus the highest level authority permitted for that partial key holder. The highest level in the overall scheme, m, is the same as the above scheme. The first through $(m-1)$ levels' master key is S_i, for level i, which is a set which contains all possible solutions for valid

partial keys for level i to $s_1 z_1 + \cdots s_{k_i} z_{k_i} \bmod d_1 d_2 \ldots d_{k_i}$ where k_i is the threshold for level i.

For each of the lower levels, γ, the order of S_γ is at most $\binom{n}{k_\gamma}$ (S_γ is smaller when all n participants are not granted authority for level γ). While the storage space for the partial keys remains the same as for single level information, the space required for the master key greatly increases. The computation required to find the S_i's to set up the scheme is equivalent to the required time for the master key constructor. However, this must be computed $\binom{n}{k_i}$ times for each of the i lower levels. Thus, if the master key constructor requires an average time of T, there is added overhead time of $\prod_{i=1}^{m-1} \left\{ \binom{n}{k_i} * T \right\}$ added to the set-up time for this scheme.

An example for 4 partial keys where level one requires (2,4)-threshold and level two requires a (3,4) threshold follows. Let $S_1 = 48, S_2 = 356$. Let the d_i's and the partial keys, $s_1 \cdots s_4$ be the following.

d_i	$s_{i1} \equiv 356 \bmod d_i$
$d_1 = 7$	6
$d_2 = 9$	5
$d_3 = 11$	4
$d_4 = 13$	5

Table 6.2: Partial Keys for Alternate Hierarchical Information Scheme

For level two, the secret would be revealed as before. There are $\binom{4}{2} = 6$ elements in S_1 to be found. To find the elements of S_1, we must solve $S' = s_i z_i + s_j z_j \bmod d_i d_j$ for all unordered combinations of $\{1, 2, 3, 4\}$. Using the partial keys s_1 and $s_2, w =$

$63, y_1 = 4, y_2 = 4$. Thus the z_i's are as follows:

$$z_1 = \frac{63}{7} * 1 = 36$$

$$z_2 = \frac{63}{9} * 2 = 28.$$

Thus,

$$S' = (6 * 36 + 5 * 28) \bmod 63 \equiv 41 \in S_1$$

Similarly, to find a second element of S_1, using partial keys $s_3 s_4$, $w = 143, y_3 = 6, y_4 = 6, z_3 = 78, z_4 = 66$ and $70 \in S_1$.

The rest of the members of S_1 are found in the same manner.

Chapter 7

Conclusion

Numerous uses for threshold schemes are presented. These uses range from protecting encryption keys to preventing military and management actions without proper authority. Several general methods for implementing such schemes are examined in the literature. The implementations have different mathematical foundations. In this thesis we looked at methods based on polynomial interpolation, on the intersection properties in finite geometrics, on the more general Steiner systems, on those utilizing error correcting codes as well as the Chinese Remainder Theorem.

The are several things one needs to consider when setting up a hierarchical information threshold scheme. The first concerns the requirements needed for the higher level information. The second is a set of concerns regarding the criteria as defined in chapter 1. Table 7.1 and table 7.2 present summaries of our research with regard to these concerns. Table 7.1 is a summary of the threshold schemes with hierarchical information presented in this thesis. In this table, an 'X' indicates a threshold scheme with that type of access is presented in this thesis. According to the information presented in this table, we observe that, in terms of the types of thresholds used to

implement hierarchical information, the method based on Steiner systems seems to be most restrictive in the sense that there are no obvious ways to implement hierarchical information based on strictly more authoritative participants other than to distribute multiple keys.

In addition to determining the type of threshold, there may be additional constraints to the type of threshold scheme one may use. This is the aforementioned 'second set of concerns.' We have identified several criteria one may consider when implementing a threshold scheme particularily with hierarchical information. Table 7.2 summarizes the evaluation of the methods presented in this thesis in terms of these criteria. If **criterion 1**, the size of the partial key, is important as well as **criterion 2**, the master key construction time, one might consider the approaches based on finite geometries or Steiner systems. If only **criterion 1** is important, the second approach discussed in section 6.3, based on the Chinese Remainder Theorem implemented using the same s_i's and d_i's for each level, may be used. However, if **criterion 1** is not of concern but the set up time is, any of the approaches except the 2nd Chinese Remainder Theorem approach could be utilized. The chart also reminds us by **criterion 5** that little successful investigation has been accomplished in the area of solving the problem of decomposing Steiner systems [CS89]. Specifically, the Steiner systems needed are those which are partitionable into Steiner systems which are themselves partitionable. Furthermore, only a few Steiner systems are known for $k = 4$ and $k = 5$ and none are known for $k > 5$ [BV87]. Overall, the finite geometry based approach to hierarchical information appears to be the best in terms of types of thresholds that can be used as well as in terms of the size of the keys.

Ideally, any of these methods would be usable for all purposes. Thus, future work includes developing schemes which can optimize the size of the partial keys and minimize the computational time and overhead for the master key and master key

	more partial key holders	more authoritative partial key holders	more partial key holders with more authority
Interpolating Polynomials	X	X	X
Finite Geometry		X	X
Steiner systems	X		
Error Correcting Codes		X	
Chinese Remainder Theorem	X		X

Table 7.1: Hierarchical Information Schemes Presented

	Criterion 1 Size of partial key	Criterion 2 Master Key construct. time	Criterion 3 Storage Req. for partial and master key	Criterion 4 Amount of info. revealed by $< k-1$ keys	Criterion 5 Variety of known schemes of this type
Interpolating Polynomials	I $\gamma + L\gamma$	S	I/I	S	N.A.
Finite Geometries	S	S	S/S	S	N.A.
Steiner systems	S	S	S/S	S	very limited
Error Correcting Codes	I	S	S/S	S	N.A.
Chinese Remainder Theorem	I(1st) S(2nd)	S(1st) I(2nd)	I/S (1st) S/I (2nd)	S	N.A.
I=increased: S=same as uni-level information scheme					

Table 7.2: Hierarchical Information Schemes evaluated by Criteria

constructor. Additionally, one would like to be able to use any of the methods to implement any type of hierarchical information threshold scheme. As the research in the area of Steiner systems advances, this approach may become more viable of an approach to hierarchical information threshold schemes. Additional work is needed to find out other natural implementations of hierarchical information threshold schemes. The polynomial interpolation method and the Chinese Remainder theorem approach may be implementable with smaller partial and master keys. The Chinese Remainder theorem is polynomial interpolation in a different domain. Unification of the two methods along with all the variations is also a topic of future research. Furthermore, the finite geometries seem to provide an easy method for storing the master key without storing the whole master key. Determining if this is possible for the other methods is another topic for future research. Several uses for threshold schemes have been proposed. Future research includes determining which of these uses may be implemented with each of the methods. In addition, there is a need to determine exactly how practical are each of the methods.

Another method not examined in this thesis is based on graph theory. Such a graph theory based method has been proposed in [BS89]. The partial keys in this scheme are the vertices of the graph. Pairs of participants, represented as edges in a graph, are able to compute the master key, the graph. A general result is proven for the information rate* which is at least $2/(n+3)$, where n is the maximum degree in a graph, G. The information rate is the amount of information being distributed as partial keys as compared to the size of the master key. While there has been very limited research into this type of implementation, this method may prove to be very promising in terms of hierarchical information.

Some papers present threshold schemes which deal with cheating. There are various forms of cheating to prevent. These include reconstruction of legal but incorrect

master keys, unauthorized control of key distribution, distribution of invalid partial keys as well as acquiring unauthorized information about the set of partial keys. Additional research is needed to accommodate these features into hierarchical information threshold schemes.

Also reviewed in this thesis are some methods which allow a threshold scheme to implement various levels of authority or to permit conditional distribution of authority. The geometrical hierarchical authority schemes seem to naturally adapt to hierarchical information. As more is known about hierarchical authority implementations (other than the distribution of more partial keys to more authoritative participants), there will be an increased amount of future work to determine if the relationship may be extended to other methods as well as for the implementation of hierarchical information. An additional topic for future research includes expanding the idea of yes-no threshold schemes to other methods, to accomodate the detection and prevention of cheaters as well as to possible expand hierarchical information threshold schemes to yes-no hierarchical information schemes.

Appendix A

Terms

1. **block** [BM82] - a connected graph that has no cut vertices.

2. **Chinese Remainder Theorem** [Fis77] -Let $n_1, n_2, \ldots, n_k$ be positive integers such that $gcd\{n_i, n_j\} = 1$ for $i \neq j$. If $n = n_1 n_2 \cdots n_k$ and a, $b_1, b_2, \ldots, b_k$ are integers, then there exists a unique integer b such that $a \leq b \leq a + n$ and $b \equiv b_i \bmod n_i$ for $i = 1, \ldots, k$.

3. **k-compatible** [SV88b] [SV88a] - two hypergraphs, A_1 and A_2, are considered to be k-compatible if $A_1(k-1) = A_2(k-1)$ and $A_1(k) \cap A_2(k) = \emptyset$ where $A(k)$ equal the set of all subsets of vertices of order k.

4. **Desarguesian plane** [BJL85] planes arising from fields, if the field is finite then the plane is also considered a Pappian plane.

5. **A (finite) generalized quadrangle (GQ) of order** (σ, τ) [DSV88] -an incidence structure which satisfies the following axioms:

   (a) Each point is incident with exactly $1 + \tau$ lines ($\tau \geq 1$) and two distinct points are incident with at most one line.

(b) Each line is incident with exactly $1 + \sigma$ points ($\sigma \geq 1$) and two distinct lines are incident with at most one point.

(c) $\forall x$ and $\forall L$, where x is a point and L is a line, which are not incident with each other, there exists a unique line which is incident with both x and a (unique) point on L.

6. **finite geometry** [Tul67] - a geometry defined in terms of a system of axioms and undefined terms which limits the set of elements(such as points and lines) to a finite number [Tul67].

7. **Hamming distance** [VvO89] - the number of coordinate positions in which two codewords or vectors differ also known as the minimum distance. The Hamming distance of a code is the minimum of the Hamming distance between any two codewords in the code.

8. **Hamming weight** [VvO89]- the number of non-zero coordinates of the error vector, s, denoted $w(s)$.

9. **hyperplane** - the largest proper subspace of R^m whose dimension is $m - 1$. (eg. a line in R^2).

10. **Ideal** (of a ring) - A is an ideal if it is a subring of a ring R such that for every r in R, and for every a in A, ra and ar are in A.

11. **incidence structure** [DSV88] - an incidence structure, I, is a subset of $p \times b$ where p is a set of points and b is a set of blocks.

12. **information rate** [BS90] - the amount of information being distributed as partial keys as compared to the size of the master key.

13. **Latin square of order** n [Wu85] - is a $n \times n$ matrix in which each row and column is a permutation of it row or column elements. An example of a latin square of order 3 is:

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$$

14. **mutually orthogonal latin squares** [Wu85] - two latin squares are mutually orthogonal if the superimposition determines another latin square in which all the entries are distinct.

15. **perfect threshold scheme** [SV88a], [SS89] and [BS89]- If the $k-1$ participants pool their information, they have no more knowledge than a complete outsider.

16. **Reed-Solomon code** [VvO89] - The code generated by $g(x)$ where $g(x) = (x - \beta^{1+\alpha})(x - \beta^{2+\alpha}) \cdots (x - \beta^{\delta-1+\alpha})$ and $\beta \in F = GF(q), |\beta| = n$ (i.e. $\beta^n = 1$ but $\beta^s \neq 1$ for an positive $s < n$) and where $\delta \geq 2$ and $a \geq 0$.

17. **Steiner system** $\mathcal{S}(t, w, v)$ - A simple w-uniform hypergraph on v points such that every t-subset of points define a unique block*.

18. **incidence matrix** [BJL85] - Let D be a finite structure and label the points as $p_1 \ldots p_v$ and let the blocks be labeled as $B_1, \ldots B_b$. The matrix $M = (m_{ij})$ where $i = 1, \ldots, v;\ j = 1, \ldots, b$. The incidence matrix for D is then defined by

$$m_{ij} := \begin{cases} 1 & \text{if } p_i \ I \ B_j \\ 0 & \text{otherwise} \end{cases}$$

Where $p_i \ I \ B_j$ indicates that $(p, B) \in I \subseteq V \times B$ where V is the set of points.

Bibliography

[AB82] C.A. Asmuth and G.R. Blakley. Pooling, splitting and reconstructing information to overcome total failure on some channels of communication. In *Proc. IEEE Computer Society 1982 Symp. on Security and Privacy*, pages 156–169, 1982.

[AB83] C.A. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Trans. Info. Theory*, IT-29(2):208–210, March 1983.

[AHU74] A. Aho, J. Hopcroft, and J. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Mass., 1974.

[BD86] G.R. Blakley and R.D. Dixon. Smallest possible message expansion in threshold schemes. In A. M. Odlyzko, editor, *Advances in Cryptology*, pages 266–274, Berlin, 1986. Springer-Verlag. Crypto '86, Santa Barbara, August 11-15, 1986.

[Ben86] J.C. Benaloh. Secret sharing homorphisms: Keeping shares of a secret secret. In A. M. Odlyzko, editor, *Advances in Cryptology*, pages 251–260, Berlin, 1986. Springer-Verlag. Crypto '86, Santa Barbara, August 11-15, 1986.

[Beu] A. Beutelspacher. Applications of finite geometry to cryptography. preprint.

[Beu88] A. Beutelspacher. Enciphered geometry: Some applications of geometry to cryptography. In *Annals of Discrete Mathematics volume 37*, pages 59–68. North-Holland, 1988.

[Beu89] A. Beutelspacher. How to say 'no'. In *Advances in Cryptology*, Berlin, 1989. Springer-Verlag. Proceedings of Eurocrypt 1989, April 11-13, 1989: Houthalen, Belgium; to appear.

[BJL85] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory.* Bibliographisches Institut Mannheim, Vienna, Austria, 1985.

[BL88] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology*, pages 27–35, 1988. Crypto '88, Santa Barbara, August 21-25, 1988.

[Bla79] G.R. Blakley. Safeguarding cryptographic keys. *Proceedings AFIPS 1979 national Computer Conference*, 48:313–317, June 1979. New York, NY.

[Bla80] G.R. Blakley. One-time pads are key safeguarding schemes, not cryptosystems: Fast key safeguarding systems (threshold schemes) exists. In *Proc. IEEE Computer Society 1980 Symposium on Security,and Privacy*, 1980. Oakland, CA, April 14-16.

[BM82] J.A. Bondy and U.S.R. Murty. *Graph Theory with Applications.* North Holland, New York, 1982.

[BM85] G.R. Blakley and C. Meadows. Security of ramp schemes. In G.R. Blakley and D. Chaum, editors, *Advances in Cryptology Volume 196*, pages 242–268, Berlin, August 1985. Springer-Verlag. Proceedings of Crypto '84, Santa Barbara , CA.

[BS81] G. Blakley and L. Swanson. Security proofs for information protection systems. In *Proc. IEEE Computer Soc. 1981 Symp. on Security and Privacy*, pages 75–88, 1981. Oakland, CA, April 27-29, 1981.

[BS89] E. F. Brickell and D. R. Stinson. The detection of cheaters in threshold schemes. In *Congressus Numerantium vol. 68-69*, to appear 1989. 18th Annual Conference on Numerical Mathematics and Computing, Sept. 29-Oct 1, Winnipeg, Canada.

[BS90] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. Technical Report 106, University of Nebraska - Lincoln, May 1990. Report Series.

[BV87] A. Beutelspacher and K. Vedder. Geometric structures as threshold schemes. In *Proc. 1987 IMA Conf. on Cryptography and Coding Theory*, Cirencester, England, to appear 1987. Oxford University Press.

[BV89] A. Beutelspacher and K. Vedder. Geometric structures as threshold schemes. *Cryptography and Coding*, conference series 20:255–268, 1989. Based on the Proceedings of the conference held by The Institute of Mathematics and Its Applications, Royal Agricultural College, Cirencester, December 15-17, 1986.

[CCD88] D. Chaum, C. Crepeau, and I. Damgard. Multiparty unconditionally secure protocols. In *SIAM Final Program Abstracts: Minisymposia*, page A8, 1988. 4th SIAM Conference on Discrete Mathematics, San Francisco, CA, June 13-16, 1988.

[CS89] D. Chen and D.R. Stinson. Recent results on combinatorial constructions for threshold schemes. preprint, 1989.

[CvO89] C. J. Colbourn and P. C. van Oorschot. Applications of combinatorial designs in computer science. *ACM Computing Surveys*, 21(2):223 – 250, June 1989.

[DDL80] G.I. Davida, R.A. DeMillo, and R.J. Lipton. Protecting shared cryptographic keys. In *Proc. IEEE Computer Society 1980 Symp. on, Security and Privacy*, pages 100–102, 1980. Oakland, Ca, April 14-16, 1980.

[Den82] D. Denning. *Cryptography and Data Security.* Addison-Wesley, Reading, Mass., 1982.

[DK90] J. Denes and A.D. Keedwell. On Golomb-Posner codes and a remark of W.W. Wu about secret sharing systems. *IEEE Transactions on Communications*, 38(3):261–262, March 1990.

[DSV88] M. De Soete and K. Vedder. Some new classes of geometrical threshold schemes. In *Proc. Eurocrypt '88*, pages 389–401, 1988. May 25-27, 1988, Davos, Switzerland.

[Eck] A. Ecker. Tactical configurations and threshold schemes. Preprint.

[Fel87] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings 28th Annual Symposium on Foundations of Computer Science*, pages 427–437, Washington, D.C., 1987. IEEE Computing Society Press. Los Angeles, CA, October 12-14, 1987.

[Fis77] J.L. Fisher. *Application-Oriented Algebra.* Crowell, Harper, & Row, New York, 1977.

[GP64] S. Golomb and E. Posner. Rook domains, latin squares, affine planes, and error-distributing codes. *IEEE Transactions on Information Theory*, It-10:196–208, July 1964.

[Har83] S. Harari. *Secret Sharing Systems*, pages 105–110. Springer-Verlag, Wien, 1983. Giuseppe Longo, ed.

[IS90] I. Ingemarson and G.J. Simmons. How mutually distrustful parties can set up a mutually trusted shared secret scheme. *IACR Newsletter*, 7(1):4–8, January 1990.

[ISN87] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *Proc. IEEE Global Telecomunication Conf., Globecom '87*, pages 99–102, Washington, D.C., 1987. IEEE Communications Soc. Press. Tokyo, Japan, 1987.

[KGH83] E.D. Karnin, J.W. Greene, and M.E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, It-29(1):35–41, January 1983.

[Knu69] D. Knuth. *The Art of Computer Programing*, volume 2, Seminumerical Algorithms. Addison, Wesley, Reading, Mass., 1969.

[Kot85] S.C. Kothari. Generalized linear threshold scheme. In G.R. Blakley and D. Chaum, editors, *Advances in Cryptology*, pages 231–241, Berlin, 1985. Springer-Verlag. Crypto '84, Santa Barbara, CA, Aug. 19-24, 1984.

[Mea88] C. Meadows. Some threshold schemes without central key distributors. preprint, 1988.

[Mer83] M. Merritt. Key reconstruction. In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, *Advances in Cryptology*, pages 371–375, New York, 1983. Plenum Press. Crypto '82, Santa Barbara, CA, Aug. 23-25, 1982.

[Mig83] M. Mignotte. How to share a secret. *Cryptography*, pages 371–375, 1983. Workshop on Cryptography, Burg, Germany, March 29-April 2, 1982.

[MS81] R.J. McEliece and D.V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, September 1981.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[Sim88] G.J. Simmons. How to (really) share a secret. In *Advances in Cryptology*, pages 390–448, 1988. Crypto '88, Santa Barbara, August 21-25, 1988.

[Sim89] G. J. Simmons. Robust shared secret schemes. *Congressus Numerantium*, to appear 1989. 18th Annual Conference on Numerical Mathematics and Computing, September 29 - October 1, 1988, Winnipeg, Manitoba, Canada.

[Sim90] G.J. Simmons. Prepositioned shared secret and/or shared control schemes. In *Advances in Cryptology*, 1990. Proceedings of Eurocrypt '89, Houthalen, Belgium, April 11-13, 1989, to appear.

[Sma88] J. R. Smart. *Modern Geometries*. Brooks/Cole Publishing Co., Pacific Grove, California, 1988.

[SS89] P. J. Schellenberg and D.R. Stinson. Threshold schemes from combinatorial designs. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 5:143–160, 1989.

[SV88a] D.R. Stinson and S.A. Vanstone. A combinatorial approach to threshold schemes. *Siam J. Disc. Math*, 1(2):230–236, May 1988.

[SV88b] D.R. Stinson and S.A. Vanstone. A combinatorial approach to threshold schemes. In C. Pomerance, editor, *Advances in Cryptology*, pages 330–339, 1988. Crypto '87, Santa Barbara, CA, Aug. 16-20, 1987.

[Tei89] L. Teirlinck. A completion of Lu's determination of the spectrum for large sets of disjoint Steiner triple systems. preprint, 1989.

[Tul67] A. Tuller. *A Modern Introduction to Geometries*. D. Van Nostrand Company, Inc., Toronto, 1967.

[TW86] M. Tompa and H. Woll. How to share a secret with cheaters. In A. M. Odlyzko, editor, *Advances in Cryptology*, pages 261–265, Berlin, 1986. Springer-Verlag. Crypto '86, Santa Barbara, August 11-15, 1986.

[VvO89] S. Vanstone and P. van Oorschot. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, 1989.

[Wu85] W. W. Wu. *Elements of Digital Satellite Communication*, volume II. Computer Science Press, Maryland, 1985.

[Yam86] H. Yamamoto. On secret sharing schemes using (k,l,n) threshold schemes. *Electronics and Communications in Japan*, 69, Part 1(9):46–54, 1986. English translations of article that appeared in Trans.IECE, Vol. J68-A, No.9, 1985, pp. 945-952.

[Yam89] H. Yamamoto. Coding theorem for secret sharing communication systems with two noisy channels. *IEEE Transactions on Information Theory*, 35(3):572–578, May 1989.