SOME GENERALIZED MULTIPARTITE ACCESS STRUCTURES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

KEREM KAŞKALOĞLU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

MAY 2010

Approval of the thesis:

SOME GENERALIZED MULTIPARTITE ACCESS STRUCTURES

submitted by **KEREM KAŞKALOĞLU** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Ersan Akyıldız _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Department of Mathematics, METU**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy _____
Department of Mathematics, METU

Prof. Dr. Ferruh Özbudak _____
Department of Mathematics, METU

Assoc. Prof. Dr. Ali Aydın Selçuk _____
Department of Computer Engineering, Bilkent University

Assist. Prof. Dr. Zülfükar Saygı _____
Department of Mathematics, TOBB ETU

Dr. Burcu Gülmez Temur _____
Department of Mathematics, Atılım University

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: KEREM KAŞKALOĞLU

Signature :

ABSTRACT

SOME GENERALIZED MULTIPARTITE ACCESS STRUCTURES

Kaşkaloğlu, Kerem
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

May 2010, 52 pages

In this work, we study some generalized multipartite access structures and linear secret sharing schemes for their realizations. Given a multipartite set of participants with m compartments (or levels) and m conditions to be satisfied by an authorized set, we firstly examine the intermediary access structures arousing from the natural case concerning that any c out of m of these conditions suffice, instead of requiring anyone or all of the m conditions simultaneously, yielding to generalizations for both the compartmented and hierarchical cases. These are realized essentially by employing a series of Lagrange interpolations and a simple frequently-used connective tool called access structure product, as well as some known constructions for existing ideal schemes. The resulting schemes are non-ideal but perfect. We also consider nested multipartite access structures, where we let a compartment to be defined within another, so that the access structure is composed of some multipartite substructures. We extend formerly employed bivariate interpolation techniques to multivariate interpolation, in order to realize such access structures. The generic scheme we consider is perfect with a high probability such as $1 - O(q^{-1})$ on a finite field $\mathbb{F}_q$. In particular, we propose a non-nested generalization for the conventional compartmented access structures, which depicts a stronger way of controlling the additional participants.

Keywords: Secret Sharing Scheme, Multipartite Access Structures, Nested Multipartite Secret Sharing

ÖZ

BAZI GENELLEŞTİRİLMİŞ ÇOKPARTİLİ ERİŞİM YAPILARI

Kaşkaloğlu, Kerem
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Mayıs 2010, 52 sayfa

Bu çalışmada, bazı genelleştirilmiş çokpartili erişim yapıları ve bunları gerçekleyen doğrusal sır paylaşım şemalarını ele alıyoruz. İlk olarak, m kompartmanlı (veya seviyeli) ve bunlar üzerinde belirli m koşul bulunan bir çokpartili katılımcı kümesi için, tüm koşulların birden veya yalnızca herhangi birinin sağlandığı durumlar yerine, herhangi c tanesinin yeterli olma yaklaşımında, hem kompartmanlı hem de hiyerarşik durumlarda ortaya çıkan genelleştirilmiş ara erişim yapılarını inceliyoruz. Gerçekleştirmeler için ardısıra Lagrange interpolasyonları yanında erişim yapısı çarpımı olarak bilinen basit bir bağlayıcı araç ve varolan bazı erişim yapıları için önerilmiş olan bilinen inşalar kullanıyoruz. Ortaya çıkan şemalar, ideal olmasalar da sır paylaşım şemaları için önerilmiş mükemmellik özelliğini sağlamaktadırlar. Bunun yanısıra kompartmanları içerisinde başka kompartmanlar barındırma olanağı tanıdığımız içiçe çokpartili erişim yapılarını ele alıyoruz. Daha önce kullanılmış iki değişkenli interpolasyon tekniklerini çokdeğişkenli interpolasyonu kapsayacak şekilde düzenleyerek, bu bahsedilen erişim yapılarının gerçeklenmesini, $\mathbb{F}_q$ sonlu cismi üzerinde ideal olarak ve $1 - O(q^{-1})$ gibi yüksek bir olasılıkla mükemmel olacak şekilde sağlıyoruz. Bunun yanısıra, geleneksel kompartmanlı erişim yapılarında kompartmanların belirlenen eşik değerleri üstündeki katılımcıları üzerinde daha güçlü kontrol sağlayan içiçe olmayan bir başka genellemeyi de ele alıyoruz.

Anahtar Kelimeler: Sır Paylaşım Şeması, Çokpartili Erişim Yapıları, İçiçe Çokpartili Sır Paylaşımı

To my parents..

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my thesis advisor Ferruh Özbudak for encouragement on the topic that I desire to study, to Ali Aydın Selçuk for useful discussions and helpful conversations, to Ali Doğanaksoy for making me eager to study cryptography, thereby initiating me on the area and for further support, to Atılım University for their understanding and tolerance for the durations that I needed to concentrate on my work, to all my instructors that I have benefited so much during the past years in cryptography, mathematics and computer science, again to all the aforementioned names for not only depicting a good model as a scientist but also for being a good model as a person, to C. Padró and T. Tassa for generously helping about some specific e-questions on their seminal studies, and finally to all my friends and colleagues for helping me getting positively motivated by creating a pleasant study environment.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Secret sharing and its numerous variations form an important primitive in cryptography. The essential idea is that, the secret can be recovered only if a possibly large and responsible authorized group of participants, acting together, perform some predefined steps so that a high degree of security is attained. In information based systems, operations are carried on commonly by requiring certain access rights, which are gained through a key, password or some biometric specialty. The initial motivation for proposing first secret sharing schemes [1,2] was sharing a sensitive cryptographic key among a set of participants. However, secret sharing turned out to be useful in many scenarios and the interconnections or theoretical relations with other disciplines aroused since its proposal. One may encounter a shared security system in communication networks, information systems, military substructures and financial institutions. A classical example for the use of secret sharing is the activation of a nuclear weapon. For such an action, it is usually not desirable to put the responsibility and authorization onto a single person. Several high-level officers must join together before the necessary password can be reconstructed. Secret sharing has been studied from the point of view of a vast number of distinct mathematical structures. Among them, there are well-known geometric, algebraic, combinatoric, cryptographic or coding theoretic approaches interconnected with secret sharing.

A *secret sharing scheme* is basically composed of two phases. In the first phase, a *dealer* determines and privately distributes shares to participants via a share distribution algorithm. In the second phase, an authorized subset of participants join their shares together and reconstruct the secret via some combiner, defined by some secret reconstruction algorithm. The set of all authorized subsets of participants is called the *access structure* of a secret sharing

scheme. The main focus of attention of the early secret sharing schemes studied in [1,2] was the access structure formed by any t out of n participants, denoted (t, n). However, in most real-life applications, the corresponding access structure may not be that simple and more sophisticated access structures together with corresponding secret sharing schemes turn out to be useful in distinct scenarios. In this respect, *multipartite access structures* took special attention mainly because they model very natural and well-motivated situations in practice. Besides, theoretically, they form a generalization of conventional (t, n) access structures, that is, every (t, n) access structure can be seen as a multipartite access structure. In this work, we study some generalized multipartite access structures and linear secret sharing schemes for their realization.

Brickell [7] and Simmons [3] were the first to study multipartite access structures. Given a multipartite access structure with m compartments (or levels) and m conditions, Simmons' definition of a hierarchical access structure identifies a subset of participants as authorized, if any 1 out of m conditions by the subset is satisfied. On the other hand, Tassa's version as well as the well-known compartmented access structure of Brickell can be considered as requiring all the m conditions.

• In chapter 2, we give some preliminary definitions that are used throughout this work. We then briefly cover some interrelations of secret sharing with other disciplines, its applications and distinct approaches on the field.

• In chapter 3, we examine the natural case concerning that any c out of m of the conditions on compartments (or levels) suffice, yielding to generalizations for both the compartmented and hierarchical cases. These are realized essentially by employing a series of Lagrange interpolations and a simple frequently-used connective tool called *access structure product*, as well as some known constructions for existing ideal schemes. Due to the building blocks used, the schemes are perfect with probability 1. The information rates of the schemes we consider range from $\frac{1}{2}$ to $\frac{1}{m}$, except a naive ideal case, what we call the (c, m) compartmented access structure. This chapter is mainly in line with our studies [17,18].

• In chapter 4, we consider some generalizations that we identify as *nested multipartite access structures*, where we let a compartment to be defined within another, so that the access structure is composed of some multipartite substructures, yielding to many combinations when formed by different types of such substructures. This time, we give an ideal realization as

long as ideal schemes for the substructures exist. We extend formerly employed bivariate interpolation techniques to multivariate interpolation in order to realize such sophisticated access structures. In other words, the key design technique of the generic scheme we propose is the distribution of the nonzero entries in the reconstruction matrix, for which we extend the linear algebraic techniques employed in some former realizations of multipartite access structures. The scheme we consider is perfect with probability $1 - O(q^{-1})$ on a finite field $\mathbb{F}_q$. In particular, we propose a non-nested generalization for the conventional compartmented access structures, which depicts a stronger way of controlling the additional $t - (t_1 + \ldots + t_m)$ participants.

• In chapter 5, we conclude with a summary of our contribution and some remarks.

We would like to cite the following from [19], a study on hierarchical multipartite access structures, as it essentially describes the purpose of this study.

"Every access structure admits a secret sharing scheme [33,10], but in general the shares must be larger than the secret [34,36]. Very little is known about the optimal complexity of secret sharing schemes for general access structures, and there is a wide gap between the best known general lower and upper bounds. Because of that, the construction of ideal secret sharing schemes for particular families of access structures that may have interesting applications is worth considering."

General access structures has been first being considered in [10], proving that any monotone access structure can be realized by a perfect scheme, and a better solution to for such a realization has been given in [10]. Since then, a wide range of studies has been conducted on general access structures from different aspects such as graph theory [35] and there are some Chinese Remainder Theorem (CRT) based studies such as [37,38,39]. However, the common unfortunate aspect of the studies mentioned is that their information rate is exponentially small on the number of participants involved in the access structure. Indeed, this is not surprising when we take into account the fact that the results of the aforementioned works are so general and do not benefit from the specific feature or description of an access structure. This describes our goal, which is to build a brick onto the study of best possible realizations of some specific access structures that may have some real-world applications. Hence we not only search for the ideal solutions (as in chp. 4), being mentioned as a best goal in the above citation of [19], we also study some specific non-ideal cases (chp. 3), solutions of which are still far better

than the exponential realizations obtained when the corresponding access structures are taken as general.

To mention something about the theories involved in the thesis, chapter 2 overwhelmingly enfolds some nontechnical information while presenting preliminaries and a small literature survey. Chapter 3 is also soft in the sense of amount of mathematical structures involved as the results are expressed rather more verbal, exploiting some well-known mathematical schemes on the field. The study presented in Chapter 4, on the other hand, involves some linear algebra and a little bit of complexity theory.

CHAPTER 2

PRELIMINARIES

2.1 Some Essentials

2.1.1 Definitions

A *secret sharing scheme* (SSS) is a method to share a secret s among a set $\mathcal{U}$ of participants. As mentioned in the introduction chapter, the basic model for a SSS is composed of two protocols:
(i) a distribution protocol in which the secret is distributed by a dealer among the participants.
(ii) a reconstruction protocol in which the secret is recovered by pooling the shares of a qualified subset of the participants.

The *access structure* Γ over a set of participants $\mathcal{U}$, denoted $\Gamma \subset 2^{\mathcal{U}}$, of a SSS is the set of all qualified subsets of participants such that each subset is allowed to access the secret. Furthermore, the subsets of participants contained in the access structure are the only ones that are expected to do so. It is reasonable to assume that an access structure Γ defined over the set of participants $\mathcal{U}$ to be *monotone*, that is, if $A \in \Gamma$ and $A \subset B \subseteq \mathcal{U}$ then $B \in \Gamma$. A SSS is called *perfect* if participants of any qualified subset of $\mathcal{U}$, pooling together their private information (*shares*), can always reconstruct s, whereas a non-qualified subset of $\mathcal{U}$ obtains information about it. In other words, a perfect scheme guarantees the protection against unauthorized subsets by unconditional information-theoretic means. More formally, a perfect SSS taking as input a secret s chosen from some finite set S, and outputting n shares $s_1, \ldots, s_n$ on an access structure Γ must satisfy the following conditions:

Privacy: Take any subset $I \notin \Gamma$ and run the scheme for some input $s \in S$. Then the probability

distribution of $\{s_i | i \in I\}$ is independent of s.

Correctness: Take any subset $J \in \Gamma$ and run the scheme on some input $s \in S$. Then there is an efficient algorithm such that s is uniquely determined by $\{s_i | i \in J\}$.

It is well-known that in all perfect schemes, shares must be at least at the size of the secret. On the other side, if sizes of the shares becomes greater, it results in lower information rates and the scheme is regarded as being less efficient. Consequently, ideal perfect schemes were naturally defined as those optimal cases when the shares and the secret are of equal size.

Threshold access structures are among the first studied ones. Letting $\mathcal{U}$ denote the set of participants where $|\mathcal{U}| = n$, a (t, n) threshold access structure consists of all subsets of participants from $\mathcal{U}$ with at least t the participants in the subset. That is, $\Gamma = \{A | A \in \mathcal{U}, |A| = t\}$. In contrast to perfect schemes, *ramp schemes* were introduced and first considered in [66]. In a ramp scheme of a threshold access structure, sets of at least t participants can reconstruct s as in the case of perfect schemes. Less than c participants obtain no information about s, whereas sets of participants with greater than c and less than t members might have "some" information on s. Ramp schemes are also point of attraction as they might provide some better capabilities such as a higher information rate when compared to perfect ones. Unfortunately, the security provided by these schemes is questionable in many applications.

Most SSS's in the literature are linear. That is, the shares are obtained by basically applying a linear mapping to the secret. In other words, in a linear scheme, the dealer independently and uniformly chooses some field elements, forming a vector of unknowns, that an authorized set of participants solve via a linear system of equations. The secret is a linear combination of the field elements in the unknown vector and can be represented as the dot product of the unknown vector and the so-called *target vector*.

A well known measure of efficiency for SSS's is the notion of information rate which is concerned with the ratio of the size of the secret and the size of the private share that a participant must keep. More formally, let $\mathcal{F}$ be a set of distribution rules for a secret sharing scheme that is defined on a set of w participants. Define $s_i = \{f(P_i) | f \in \mathcal{F}\}$, $1 \leq i \leq w$, so that s_i represents the set of all possible shares that participant P_i can receive. Letting $\mathcal{S}$ denote the set of all possible keys, the information rate for P_i is the ratio

$$\rho_i(\mathcal{F}) = \frac{\log_2 |\mathcal{S}|}{\log_2 |s_i|}$$

The *information rate* of the scheme is defined as $\rho(\mathcal{F}) = min\{\rho_i(\mathcal{F})|1 \leq i \leq w\}$. The *average information rate* is the harmonic mean of $\rho_i(\mathcal{F})'s$ defined by

$$\tilde{\rho}(\mathcal{F}) = \frac{w \log_2 |S|}{\sum_{i=1}^{w} \log_2 |s_i|}$$

A secret sharing scheme is called *ideal* if the domain of shares of each user equals to the domain of secrets, in which case, $\rho = \tilde{\rho} = 1$, yielding to an optimal situation.

2.1.2 Threshold and Multipartite Access Structures

The first SSS's were introduced by Blakley[2] and Shamir[1]. In those schemes, the corresponding so-called threshold access structure was any t out of n participants, denoted by (t,n). The schemes were correspondingly called threshold secret sharing schemes.

Succeeding threshold access structures, Brickell [7] and Simmons [3], later on, studied multipartite access structures, wherein participants are divided into several subsets, named *compartments*. Participants in the same compartment are not distinguished and are assumed to be of equal trust. However, members of different compartments may not be equally trusted. If these compartments are hierarchically ordered, they are usually identified as *levels* and the access structure is said to be hierarchical or multilevel, otherwise, they are said to form a compartmented access structure. Essentially, an authorized set of a compartmented access structure must involve at least t_i participants from each compartment C_i as well as a minimum of t participants in total.

The three main types of "hierarchy-involved" access structures are as follows: Shamir's weighted threshold access structures [1], Simmons' hierarchical access structures [3] and Tassa's hierarchical threshold access structures [4]. In his influential work [4], Tassa considered conjunctive hierarchical access structures, for which a perfect and ideal scheme employing Birkhoff interpolation, making use of the derivative values of a univariate polynomial, is also provided. This approach gained attention and found place in distinct areas, such as the ad hoc network applications [14,15]. A former work on this area is due to Simmons [3], where he proposed disjunctive hierarchical access structures, though his solution was not efficient. Later on, with the help of Tassa's conjunctive hierarchical threshold access structures [4] as a building block, an ideal and perfect scheme for realizing the disjunctive case is proposed

in [4] as well, via an approach of taking the dual access structure. Hierarchical access structures that admit an ideal secret sharing scheme are characterized within a unified framework in [19].

As mentioned in chapter 1, it is known, due to [10], that every monotone access structure admits a secret sharing scheme, but it is often the case that the shares must be larger than the secret.

2.1.3 Shamir's Scheme

The basic scheme proposed by Shamir[1] uses standard Lagrange's polynomial interpolation. The scheme works as follows: Let q be a large prime and $s \in \mathbb{Z}_q$ be the secret to be shared. The dealer chooses a random univariate polynomial

$$f(x) = s + \sum_{i=1}^{t-1} a_i x^i \in \mathbb{Z}_q[x]$$

of degree $t-1$ where the constant term is the secret. In order to distribute S among n participants, just fix n distinct real numbers $\{x_1, \ldots, x_n\}$ and assign to the j-th participant the share $y_j = f(x_j) = s + \sum_{i=1}^{t-1} a_i {x_j}^i$.

While the reconstruction of the secret can be described by a formula resulting from Lagrange's polynomial interpolation, a linear algebra point of view heads us towards the following linear system that the authorized subset of participants $\{x_1, \ldots, x_t\}$ must solve,

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ \vdots & & & \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} f(x_1) \\ \vdots \\ f(x_t) \end{pmatrix}$$

As pointed out by Shamir himself in [1], a hierarchical variant can be introduced by simply assigning a higher number of shares to higher level participants. However such a solution is far away from being ideal. While Shamir's SSS, having a Vandermonde matrix on its basis, enjoys the property of reconstructibility of the secret with probability exactly 1 by an authorized subset, a non-authorized subset that is formed by a missing number of participants learn no information about the secret. Hence the privacy and correctness properties are satisfied, resulting in a perfect scheme. A more formal treatment is as follows.

Theorem 2.1.1 *For any field* $\mathbb{F}$ *and any set of pairs* $(x_1, y_1), \ldots, (x_t, y_t) \in \mathbb{F} \times \mathbb{F}$ *where the* x_i*'s are distinct, there exists exactly one polynomial f(x) over* $\mathbb{F}$ *of degree at most* $t - 1$*, with* $f(x_i) = y_i, i = 1, \ldots, t$ *such that all coefficients of the polynomial* $f(x)$ *can be efficiently computed from* $(x_1, y_1), \ldots, (x_t, y_t)$*.*

Proof. Define polynomials

$$f_i(x) = \prod_{\substack{\{j=1,\ldots,t\} \\ j \neq i}} \frac{x_j - x}{x_j - x_i}$$

satisfying $f_i(x_i) = 1 \; \forall i$, $f_i(x_j) = 0$ for $i \neq j$, where each $f_i(x)$ has degree at most $t - 1$. It follows that $f(x) = \sum_{i=1}^{t} y_i f_i(x)$ and in particular the secret $f(0) = \sum_{i=1}^{t} y_i f_i(0)$ can be feasibly computed and $f(x)$ is unique since if two different polynomials $f(x)$, $f'(x)$ were both solutions, then $f(x) - f'(x)$ would be a nonzero polynomial of degree at most $t - 1$ with t roots, which is impossible. ■

2.2 Approaches to Secret Sharing

Many of the manuscripts and surveys on secret sharing consider a certain and only one aspect. The purpose of this section is to give some flavor of distinct approaches to secret sharing, its applications, and some alternative underlying mathematical structures, pointing some significant connections to other disciplines. Our aim is neither to give a complete treatment about the aforementioned topics, nor to provide an extensive list of references. Though many of the introduced concepts herein are not directly connected with the work on the succeeding chapters, this section hopefully constitutes some motivation to study secret sharing and is substantially oriented for a non-expert reader.

2.2.1 Secure Multi-Party Protocols and Verifiable Secret Sharing

The mathematical schemes consider the case that a non-authorized set of participants should not be able to learn any information about the secret, which means we assume dishonest third parties, but honest participants, both of whom are rather called *players* in terms of multi-party protocols. However, the assumptions on the honesty of the participants and even on the trustfulness of the dealer may be too strong for some scenarios.

A first problem that arises is that there may be no dealer. In this case, each of the players may have a secret $s_1, \ldots, s_n$, and the common purpose might be the computation of a function $f(s_1, \ldots, s_n)$ without revealing any information about their secrets. This problem first aroused with a more specific case named Yao's millionaires' problem [22], which is indeed a secure multi-party communication problem being introduced by Andrew Yao. The problem discusses two millionaires, Alice and Bob, who are interested in knowing who is richer without revealing their actual wealth. Though Yao's own solution is exponential in time and space, many other solutions are proposed and play a centralized role in e-commerce and data mining. The reason is that, commercial applications sometimes need to compare between numbers which are confidential.

Another case is that, some of the players may be malicious and give fake or incorrect shares to the other participants. For the detection of players who are dishonest, the concept of information checking was introduced in [23], which extends the secret sharing protocol so that, when more than half of the players are honest and communications are not corrupted, any multi-party protocol is successfully accomplished. An early study considering protection against cheaters is [71]. A recent extension of Shamir's scheme for detection and identification of cheaters in a threshold secret sharing setting is considered in [83].

Another problem shows up in the case of a dishonest dealer. That is, the dealer may be distributing shares to the players so that when players $p_1, \ldots, p_k$ put their shares together, they get the secret s, but when players $p_1', \ldots, p_k'$ put their shares together, they get another secret $s' \neq s$. In this respect, a dealer is assumed to be honest if and only if the secret reconstructed by any combination of an authorized set of players is the same. To address this problem, the concept of *verifiable secret sharing* is introduced in [24].

In a verifiable secret sharing scheme, the dealer usually gives some additional public information, revealing as little information as possible about the shares, so that player can verify that their shares are consistent. Studies concentrate on giving the players the ability of not only detecting a dishonest dealer, but also detecting dishonest players, up to a certain number, which is a fraction of the total threshold of players, with a reasonable probability of error. Informally, such schemes are constructed in a manner that the players collectively add and multiply numbers without any individual knowing what exactly is being added and multiplied. Usually, an adaptive attacker, whose strategy may change according to the current state

of his information and who has the control on the corrupted players is assumed. In [56], a publicly verifiable SSS construction running in linear time on the number of participants and an election scheme based on the given SSS is considered. A general secure multiparty computation from any linear SSS is proposed in [13]. For more information about (publicly) verifiable secret sharing, related concepts in secure multi-player protocols and applications to e-voting, we refer the reader to [21].

One related concept is *threshold cryptography*, which deals with sharing of the private key among a set of receivers, without revealing it, so that only authorized sets of users can decrypt messages. The sub-protocols of such a system may involve a key generation protocol, where the key is generated jointly by all participants and a decryption protocol, where an authorized set can decrypt a ciphertext without explicitly reconstructing the private key. Such a procedure is sometimes referred to as *function sharing*.

The concept of threshold cryptography was first formally stated by Desmedt in [58]. Since then, various studies conducted on the topic, such as [59,60]. Threshold versions of encryption schemes are built for many public encryption schemes and via different secret sharing schemes. The prescribed goal of such schemes is to be as secure as the original scheme. Such threshold versions have been defined for RSA, Pallier cryptosystem and El-Gamal cryptosystem. However, most of the early solutions were depending on El-Gamal cryptosystem, as the discrete logarithm based threshold systems were easier to design. The reason is that, the decryption works in a group whose order is publicly known, which is not the case for RSA, as $\phi(N)$ is hidden except the party who is performing encryption. However, later on, studies overcoming this problem raised, such as the complete solution in [57]. An alternative, exploiting Blakley's scheme for performing RSA threshold cryptosystem is studied in [62]. A more comprehensive study for RSA threshold cryptography can be found in [77]. In general, a similar threshold approach might be applied to signature schemes, resulting in threshold signatures, an example of which is considered in [61].

2.2.2 Proactive Secret Sharing

Secret sharing protect secrecy and integrity of some private information by distributing shadows of information over different locations. It may be possible for an attacker to capture multiple locations in order to learn the information. For a (t,n) threshold scheme, in par-

ticular, the adversary needs to compromise t locations to acquire the secret, or alternatively, corrupt at least $n - t + 1$ shares to destroy the secret information. In this case, the life-time of the secret becomes an important concern as it determines the period of vulnerability to an attack. Hence, the protection provided by traditional and naive secret sharing may be insufficient. In case that the attacker steal shares of some players, it might not be practical to change the secret, it might be more convenient to replace the uncompromised shares by new ones. So the essential idea of proactive secret sharing is to *periodically renew the shares without changing the secret*, in such a way that the information gained by the adversary by stealing the legal shares becomes useless after the shares are renewed. This is accomplished via a periodical *update protocol*, to perform which, a participant communicates with the dealer. Now, to be able to learn the secret, the adversary needs to compromise t locations in a single period, instead of the entire life-time of the secret.

For Shamir's scheme, renewing of the shares can be achieved by the dealer generating a new random polynomial with constant term zero and calculating for each remaining player a new ordered pair (x, y), where the x-coordinates of the old and new pairs are the same. To obtain the new y-coordinate, or share, of the secret, each player adds the old and new y-coordinates to each other. It is also possible for the dealer to change the threshold number while distributing updates, via the techniques employed in proactive secret sharing. Proactive security is a term introduced in [25], first applied to secret sharing in [26], a recent study [27] considers some attacks related to a mobile adversary, and some alternative approaches for proactivity.

2.2.3 Two extremes: Short and Long shares

Conventional secret sharing deals with the ideal case, that is shares are the same length with the secret. If the secret is short, sizes of the shares is not a problem. If the secret is something long (a textbook,etc.), one approach might be encrypting the share via a symmetric cryptosystem, and sharing the key among participants. Another direct approach is to use shares shorter than the secret. This case is usually referred to as *computational secret sharing* (CSS), as this time the essential requirement of secret sharing: "an authorized set of players will reconstruct the secret, yet an unauthorized set of players learns nothing about the secret", becomes more relaxed as this time the guarantee is computational, rather than being information theoretic. Size of shares being shorter than the secret is impossible in information theoretical

means. For CSS, the term adversary thereby becomes more important when compared to the information theoretical secret sharing. If we add term *robustness* (recoverability despite some wrong shares), we obtain the generalization robust CSS (RCSS), having more capability. Krawczyk is first to study CSS [28], even though no proofs or formal definitions are given therein. Later on, he added the capability of robustness via some hash function in [29]. Many studies thereafter such as [30,31] concentrate on more general access structures. A rather more recent paper applying the techniques of provable security to analyze some main protocols of RCSS is [32]. A *robust secret sharing scheme* ensures that no unqualified subset of players can modify their shares and in case of such an attempt, the reconstruction yields some value other then the original secret s. Efficient conversion of any linear secret sharing scheme into a robust secret sharing scheme is considered in [73].

Well long shares result in obviously small information rates, and hence schemes involving long shares become inefficient. Then why do we need them? The answer is, we are able to realize more sophisticated access structures. To put it on the other way, not all access structures are realizable via ideal schemes. This fact is indeed proven by Benaloh and Leichter [33], thereby, in some cases the shares must be much larger than the secret. There are studies such as [65] which employs ramp schemes for general access structures, for the sake of better information rates. Obtaining the best possible rates for distinct access structures is an open problem, indeed an extensive one.

2.2.4 Image Sharing

Another recent field of study in the context of secret sharing is image sharing, helping protection of digital images. Naor and Shamir [42] first introduced the secret image sharing problem, and proposed a scheme for sharing a binary black and white secret image. This method has been extended to share a gray-level image [43], and then to color images [44]. Thien and Lin presented consequent works [45,46], where in the former, a mapping key permuting the secret image is employed, followed by Shamir's scheme. This way, the size of each shared image is smaller than the secret image, resulting in some benefit when processing the shared images, such as storage and transmission. In the latter of their works, they propose a method with fault tolerance property. Fang [47] recently presented a progressive method with applications to binary images supporting fast decoding, distinguish the group to which

the share belongs through friendly meaningful shares, and which is lossless.

Chen and Chien [48] proposed a method to share many secret images such that each participant is given only one shared image. In [49] a method is presented reducing the shared image size and hiding the shared images into any given natural images to reduce the possibility that an attacker may notice them. There are also other studies depending on Blakley's sharing scheme [50] and recently, Chinese Remainder Theorem [51].

Shyu et al. [52] applied Mignotte's secret sharing scheme [54] to image sharing involving a random number generator (RNG). To eliminate the necessity of the knowledge of the RNG, in [53], another method is proposed employing Asmuth-Bloom's secret sharing scheme [55].

2.2.5 Multi-Secret Sharing

Using the naive version of Shamir's scheme, one can share multiple secrets only via a re-employment of the scheme. This needs redistribution of renewed shares of participants. However, this reissuing process can be turned out to be less less time and resource consuming when the first shares of the participants are somehow involved in the process to obtain new ones, as described by He and Dawson in [89], where a multistage secret sharing scheme based on the one-way function is proposed. Such an approach is sometimes referred to as dynamic secret sharing. Recently, another multi-secret sharing scheme with so-called multi-policy is proposed in [90] and further improved in [91] in terms of computational complexity.

2.3 Mathematical Connections

In this section, we briefly mention about some essential secret sharing schemes other than Shamir's and depending on some distinct aspects of mathematics. We also investigate some essential interrelations of secret sharing with other mathematical disciplines.

Even though Shamir's scheme [1] turned out to be more popular being employed in a higher number of applications, Blakley's scheme [2] was more general indeed involving Shamir's scheme as a subcase. Another important alternative to Shamir's Lagrange interpolation based scheme is the employment of Chinese Remainder Theorem (CRT). First such scheme is considered by Mignotte [54], which is followed by Asmuth and Bloom [55], providing better

security. Although CRT seems suitable to handle secret sharing problem, the handicap of both the schemes is that they are not perfect as a set of less than necessary number of participants obtains some information about the secret, though providing adequate security for many applications. Later on, some essential multipartite access structures were realized by Iftene [67,68]. In particular, realizing more general access structures via CRT is considered in [69]. A recent study [70] of the same author, considers a solution for compartmented threshold decryption or compartmented threshold digital signature generation for RSA.

Among numerous known connections with known mathematical structures, some recent advances [63,64] in secret sharing involves algebraic geometry, employing high degree rational points on algebraic curves, introducing and improving algebraic geometric ramp schemes for the sake of better information rates. The latter of these works, allows the secret to be chosen in an extension field, whereas the shares lie in a base field.

There is a one-to-one connection between linear secret sharing schemes and linear codes. So, one approach to the construction of secret sharing schemes is based on coding theory. In principle, every linear code can be used to construct secret sharing schemes. Both reconstructing the secret of a linear SSS and decoding of a linear code corresponds in essence to solving a system of linear equations thereby interpolating some unknown polynomial. Since early 80's [72], this topic has been extensively studied.

Many combinatorial structures are closely related with secret sharing. As an example, *matroids* play an important role in establishing a classification for hierarchical access structures as in [19]. In [76] a SSS for the graph coloring is purposed and is applied to the public-key cryptosystem "Polly Cracker". Ideal schemes for connected graphs were characterized by Brickell and Davenport [87]. A recursive construction depending on graph decompositions are studied in [12,35] and [78-82]. Also there are several connections such as construction of secret sharing via latin squares [74]. A specific family of combinatorial designs and their applications to secret sharing schemes are considered in [84]. An interesting application [85] dealing with construction of *anonymous secret sharing schemes*, in which the secret is supposed to be constructed without knowledge of which participants hold which shares, depends again on combinatorial designs known as Steiner systems. A nice study investigating connections between combinatorial structures, codes and secret sharing is [88].

Though researchers usually deal with linear secret sharing schemes, there is an ongoing re-

search in nonlinear counterpart, as described in [86].

Perhaps contributing to explicitness of direct applicability of secret sharing, a computer science engagement via databases is as follows: A secret sharing scheme to realize access structures of *quorum systems* in the context of access control is studied in [41]. A quorum system essentially employs a collection of sets (quorums) every two of which have a nonempty intersection. Another interesting application is the employment of secret sharing with the purpose of performing data mining without violating privacy [75].

CHAPTER 3

SOME GENERALIZED COMPARTMENTED AND HIERARCHICAL ACCESS STRUCTURES

Non-ideal secret sharing schemes are usually underrated and regarded as inefficient. However, one might still be in the need of employing such a scheme, especially when there is no known ideal scheme that applies to a certain access structure. Indeed, there are many examples emerging in real life that gives rise to such cases. In this chapter, we consider a family of access structures motivated by the following. Tassa's definition of hierarchical threshold access structures as well as the compartmented access structures of Brickell can be considered as requiring m conditions on m compartments. We examine the natural case concerning that any c out of m of these conditions suffice, yielding to generalizations for both the compartmented and hierarchical cases. We consider a rich variety of access structures obtained via this spirit, realized essentially by employing a series of Lagrange interpolations and a simple frequently-used connective tool called access structure product, as well as some known constructions for existing ideal schemes. The information rates of the schemes we consider range from $\frac{1}{2}$ to $\frac{1}{m}$, except a naive ideal case, what we call the (c, m) compartmented access structure.

Related work. Unlike the compartmented access structures [7], a recent proposal of an interesting multipartite access structure by Herranz and Sáez [6] considers a case such that besides having a total of at least t participants, each authorized subset must involve representatives from at least ℓ distinct compartments instead of satisfying a separate threshold condition on the number of participants from each compartment.

Organization of the chp. After giving some preliminaries in section 3.1, we consider (c, m) compartmented access structures as well as some alternative definitions and realizations in

section 3.2. With a similar approach, we consider (c, m) hierarchical access structures in section 3.3, where we also concern again with some particular cases.

3.1 Preliminaries

Linear SSS's (LSSS) are widely studied under the notion of monotone span programs (MSP). Formally, a MSP is a 5-tuple $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{t})$, where $\mathbb{F}$ is a field, M is a matrix of dimensions d x e over $\mathbb{F}$, $\mathcal{U} = \{u_1, \ldots, u_n\}$ is a finite set, ϕ: $\{1, \ldots, d\} \to \mathcal{U}$ is a surjective function assigning each row to a participant in $\mathcal{U}$, and $\mathbf{t} \in \mathbb{F}^{\mathbf{e}}$ is the so-called target vector. Participants are said to own or privately hold one or more certain row(s) of M. The MSP $\mathcal{M}$ is said to realize (compute) the monotone access structure Γ in case that $\mathbf{t}$ is spanned by the rows of the matrix $M_{\mathcal{V}}$ if and only if $\mathcal{V} \in \Gamma$, where $M_{\mathcal{V}}$ is the matrix whose rows are formed by participants of the set $\mathcal{V} \in \mathcal{U}$. The *size* of $\mathcal{M}$ is d, the number of rows of M. Now giving share s_i to participant $\phi(i)$, we can identify an LSSS with its underlying MSP. We refer the reader to [33] for a detailed discussion on MSPs.

If Γ is a monotone access structure realizing $\mathcal{U}$, its *dual* $\Gamma^* = \{\mathcal{V} : \mathcal{V}^c \notin \Gamma\}$ is also monotone and if $\mathcal{M} = (\mathbb{F}, M, \mathcal{U}, \phi, \mathbf{t})$ is a MSP that realizes Γ, then there exists an $\mathcal{M}^* = (\mathbb{F}, M^*, \mathcal{U}, \phi, \mathbf{t}^*)$ of the same size as $\mathcal{M}$ that realizes the dual access structure Γ^* and $\mathcal{M}^*$ can be efficiently constructed as described in [20]. An access structure is ideal if and only if its dual is.

Given two monotone access structures Γ_1 and Γ_2 defined on sets of participants $\mathcal{U}_1$ and $\mathcal{U}_2$ respectively, define ([12]) the product $\Gamma_1 \times \Gamma_2$, as the monotone access structure defined on $\mathcal{U}_1 \cup \mathcal{U}_2$ such that for any $\mathcal{V} \subseteq \mathcal{U}_1 \cup \mathcal{U}_2$ it holds that

$$\mathcal{V} \in \Gamma_1 \times \Gamma_2 \iff (\mathcal{V} \cap \mathcal{U}_1 \in \Gamma_1 \text{ and } \mathcal{V} \cap \mathcal{U}_2 \in \Gamma_2)$$

The following is a well-known realization of the product $\Gamma_1 \times \Gamma_2$.

Lemma 3.1.1 *If MSPs $\mathcal{M}_1$ and $\mathcal{M}_2$ with matrices $M_1 = (c_1 M_1')$ and $M_2 = (c_2 M_2')$ (where c_1 and c_2 are the first columns of the matrices) and target vectors $\mathbf{1} = (1, 0, \ldots, 0)$ realize the access structures Γ_1 and Γ_2 respectively, then the MSP $\mathcal{M}_1 \times \mathcal{M}_2$ with the matrix*

$$\begin{pmatrix} c_1 & \mathbf{0} & M_1' & \mathbf{0} \\ \mathbf{0} & c_2 & \mathbf{0} & M_2' \end{pmatrix}$$

realizes $\Gamma_1 \times \Gamma_2$ *with the target vector* $(1, 1, 0, \ldots, 0)$.

The reason that the first columns of the matrices M_1 and M_2 has been taken out is to simply be able to use the target vector $(1, 1, 0, \ldots, 0)$. One can directly employ matrices M_1 and M_2 without separating their first columns c_1 and c_2 as long as a target vector such as $(1, 0, \ldots, 0, 1, 0, \ldots, 0)$ is used. Note that the definition of product of two access structures, $\Gamma_1 \times \Gamma_2$, and lemma 3.1.1 can naturally be extended to $\Gamma_1 \times \Gamma_2 \times \ldots \times \Gamma_k$ in a straightforward manner.

Lemma 3.1.2 *Given MSPs* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *realizing access structures* Γ_1 *and* Γ_2 *defined on sets* U_1 *and* U_2*, respectively,*
i) if $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *are ideal and* $U_1 \cap U_2 = \emptyset$*, then* $\mathcal{M}_1 \times \mathcal{M}_2$ *is also ideal.*
ii) if $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *are perfect, so is* $\mathcal{M}_1 \times \mathcal{M}_2$.

Proof. If $\mathcal{M}_1$ and $\mathcal{M}_2$ are ideal, participants from Γ_1 and Γ_2 own one and only one row apiece in the corresponding matrices M_1 and M_2, respectively. Let the reconstruction matrix of $\Gamma_1 \times \Gamma_2$ be $M_{1\times2}$. Then participants of $\Gamma_1 \times \Gamma_2$ will obviously own one row in $M_{1\times2}$ as well, since no participant who is both in U_1 and U_2 exists. Similarly if $\mathcal{M}_1$ and $\mathcal{M}_2$ are perfect, determinants $|M_1|$ and $|M_2|$ will be nonzero for every possible sets of authorized participants in Γ_1 and Γ_2 respectively, yielding to a nonzero determinant $|M_{1\times2}| = |M_1||M_2|$. □

3.2 (c, m) Compartmented Access Structures

The compartmented access structure that was presented in [7] is as follows. Let $\mathcal{U} = \bigcup_{i=1}^{m} C_i$ be the set of participants with m disjoint compartments, that is, $C_i \cap C_j = \emptyset$, $1 \leq i < j \leq m$. Let $t_i \in \mathbb{N}$ be threshold values for compartments C_i, $1 \leq i \leq m$, respectively and let $t \in \mathbb{N}$ be the threshold such that $t \geq \sum_{i=1}^{m} t_i$. Then $\Gamma_0 = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V}$ such that $|\mathcal{W} \cap C_i| \geq t_i \ \ \forall i \in \{1, \ldots, m\}$ and $|\mathcal{W}| = t\}$. In this definition, if we identify the requirement that at least t_i participants from compartment C_i will be present as a condition on C_i, one can say that the definition imposes m conditions on m compartments. However, it might be the case that one may be satisfied with any c (out of m) of these threshold conditions. In such an a setting, the dealer does not know (or care) which compartments will form a coalition while setting up the scheme. This leads us to the following definition.

Definition 3.2.1 *Let $\mathcal{U} = \bigcup_{i=1}^{m} C_i$ be the set of participants with $C_i \cap C_j = \emptyset$, $1 \leq i < j \leq m$, let $t_i \in \mathbb{N}$ and $t \in \mathbb{N}$ with $t \geq \sum_{i=1}^{m} t_i$. Then the corresponding (c, m) compartmented access structure* [1] *is*

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V} \text{ such that } |\mathcal{W} \cap C_i| \geq t_i \text{ for } c \text{ indices } i \in \{1, \ldots, m\}\}$$

Theorem 3.2.2 (c, m) *compartmented access structures are ideal and perfect.*

Proof. To obtain the result in a constructive fashion, we need to show that the access structure Γ of definition 3.2.1 admits an ideal and perfect scheme. Indeed, such an access structure can be realized in a straightforward manner, which is as follows. The dealer first applies a (c, m) Shamir's scheme on the secret to obtain private values $s_1, \ldots, s_m$ so that any c of them are sufficient to find the secret. Then, the dealer applies m separate schemes of Shamir, distributing shares for each partial secret s_i to members of each compartment C_i, to assure that there are at least t_i participants from compartment C_i, $1 \leq i \leq m$. Observe that, such a scheme involves only a series of $(m + 1)$ Lagrange interpolations combined with the access structure product operator and, by lemma 3.1.2, is ideal and perfect as the scheme of Shamir's. □

Consider again definition 3.2.1. One may wish to fix some compartments, say $C_1, \ldots, C_k$, by requiring $|\mathcal{W} \cap C_i| \geq t_i \ \forall i, 1 \leq i \leq k$, but may still be pleased with satisfaction of any c conditions on the remaining $m-k$ compartments so that $|\mathcal{W} \cap C_i| \geq t_i$ for c indices $i \in \{k+1, \ldots, m\}$. Calling this generalization Γ', it coincides with Γ of definition 3.2.1 in case of $k = 0$. Since the compartments are assumed to be disjoint and since both the compartmented access structure not requiring a total threshold value t defined on $C_1, \ldots, C_k$ and the (c,m) compartmented access structure defined on $C_{k+1}, \ldots, C_m$ are ideal and perfect, by lemma 3.1.1, Γ' can easily be realized by a product of access structures and combining the corresponding matrices and is again ideal and perfect by lemma 3.1.2. We will refer to this procedure as *fixing* ($k < m$ of the m) compartments. It is of course possible to fix some number of compartments in the following modifications as well.

Before moving further, we would like to remind that our purpose in considering the following variants of definition 3.2.1, in this section, is not to give a complete list of possibly endless

[1] The notion (c, m), *c-out-of-m*, of definition 3.2.1, should not be confused with the standard notation (t, n) as c represents the number of *conditions* to be satisfied (out of m), while t stands for the threshold for total number of participants (out of n).

modifications that can be performed on Γ, but just to draw attention to some potential main applications, obtained via access structure product, that might correspond to cases in real life and be of public interest.

modification 1: One may wish to impose a threshold $t \in \mathbb{N}$ on the total number of participants and therefore obtain an alternative access structure such as $\Gamma_1 = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V}$ such that $|\mathcal{W} \cap C_i| \geq t_i$ for c indices $i \in \{1, \ldots, m\}$ and $|\mathcal{W}| = t\}$ under the setting of definition 3.2.1. Letting $\{t_j\}_{j=1}^{c}$ be a sequence of c distinct threshold values with minimum total sum $t_{min} = min(\sum_{j=1}^{c} t_j | t_j \in \{t_1, \ldots, t_m\})$ one can choose any $t > t_{min}$. It is clear that putting $c = m$ in the definition of Γ_1 makes it fall into the definition of conventional compartmented access structure Γ_0 of Brickell for $t \geq \sum_{i=1}^{m} t_i$. One can realize Γ_1 with two systems of linear equations, one for assuring that there are t_i participants from any c of the C_i compartments $1 \leq i \leq m$ in the same fashion as described before and the other for assuring that there are at least t participants in total. The latter linear system can be handled for example with a naive employment of the scheme of Shamir's. Since both such schemes are perfect, by lemma 3.1.2, the resulting scheme formed by combining these systems via the tool in lemma 3.1.1 is perfect. However, it is inevitable that two shares will be given for each participant, one for each of the aforementioned systems, yielding to an information rate $\frac{1}{2}$. Besides being realized by such a non-ideal scheme, this modification of (c, m) compartmented access structures with additional total threshold condition t may be somehow unfair, which is the main motivation of the subsequent modifications. For now, we only point out that since the dealer does not know which compartments will form a coalition while setting up the scheme, he also does not know how much additional participants to require in advance, which makes the problem of establishing an ideal scheme for the access structure Γ_1 involving the threshold condition t, a hard one.

modification 2. This time, we require the additional condition that there are representatives from at least ℓ distinct compartments, which is helpful in improving the diversity of coalition. Let $\mathcal{U} = \bigcup_{i=1}^{m} C_i$ with $C_i \cap C_j = \emptyset$. Let $t_i \in \mathbb{N}$ be the thresholds for compartments C_i, $1 \leq i \leq m$, respectively and let $c, \ell \in \mathbb{N}$ with $1 \leq c \leq \ell \leq m$. Then the corresponding (c, m) *compartmented ℓ-varying access structure* is;

$$\Gamma_2 = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V} \text{ such that } |\mathcal{W} \cap C_i| \geq t_i \text{ for c indices } i \in \{1, \ldots, m\}$$

$$\text{and } |\mathcal{W} \cap C_j| > 0 \text{ for } \ell \text{ indices } j \in \{1, \ldots, m\} \text{ and } |\mathcal{W}| = t\}$$

Recall that the ideal access structure of Herranz and Sáez [6] require the conditions that each authorized subset must involve representatives from at least ℓ distinct compartments as well as having a total of at least t participants.

Naming the condition $|\mathcal{W} \cap C_j| > 0$ of such an access structure as ℓ-varying, it is shown in [6] that there exists an allocation of identities for which the resulting scheme is perfect. However, in such an access structure, the conditions requiring t_i participants from C_i are missing. These conditions can be imposed by a second linear system, which is as described in the proof of theorem 3.2.2. So to realize Γ_2, one may employ again lemma 3.1.1 to combine two such systems, one for assuring that there are a total of t participants of from ℓ distinct compartments, the other to confirm that $|\mathcal{W} \cap C_i| \geq t_i$ for c indices $i \in \{1, \ldots, m\}$. The information rate of such a scheme is again $\frac{1}{2}$ and we believe that Γ_2 is quite a sophisticated access structure to be realized with such an information rate, regarding that it embodies three distinct types of thresholds in its definition.

Consider again Γ_2. When the variance of the thresholds t_i of the compartments is high, coalitions formed by compartments with greater t_i thresholds obviously reach the total threshold t in an easier way. This unfairness among compartments heads us to a definition obtained by dropping the condition $|\mathcal{W}| = t$ of Γ_2. Such an alternative might be preferred when there are large gaps among the t_i values and can be realized again with an information rate of $\frac{1}{2}$ as follows. Instead of the scheme proposed in [6], as a building block, the dealer may employ a naive (ℓ, m) Shamir's scheme, where all members of a certain compartment are given the same private value, so that participants from at least ℓ distinct compartments can solve the system. In either of the cases, that is, whether we let the total threshold condition t be involved or not, the resulting scheme is perfect by lemma 3.1.2.

modification 3. Requiring any c out of m conditions on compartments may be identified as a loose way of controlling the number of participants coming from each compartment, especially when c is a small number. While the classical compartmented access structure Γ_0 is always there to be chosen, one may alternatively be in the wish of imposing more than one such "loose" ways of controlling the minimum cardinality of representatives of compartments. That is, one can presume, for instance, two distinct conditional threshold values say c_1 and c_2, with $c_2 > c_1$, on compartments C_i, $1 \leq i \leq m$ with two distinct sets of threshold values $\{t_{1i}\}_{i=1}^{m}$ and $\{t_{2i}\}_{i=1}^{m}$ respectively with $t_{1i} \geq t_{2i}$ $\forall\, i \in \{1, \ldots, m\}$. For such a setting, define the

doubly thresholded (c_1, c_2, m) *access structure* as

$$\Gamma_3 = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V} \text{ such that } |\mathcal{W} \cap C_i| \geq t_{1i} \text{ for } c_1 \text{ indices } i \in \{1, \ldots, m\}$$

$$\text{and } |\mathcal{W} \cap C_j| \geq t_{2j} \text{ for } c_2 \text{ indices } j \in \{1, \ldots, m\}\}$$

It is obvious that Γ_3 can be realized with an information rate $\frac{1}{2}$. With a similar reasoning, one may consider r-tuple thresholded $(c_1, \ldots, c_r, m)$ access structures of information rate $\frac{1}{r}$ in general. Again by lemma 3.1.2, the resulting scheme will be perfect no matter how many instances of access structure product are exploited. Alternatively, one may further require an authorized set to be ℓ-varying combined with any number of sets of threshold conditions at the cost of lower information rates.

3.3 (c, m) Hierarchical Access Structures

3.3.1 Motivation

Let us first recall hierarchical threshold access structures introduced in [4]. Let $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$ be the set of participants with m disjoint levels, i.e., $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$, $1 \leq i < j \leq m$ and let $\{k_i\}_{i=1}^{m}$ be a sequence of integers with $0 < k_1 < \ldots < k_m$. Then the corresponding hierarchical threshold access structure is

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \quad \forall i \in \{1, \ldots, m\}\} \quad (1)$$

Under the same assumptions of the above definition, the former hierarchical access structure that is studied by Simmons is as follows.

$$\Gamma = \{\mathcal{V} \subset \mathcal{U}, \exists i \in \{1, \ldots, m\} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i\} \quad (2)$$

Observe that the only difference in (2) is the replacement of the universal quantifier $\forall$ with the existential quantifier $\exists$. If we identify the requirement $|\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i$ as the threshold condition to be satisfied by levels $\mathcal{U}_j$, $j \leq i$, yielding to m conditions, then the distinction among (1) and (2) is that while Simmons' version exploits a disjunction of threshold conditions, Tassa's definition involves a conjunction of such conditions. Letting $c \in \mathbb{N}$ be the threshold number for conditions to be satisfied among m, the definitions above describe access structures that either demand the presence of exactly one of such conditions (c=1) or

all of them simultaneously (c=m). That is, neither of the definitions above has flexibility to contain the intermediary access structures corresponding to values of $1 < c < m$. With this motivation, we consider the following generalization of the access structures (1) and (2).

Definition 3.3.1 *Let $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$ be the set of participants with m disjoint levels, i.e., $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$, $1 \leq i < j \leq m$, let $\{k_i\}_{i=1}^{m}$ be a sequence of integers with $0 < k_1 < \ldots < k_m$. Then the corresponding (c, m) hierarchical access structure is*

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \text{ forat least c indices } i \in \{1, \ldots, m\}\}^2 \quad (3)$$

In Tassa's seminal work [4], the generalization (3) is indeed mentioned and a question asking whether it is an ideal access structure or not, is raised. To the best of our knowledge, no known SSS applies for the case of (c, m) hierarchical access structures for $1 < c < m$. Though we do not solve the open problem stated by Tassa, we nevertheless give a non-ideal scheme realizing (3) herein and discuss the difficulty of establishing an ideal scheme in section 4.2.

It follows from the definition that a (c, m) hierarchical access structure is also a (c', m) hierarchical access structure for $c' < c$. Let us give a toy illustration of (3).

Example 3.3.2 *Consider a scenario where a secret is to be shared among participants from levels $\mathcal{U}_1, \mathcal{U}_2$ and $\mathcal{U}_3$ which are formed by admirals, brigadiers and colonels respectively. Let us represent each participant of a certain level by the initial of the identifier of the level. That is, for instance, the phrase aab stands for a set formed by two admirals and one brigadier. Now $m = 3$ and let $k_1 = 1, k_2 = 2$ and $k_3 = 3$ for the sake of simplicity. The minimal authorized sets in the (c, m) hierarchical access structures for $c = \{1, 2, 3\}$, according to definition 3.3.1 are as follows.*

	minimal authorized sets in (c,3) hierarchical access structure
$c = 1$	$\{a, bb, ccc, bcc\}$
$c = 2$	$\{aa, ab, acc, bbb, bbc\}$
$c = 3$	$\{aaa, aab, abb, abc\}$

Here, the term *minimal authorized set*, sometimes being called *minterm*, refers to a qualified set such that no participant within the set is redundant for the reconstruction of the secret. It is exemplified that all minimal subsets of (1) are of the same size while this is not true for (2)

[2] the access structure Γ, is considered under a slightly different naming in [4].

and (3). The k_i values suggest that basically all the sets 1 admiral, 2 brigadiers and 3 colonels are of equal trust. Regarding involvement of each of the sets a, bb and ccc (while keeping in mind the fact that the lower-leveled participants can be always replaced by upper-leveled ones) as a condition to be imposed on an access structure, it is perfectly natural in real life to require any two of these conditions to be present as well as demanding either one of the conditions or all three of them simultaneously.

One can mimic the realization of the $(2, 3)$ hierarchical access structure of example 3.3.2 with a naive employment of Shamir's weighted threshold secret sharing [1], by say assigning 3 shares to each admiral, 2 shares to each brigadier and 1 share to each colonel and establishing a $(5, n)$ SSS among the n participants via the well-known Lagrange interpolation. In this case, all the required minimal authorized sets $\{aa, ab, acc, bbb, bbc\}$ are eligible to reconstruct the secret. However, the access structure of such a scheme would embody a set of participants such as $ccccc$ which is not the case for (2,3) hierarchical access structure arousing from definition 3.3.1. Nevertheless, we can tailor a scheme for this particular case again via the well-known tools such as Lagrange interpolation and access structure product, but this time with a different distribution of shares, as follows.

scheme 1. To realize (3), assign one secret for each level and apply a scheme of Shamir's in a setting that each participant belonging to that level and the participants in the upper levels are given shares. That is, as in the case of (c, m) compartmented access structures, the dealer first applies a (c, m) Shamir's scheme on the secret to obtain m private partial shares, say $s_1, \ldots, s_m$, so that any c of these values are sufficient to recover the secret. Then he applies a separate Shamir's scheme on each s_i, $1 \leq i \leq m$, so that in each instance of such schemes, the shares are this time distributed not only to the members of the compartment $\mathcal{U}_i$ but also to the members of all compartments $\mathcal{U}_1, \ldots, \mathcal{U}_{i-1}$ accomplishing the desired property that members of the upper level compartments can always replace participants of the lower ones. Here, each Shamir's scheme on the partial secret s_i will be arranged in a setting that s_i can be reconstructed only with the presence of any $k_i - k_{i-1}$ shares (assuming $k_0 = 0$ for s_1). This allows that the partial share s_i can be computed if and only if k_i members from $(\cup_{j=1}^{i} \mathcal{U}_j)$ are present. Hence for a set of participants, reconstruction of each s_i ensures one threshold condition in Γ of definition 3.3.1. Since we require any c of such threshold conditions among m, the purpose of applying first a (c, m) scheme on the secret follows.

3.3.2 Efficiency Issues, Perfectness and Discussions

In scheme 1, each participant from $\mathcal{U}_1$ is given m shares, each participant from $\mathcal{U}_2$ is given $m-1$ shares and so on. Eventually, a participant from the lowest level $\mathcal{U}_m$ is given only 1 share. In the order of operations performed for the reconstruction of the secret, there are m Lagrange interpolations each of which is to recover one of the partial secrets $s_1, \ldots, s_m$, and there is one final occurrence of a (c, m) Shamir's scheme summing up to $m + 1$ instances of Lagrange interpolations. Again all these schemes can be combined by lemma 3.1.1. Since Lagrange interpolations are used as basic building blocks, the above scheme is perfect by lemma 3.1.2 and hence enjoys the property of reconstructability of the secret by an authorized set with probability 1.

An observation on the difficulty of establishing an ideal and efficient LSSS for the realization of (3) is as follows. In [19], it is proven that a multipartite access structure involving a hierarchy among participants is ideal if and only if the access structure admits a vector space secret sharing scheme. So if there exists an ideal and efficient scheme realizing (3), it must be in the form of a vector space scheme, that is an ideal linear scheme constructed according to the method proposed by Brickell. In such a scheme, we are allowed to assign one and only one public vector to each participant including the target vector of the dealer, so that the shares are computed by dot products of these vectors with a random (secret) vector. Within such a setting, the purpose is to design a scheme which both allows higher-leveled participants to replace their inferiors and assures the satisfaction of any c of the m conditions defined on levels. Such a design may not be easy especially when one considers the varying size of minimal authorized subsets, which makes the establishment a little more complicated. We would like to remind the reader that finding an efficient, perfect, ideal and linear solution for the disjunctive case of Simmons has remained a long standing open problem and its realization became possible in [4], only when some duality techniques were employed to the efficient and perfect vector space construction of its conjunctive counterpart, which has fixed length minimal authorized subsets. However, this approach does not seem to apply to (3), as for $1 < c < m$, the dual of a (c, m) hierarchical access structure is a $(m + 1 - c, m)$ hierarchical access structure, again having variable-length minimal authorized subsets. Indeed, regarding compartmented and hierarchical (c, m) access structures, our intuition is that the schemes that we realize herein have already attained best possible information rates. However, this

statement is no further realistic than a conjecture without a proof, which may not be easy to construct, and is out of scope of this work.

A final remark on efficiency is that, in scheme 1, the number shares of a user is at most m, yielding to an information rate such as $\frac{1}{m}$. However, we would like to note that, information rate is not he only notion of efficiency. Indeed, another similar complexity measure of secret sharing schemes is their share size, that is, the total length of all shares distributed by the dealer. Scheme 1 performs slightly better in the latter case than it does in the case of information rate. The reason is that, as there are typically more participants in the lower levels compared to that of higher ones, the average number of shares per user is usually lower than a worst case of $\frac{m+1}{2}$. The scheme we provide is obviously not be the best choice for the cases $c = 1$ or $c = m$. However, to the best of our knowledge, it is the only scheme that realizes the intermediary access structures in between two former definitions involving a hierarchy, it is perfect and is efficient enough for scenarios with small parameters.

3.3.3 Fixing first k levels

Observe that for the case $c = 2$ of example 3.3.2, it is possible for a group of brigadiers and colonels to reconstruct the secret without the presence of any admirals. However, the dealer may desire the existence of at least one admiral in an authorized set, that is, while the subsets $\{aa, ab, acc\}$ remains authorized, bbb and bbc will be identified as non-authorized. To restate this in a more general sense, the top k compartments may be distinguished by the necessity of satisfaction of all the conditions defined upon them, whereas this is not the case for the remaining lower compartments. That is, as in the case of (c, m) compartmented access structures, one may fix the first k compartments and obtain the generalized definition $\Gamma' = \{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \ \forall i \in \{1, \ldots, k\}$ and for at least c indices $i \in \{k+1, \ldots, m\}\}$ under the same settings of definition 3.3.1. Here, k is the threshold value assuring that the conjunction of k conditions on the first k levels holds in an authorized set. Among the remaining $m - k$ conditions left out, any c of them are considered to be enough. Γ' trivially becomes equivalent to Γ of definition 3.3.1 when $k = 0$. A realization of Γ' is as follows.

scheme 2. We combine Tassa's conjunctive scheme involving Birkhoff interpolation and scheme 1 in a way handling Γ'. The dealer first applies Tassa's conjunctive scheme to participants of the first k levels $\mathcal{U}_i$, $i \in \{1, \ldots, k\}$. So far, members of levels $\mathcal{U}_1, \ldots, \mathcal{U}_k$ are given

one share apiece. On the other hand, the dealer applies scheme 1 to members of the remaining levels $\mathcal{U}_{k+1}, \ldots, \mathcal{U}_m$, so that a participant from level $\mathcal{U}_{k+1}$ is given $m - k$ shares, a participant from level $\mathcal{U}_{k+2}$ is given $m - k - 1$ shares and finally, a participant from level $\mathcal{U}_m$ is given only 1 share. For now, we have only partitioned the levels to two sets with indexes $1, \ldots, k$ and $k + 1, \ldots, m$ applying Tassa's conjunctive scheme and scheme 1 to each set respectively. The only missing part for the realization of Γ' is the allowance of members of $\mathcal{U}_1, \ldots, \mathcal{U}_k$ to substitute lower-leveled participants belonging to $\mathcal{U}_{k+1}, \ldots, \mathcal{U}_m$. To achieve this, we give a set of $m - k$ additional shares to each member of levels $\mathcal{U}_1, \ldots, \mathcal{U}_k$. Such $m - k$ shares are identical to the set of shares given to members of U_{k+1}, so that members of $\mathcal{U}_1, \ldots, \mathcal{U}_k$ can always replace members of $\mathcal{U}_{k+1}, \ldots, \mathcal{U}_m$, which completes the scheme. The highest number of shares distributed belongs to members of levels $\mathcal{U}_1, \ldots, \mathcal{U}_k$, where each participant is given $m - k + 1$ shares.

Tassa's conjunctive scheme [4] is proven to be perfect for a sufficiently large field via a monotone allocation of participant identities. With such an employment of Tassa's scheme and a series of Shamir's schemes in the basis of scheme 2, perfectness follows from lemma 3.1.2. As an underlying scheme for first k levels, one can of course choose any other scheme realizing (1), say the one given in [5], instead of the one employing Birkhoff interpolation [4]. But if the chosen scheme is not perfect with certainity, scheme 2 will not reach perfectness with certainity either. Except that, the selection will not affect scheme 2.

It is described in [4] that the realization of the disjunctive access structure (2) can be achieved with the help of the conjunctive scheme realizing (1), and some duality techniques. On the other hand, scheme 2 is designed for the cases $1 < c < m$ as it combines Tassa's conjunctive scheme for (1) and scheme 1. A particular case is as follows. When $c = 1$ in Γ', one may alternatively combine both Tassa's conjunctive and disjunctive schemes and apply to compartments $\mathcal{U}_1, \ldots, \mathcal{U}_k$ and $\mathcal{U}_{k+1}, \ldots, \mathcal{U}_m$ respectively to obtain a better information rate such as $\frac{1}{2}$.

CHAPTER 4

NESTED MULTIPARTITE SECRET SHARING

Quite recently, Tassa introduced an ideal and perfect secret sharing scheme realizing conjunctive hierarchical threshold access structures motivated by the problem of sharing a private key among three employees of a bank, at least one of whom must be a department manager, for the purpose of signing an electronic funds transfer. We ask the natural question concerning "What if there are two branches of banks that are needed to be involved in the signing process?" In such a case, one might encounter the presence of two distinct hierarchies involved in the same access structure. In this chapter, being motivated by such a sample scenario, we describe a new generalization, what we name nested multipartite access structures, which may involve the well-known compartmented or hierarchical access structures as a substructure. The corresponding generic scheme we describe employs multivariate interpolation and is ideal, linear and perfect with probability $1 - O(q^{-1})$ on a finite field $\mathbb{F}_q$. We describe the scheme in particular for the trivariate case as an example. Such an approach is hopefully useful not only for the initial motivating example, but also for a variety of interesting scenarios. In particular, we propose a non-nested generalization for the conventional compartmented access structures, which depicts a stronger way of controlling the additional $t - (t_1 + \ldots + t_m)$ participants.

Motivation. Multipartite access structures are on focus mainly because they model very natural situations in practice. Besides, theoretically, they form a generalization of (t,n) access structures as every (t,n) access structure can be regarded as a multipartite access structure. In this chapter, we consider a generalization, what we call *nested multipartite access structures*. We essentially consider a case when another dimension on the access structure is added, so that we allow a compartment to be nested, that is, it may have have sub-compartments. In this case, we refer to the outer compartments involving others as *substructures* of the access structure. However, the inner compartments are not allowed to contain others in the case of

a nested access structures of order 1. To the best of our knowledge, the only study that considers access structures that may involve compartments defined within other compartments is [9]. However, in that work, the definition of Γ is so narrow in the sense that, each substructure not only contains the same number of compartments, but also does not involve any kind of threshold conditions on the compartments it involves or on the total number of participants, both of which are essential in many samples of multipartite access structures in the literature. Instead, it is required that each substructure of the access structure is required to have members from a certain number of distinct compartments, which is handled by a straightforward scheme of Shamir's on each substructure, such that, members of the same compartment are given the same share. So the essential reason that the work [9] remained somehow unfamiliar lies in the very specific way of the approach taken. Another reason maybe that it was perhaps a little early for such a generalization of a nested structure as is shown by the fact that no similar work is carried (to us) on the topic. However, since the publication of [9], namely late nineties, secret sharing has evolved significantly in the sense that some new and interesting multipartite access structures are considered, better solutions to the existing ones are provided, theoretical bounds on information rates of certain characterizations are improved, interconnections with distinct theoretical fields are investigated, and the number of applications of secret sharing, such as the ones on secure multi-party protocols and wireless sensor network security, has increased. We believe that ideal schemes for more sophisticated access structures might be of public interest, as the ones we consider throughout this work.
Multivariate interpolation in general may carry slightly different meanings such that it constitutes quite a general naming for a series of different methods. A recent and novel employment of multivariate interpolation in a closely related field, such as decoding of error correcting codes, is considered in [16]. On the other hand, in [5], the scheme realizing the recent multipartite access structure given in [6] is regarded as being based on bivariate interpolation, as it essentially involves two distinct types of variables, yielding to a bivariate secret polynomial. As the scheme we employ in is designed in a manner that the secret is a linear combination of multiple variables, we follow [5] in the sense that we identify our scheme as employing multivariate interpolation.

Organization of the chp. We consider some preliminary non-nested access structures and corresponding linear schemes, in section 4.1. In particular, we consider, in 4.1.4, a generalization named *selective compartmented access structure*, which is based upon the conventional

compartmented access structure, extending its capabilities. We describe nested multipartite access structures together with a generic linear scheme and some demonstrations in section 4.2.

4.1 Subschemes

In sections 4.1.1, 4.1.2 and 4.1.3, we cover some particular schemes for some known multipartite access structures. These schemes are to be exploited in the realization of nested access structures and will be referred to as a *subscheme* for such an employment. We particularly consider a new and a non-nested access structure in 4.1.4, followed by some remarks involving justifications of the subschemes chosen in 4.1.5. Hereinafter, let $\mathbb{F} = \mathbb{F}_q$ be a finite field and let s denote the secret to be shared. Before proceeding, let us consider a preliminary fact borrowed from [5], which will be helpful in the perfectness proof of the scheme we present herein.

Lemma 4.1.1 *(Schwartz-Zippel Lemma). Let $G(z_1, z_2, ..., z_k)$ be a nonzero polynomial of k variables over a finite field $\mathbb{F}_q$. Assume that the highest degree of each of the variables z_j that G is based on is no larger than d. Then the number of zeros of G in $\mathbb{F}_q^k$ is bounded from above by kdq^{k-1}.*

4.1.1 A Scheme for Conjunctive Hierarchical Access structures

Let us recall the hierarchical threshold access structures introduced in [4]. Let $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$ be the set of participants with m disjoint levels, i.e., $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$, for $i \neq j$, and let $k_1 < k_2 < \ldots < k_m$ be a sequence of thresholds with $0 < k_1$. Then the corresponding conjunctive hierarchical access structure is defined by

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i \quad \forall i \in \{1, \ldots, m\}\} \tag{1}$$

Let us describe a scheme that realizes (1), which can be regarded as a modified version of the scheme given in [4] involving Birkhoff interpolation. The following scheme, being implicitly given in [11], is considered therein to have better multiplicative properties than the original version considered in [4].

subscheme 1.

1. The dealer generates a random polynomial $P(x) = \sum_{j=0}^{k_m-1} a_j x^j \in \mathbb{F}[x]$ of degree $k_m - 1$ with $a_0 = s$ and truncated polynomials P_i, $1 \leq i \leq m$ each with a subset of coefficients obtained from $P(x)$ such as, $P_i(x) = \sum_{j=k_{i-1}}^{k_m-1} a_j x^j$ where we take $k_0 = 0$ for P_1.

2. Each participant u_{ij} from level $\mathcal{U}_i$ is given a public point $0 \neq x_{ij} \in \mathbb{F}$ with $x_{ij} \neq x_{i'j'}$ for $(i, j) \neq (i', j')$ and a private share $P_i(x_{ij})$.

Note that a user $u_{ij} \in U_i$ is given a linear equation for the highest degree $k_m - k_{i-1}$ coefficients of P, but this carries no information on the remaining lowest degree coefficients.

4.1.2 A Scheme for Disjunctive Hierarchical Access Structures

Under the same assumptions of (1), the former hierarchical access structure that is studied by Simmons is as follows.

$$\Gamma = \{\mathcal{V} \subset \mathcal{U}, \exists i \in \{1, \ldots, m\} : |\mathcal{V} \cap (\cup_{j=1}^{i} \mathcal{U}_j)| \geq k_i\} \tag{2}$$

In both definitions, $\mathcal{U}_1$ is the highest level in the hierarchy. Observe that the only difference in (2) is the replacement of the universal quantifier $\forall$ with the existential quantifier $\exists$. A well-known scheme realizing (2) is as follows.

subscheme 2.

1. The dealer generates a random polynomial $P(x) = \sum_{j=0}^{k_m-1} a_j x^j \in \mathbb{F}[x]$ of degree $k_m - 1$ with $a_0 = s$ and truncated polynomials P_i, $1 \leq i \leq m$ each with a subset of coefficients obtained from $P(x)$ such as, $P_i(x) = \sum_{j=0}^{k_i-1} a_j x^j$

2. Each participant u_{ij} from level $\mathcal{U}_i$ is given a public point $0 \neq x_{ij} \in \mathbb{F}$ with $x_{ij} \neq x_{i'j'}$ for $(i, j) \neq (i', j')$ and a private share $P_i(x_{ij})$.

On the contrary to subscheme 1, this time, a highest level user is given a linear equation formed by least number of coefficients.

4.1.3 A Scheme for Compartmented Access structures

The compartmented access structure given in [7] is as follows. Let $\mathcal{U} = \cup_{i=1}^{m} C_i$ be the set of participants with m disjoint compartments, that is, $C_i \cap C_j = \emptyset$, for $i \neq j$. Let $t_i \in \mathbb{N}$ be

threshold values for compartments C_i, $1 \leq i \leq m$, respectively and let $t \in \mathbb{N}$ be the threshold such that $t \geq \sum_{i=1}^{m} t_i$. Then

$$\Gamma = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V} \text{ such that } |\mathcal{W} \cap C_i| \geq t_i \ \forall i \in \{1, \ldots, m\} \text{ and } |\mathcal{W}| = t\} \tag{3}$$

For the realization of (3), there exists several schemes such as the scheme proposed by Brickell [7] and some variations. An interesting recent approach [5] employs bivariate interpolation by first applying a scheme that realizes the dual access structure of (3), namely the compartmented access structure with upper bound, and than converting this to a scheme realizing (3) by some duality techniques. A more direct approach [8] can again be identified as exploiting bivariate interpolation, though the authors do not claim so, in the sense that the given scheme makes use of polynomials with two types of variables (a_{ij} and β_i as given in the notation of [8]). In this work, the authors claim that their scheme is perfect, however they miss the crucial point of checking the determinants of the reconstruction matrices formed by authorized subsets of participants. That is, with a probability in contrast to the size of the underlying field $\mathbb{F}_q$, the reconstruction matrix may not have full rank and hence it might be the case that an authorized set of participants can not recover the secret[1]. Indeed, all the aforementioned schemes [7,8,5] realizing compartmented access structure (3) are perfect for a random allocation of participant identities with high probability. To the best of our knowledge, no ideal linear scheme realizing (1) attains perfectness with probability 1, without a precomputation of determinants of possible reconstruction matrices. Regarding the compartmented case, we nevertheless adopt the scheme given in [8], with a slight modification, as a subscheme to serve in the case of nested multipartite access structures, as it provides a rather more direct solution when compared to the one in [5]. Now the following describes a SSS to realize (3).

subscheme 3.

1. Define $\ell = t - \sum_{i=1}^{m} t_i$. We omit the case $\ell = 0$ as in this case the problem is trivial. The dealer generates ℓ random coefficients $b_0, \ldots, b_{\ell-1}$ and $m + 1$ random polynomials $P_i(x) = \sum_{j=0}^{t_i-1} a_{ij}x^j$, $1 \leq i \leq m$ and $P(x) = \sum_{i=t_i}^{t_i+\ell-1} b_{i-t_i}x^i$ over a field $\mathbb{F}_q$ such that $\deg(P_i(x)) = t_i - 1$, and the secret is $b_0 + \sum_{i=1}^{m} a_{i0}$.

2. Identify each participant $u_{ij} \in C_i$ by a unique public point $x_{ij} \neq 0$, such that no two participants are given the same x_{ij} value. The private share of the participant u_{ij} is $P_i(x_{ij}) + P(x_{ij})$.

[1] We leave the verification of such a statement with a counter-example on perfectness say formed by parameters $t_1 = 1$, $t_2 = 1$, $t = 4$ and participant identities $x_{11} = 2$, $x_{12} = 3$, $x_{21} = 1$, $x_{22} = 4$, in $\mathbb{F}_5$.

Adding the result of the evaluation of the polynomial $P(x)$ at the public point x_{ij}, to the private share of each participant u_{ij}, is a well-known common technique employed in several schemes such as the ones corresponding to compartmented cases in [8,5] and also in the scheme realizing the access structure [6] of Herranz and Sáez again in [5]. We will utilize the same technique in a slightly different way to first realize the selective compartmented access structure that we describe below and then to realize nested multipartite access structures, in the next section, where we allow any of the access structures considered in this section to be substructures.

4.1.4 A Generalization: Selective Compartmented Access Structure

Let us describe a generalization of the compartmented access structure Γ of (3) and a tweak for its realization. Suppose that the dealer wants some certain number of the additional ℓ participants come from a certain union of compartments. Indeed, he may define more than one, say r, such restrictions on the additional participants by defining r distinct unions. For this purpose, we describe a partition on ℓ additional participants as follows. First, define r *chosen sets of compartments* $\mathcal{CSC}_1, \ldots, \mathcal{CSC}_r \subseteq \{C_1, \ldots, C_m\}$, each of which is a distinct union of arbitrary compartments. More formally,

$$\mathcal{CSC}_i = \bigcup_{C_j \in \{C_1, \ldots, C_m\}} C_j, \;\; \mathcal{CSC}_i \neq \mathcal{CSC}_j \text{ for } i \neq j.$$

Each $\mathcal{CSC}$ helps defining a rule that restricts a certain number of additional participants to some certain subsets of compartments. In this respect, associate each $\mathcal{CSC}_i$ with a $p_i \in \mathbb{N}$, $1 \leq i \leq r$ to obtain the additional condition $|\mathcal{V} \cap \mathcal{CSC}_i| - \sum_{C_j \in \mathcal{CSC}_i} t_j \geq p_i$. Such a condition guarantees that at least p_i of the additional $\ell = \sum_{i=1}^{r} p_i$ participants will be coming from the specifically chosen set of compartments $\mathcal{CSC}_i$. As in the case of (3), $t - \sum_{i=1}^{m} t_i = \ell$. The modified access structure is as follows.

Definition 4.1.2 *A selective compartmented access structure* Γ' *(under the aforementioned initializations) is*

$$\Gamma' = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V} \textit{ such that } |\mathcal{W} \cap C_i| \geq t_i \;\forall i \in \{1, \ldots, m\} \qquad (3')$$

$$\textit{and } |\mathcal{W}| = t \textit{ and } |\mathcal{W} \cap \mathcal{CSC}_i| - \sum_{C_j \in \mathcal{CSC}_i} t_j \geq p_i, \;\; \forall i \in \{1, \ldots, r\}\}$$

Observe that, the generalization Γ' comprehends Γ in the sense that when $r = 1$ with one and only $\mathcal{CSC}_1 = \bigcup_{i=1}^{m} C_i$, involving all the compartments $C_1, \ldots, C_m$ and requiring $\ell = p_1 = t - \sum_{i=1}^{m} t_i$ additional participants, then such an access structure reduces to Γ of (3). For a fixed $i \in \{1, \ldots, m\}$, let the renumeration (indexed set) of the $k \leq r$ chosen sets of compartments that consist C_i be $\mathcal{CSC}_{C_i} = \{\mathcal{CSC}_1, \ldots, \mathcal{CSC}_k : C_i \in \mathcal{CSC}_j,\ 1 \leq j \leq k\}$. The realization of Γ' can be achieved as follows.

subscheme 3'.

1. Define $\ell = t - \sum_{i=1}^{m} t_i$. The dealer generates $\ell = \sum_{i=1}^{r} p_i$ random coefficients b_{ij}, $1 \leq i \leq r$, $0 \leq j \leq p_i - 1$ and m random polynomials $P_i(x) = \sum_{j=0}^{t_i - 1} a_{ij} x^j$, $1 \leq i \leq m$ over a field $\mathbb{F}_q$ such that $\deg(P_i(x)) = t_i - 1$.

2. The secret is $\sum_{i=1}^{r} b_{i0} + \sum_{i=1}^{m} a_{i0}$.

3. Identify each participant $u_{ij} \in C_i$ by a unique public point $x_{ij} \neq 0$, such that no two participants are given the same x_{ij} value. The private share of the participant $u_{ij} \in C_i$ is $P_i(x_{ij}) + \{\sum Q_c(x_{ij}) : \mathcal{CSC}_c \in \mathcal{CSC}_{C_i}\}$ where $Q_c(x_{ij}) = \sum_{d=0}^{p_c - 1} b_{cd} x_{ij}^{d + t_i + \sum_{e=1}^{c-1} p_e}$ such that the exponent of x_{ij} in $Q_1(x)$ is $d + t_i$. (That is, for all $\mathcal{CSC}_c$'s involving C_i, we add to the secret a polynomial Q_c with p_c coefficients corresponding to $\mathcal{CSC}_c$, such that Q_c is evaluated at x_{ij} and c is the index running through all $\mathcal{CSC}'s$ in $\mathcal{CSC}_{C_i}$.)

Theorem 4.1.3 *Scheme 3' realizes the selective compartmented access structure (3') and is perfect with a probability* $1 - O(q^{-1})$ *on a finite field* $\mathbb{F}_q$.

Proof. The idea is as follows. The reconstruction of the secret is essentially solving some linear system. If the set of participants $\mathcal{V}$ is non-authorized, so that $\mathcal{V} \notin \Gamma$, participants of $\mathcal{V}$ encounter a missing number of equations while solving the system for unknown coefficients. On the other hand, the number of linear equations that an authorized subset $\mathcal{V} \in \Gamma$ owns is at least as much as the number of unknowns. Indeed, with very high probability, these equations are linearly independent so that the determinant of the reconstruction matrix is nonzero. In other words, the determinant corresponding to an authorized coalition is nonzero with a probability closer to 1 as the field size approaches to infinity, which is essentially because the public coefficients of the reconstruction matrix are uniformly selected random elements from a field of size q and the determinant is defined upon them. A more formal treatment is as follows. Let $\mathcal{V}$ be a minimal authorized set of participants, such that

$|\mathcal{V}| = t$, $|V \cap C_i| \geq t_i,\ \ i \in \{1,\ldots,m\}$ and $|\mathcal{W} \cap \mathcal{CSC}_i| - \sum_{C_j \in \mathcal{CSC}_i} t_j \geq p_i,\ \forall i \in \{1,\ldots,r\}$. For the sake of simplicity of the visualization, suppose that a compartment is involved in one and only one $\mathcal{CSC}$ and the number of compartments in $\mathcal{CSC}_i$ is k_i so that $\sum_{i=1}^{r} k_i = m$. Then the recovery of the polynomials $P_i(x)$ and $P(x)$ corresponds to the solution of the system of linear equations $M.A = Q$ where the form of txt matrix M depends on the the additional conditions defined via $\mathcal{CSC}$'s and the specific set of participants that came together, $A = (a_{10}\ldots a_{1,t_1-1}a_{20}\ldots a_{2,t_2-1}\ldots a_{m0}\ldots a_{m,t_m-1}\, b_{10}\ldots b_{1,p_1-1}b_{20}\ldots b_{2,p_2-1}\ldots b_{r0}\ldots b_{r,p_r-1})^t$, and Q is the vector formed by private shares of the participants in order.

Employing linear algebra, we know that the equation $M.A = Q$ has a unique solution if and only if $det(M) \neq 0$. On the other hand, the probability that an authorized set can reconstruct the secret equals to the probability of $det(M) \neq 0$ where M is their corresponding reconstruction matrix. Considering the expansion of the determinant, we make the following observations. Firstly, $det(M)$ is a polynomial of t variables: $\sum_{i=1}^{m} t_i$ of which are a_{ij}'s and the remaining $\ell = \sum_{i=1}^{r} p_i$ of them are b_{ij}'s. Say the highest degree of the variables in $det(M)$ is d. Now applying lemma 4.1.1, we see that the number of zeros of $det(M)$ in $\mathbb{F}^t$ is bounded by tdq^{t-1}. Indeed, these are all the choices that make $det(M) = 0$ among all possible q^t selections of the t variables. So the probability that $det(M) = 0$ is bounded by $tdq^{t-1}.q^{-t} = tdq^{-1}$. ■

Example 4.1.4 *Let $m = 3$ and $t_1 = 2$, $t_2 = 2$, $t_3 = 3$ respectively for C_1, C_2, C_3 and $t = 8$. Assuming that the additional 1 participant is from C_3, the reconstruction matrix for compartmented access structure (3) formed by the scheme (3) is as follows.*

$$M_1 = \begin{pmatrix} 1 & x_{11} & 0 & 0 & 0 & 0 & 0 & x_{11}^2 \\ 1 & x_{21} & 0 & 0 & 0 & 0 & 0 & x_{11}^2 \\ 0 & 0 & 1 & x_{21} & 0 & 0 & 0 & x_{21}^2 \\ 0 & 0 & 1 & x_{22} & 0 & 0 & 0 & x_{22}^2 \\ 0 & 0 & 0 & 0 & 1 & x_{31} & x_{31}^2 & x_{31}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{32} & x_{32}^2 & x_{32}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{33} & x_{33}^3 & x_{33}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{34} & x_{34}^3 & x_{34}^3 \end{pmatrix}$$

Now suppose that we want to add a condition that restricts the additional 1 participant to be coming either from C_1 or C_3 but not from C_2 so that we arrive a selective compartmented access structure. Then using scheme 3', the reconstruction matrix of an authorized subset for

which the additional participant belongs to again C_3 would be;

$$M_2 = \begin{pmatrix} 1 & x_{11} & 0 & 0 & 0 & 0 & 0 & x_{11}^2 \\ 1 & x_{21} & 0 & 0 & 0 & 0 & 0 & x_{11}^2 \\ 0 & 0 & 1 & x_{21} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x_{22} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x_{31} & x_{31}^2 & x_{31}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{32} & x_{32}^2 & x_{32}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{33} & x_{33}^3 & x_{33}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{34} & x_{34}^3 & x_{34}^3 \end{pmatrix}$$

The unknown vector for M_1 will be $(a_{10}\, a_{11}\, a_{20}\, a_{21}\, a_{30}\, a_{31}\, a_{32}\, b_0)^t$ where the last term b_0 is to be replaced by b_{10} in the unknown vector of M_2. The target vector for both the systems is $\mathbf{t} = (1\,0\,1\,0\,1\,0\,0\,1)$.

4.1.5 Perfectness of the Subschemes

For a random allocation of participant identities, with a high probability such as $1 - O(q^{-1})$ over a field $\mathbb{F}_q$, subscheme 3' of this section is shown to be perfect. For this purpose, the well-posed proof techniques given in [5] are utilized in the same fashion they are employed for the compartmented case therein. One can similarly show the perfectness with probability $1 - O(q^{-1})$ of the subschemes 1,2,3 via the employment the same techniques. We would like to note that the solutions to cases of conjunctive and disjunctive hierarchical access structures established in [4] enjoy the reconstructability of the secret with a probability exactly 1, when compared to the solutions here attaining probabilities merely close to 1. However, this nice feature fades away when combined with the technique we employ in the next section, to obtain a nested multipartite access structure. So for our case, there is no difference of the employment of the conjunctive scheme given in [4] and subscheme 2. This explains the reason for us to choose the simple subschemes considered herein, instead of the nice solutions in [4], for the conjunctive and disjunctive cases. Finally, all the subschemes 1,2,3 and 3' are ideal and linear.

4.2 Nested Multipartite Access Structures

4.2.1 Definition and a Generic Scheme

A multipartite access structure is the one that the set of participants is partitioned into some set of compartments, and the participants in the same compartment are not distinguished. We identify an access structure as *non-nested*, if no compartment within the access structure involves any other compartments. On the contrary, a compartment of a *nested* multipartite access structure (or nested access structure in short) may involve other compartments. The simplest case is what we call a nested multipartite access structure of order 1, where an outer compartment may embody a series of inner compartments, however the inner compartments may not. In this case, an outer compartment is called a *substructure* which may be in the form of any non-nested multipartite access structure so that a substructure may have its own threshold conditions. In other words, we define a nested access structure essentially as a series of conventional multipartite access structures, which are now referred to as substructures, and are brought together with a total threshold condition t on the number of participants belonging to any substructure. Hence, the definition of an authorized set Γ, in the case of nested multipartite access structures, is generic and depends on the form of substructures. We nevertheless give a sample definition for a nested access structure that may involve widely-studied substructures of the form (1), (2) and also substructures of the form (3'), the fresh generalization of (3).

Let $\mathcal{U} = \bigcup_{i=1}^{m} C_i$ be a set of participants with m substructures, and let the number of inner compartments of each substructure C_i be m_i so that

$$C_i = \bigcup_{\substack{1\le i\le m \\ 1\le j\le m_i}} C_{ij} \text{ with } \mathcal{U}_{i_1} \cap \mathcal{U}_{i_2} = \emptyset \text{ for } i_1 \neq i_2, \mathcal{U}_{i_1 j_1} \cap \mathcal{U}_{i_2 j_2} = \emptyset \text{ for } (i_1, j_1) \neq (i_2, j_2)$$

Identify the substructures of the form (1) by $C_1, \ldots, C_{c_1}$, the substructures of the form (2) by $C_{c_1+1}, \ldots, C_{c_2}$ and the substructures of the form (3') by $C_{c_2+1}, \ldots, C_m$. Let $\mathcal{V}$ be an authorized set. Define $t, t_i, t_{ij} = t_{i,j} \in \mathbb{N}$, $1 \le i \le m$, $1 \le j \le m_i$ such that $t_{i,j+1} > t_{i,j}$ and $t_i = t_{im_i} \forall i \in \{1, \ldots, c_2\}$, $\forall j \in \{1, \ldots, m_i - 1\}$[2]. Define the vector $\mathbf{t} = (t, t_1, \ldots, t_m, t_{11}, \ldots, t_{mm_i})$. This time, we do not restrict the chosen sets of compartments to the access structures of type

[2] Note that for the hierarchical cases, we abuse the widely accepted notation of k_i of (1) and (2) and replace it with t_{ij}, for the sake of being able to express all the threshold values of the nested access structure by sub-indexes of one single letter such as t.

(3') but we let a $\mathcal{CSC}$ involve compartments from all the substructures, with one restriction. To not to disrupt the hierarchies in the substructures of the form (1) and (2), we allow a $\mathcal{CSC}$ embody a compartment within a hierarchically ordered substructure only when it involves its hierarchical superiors. Let $\mathcal{CSC}_1, \ldots, \mathcal{CSC}_r$ denote the chosen sets of compartments associated with $p_1, \ldots, p_r$ defined as $\mathcal{CSC}_n = \bigcup_{C_{ij} \in \{C_1, \ldots, C_m\}} C_{ij}$, with $C_{ij} \in \mathcal{CSC}_n \Rightarrow C_{ij'} \in \mathcal{CSC}_n \, \forall j' < j, \ \forall i \in \{1, \ldots, c_2\}, \ n \in \{1, \ldots, r\}$ and $\mathcal{CSC}_n \neq \mathcal{CSC}_{n'}$ for $n \neq n'$. Note that now it is possible for a $\mathcal{CSC}$ to involve compartments from hierarchical substructures as well as compartments of the substructure of the form (3'). For a fixed $i \in \{1, \ldots, c_2\}$, let the maximum of the threshold values t_{ij} of the compartments C_{ij} that are involved in $\mathcal{CSC}_n$ be denoted by $t_{max}(i, n) = \{max(t_{ij}) : C_{ij} \in \mathcal{CSC}_n\}$ such that $t_{max}(i, n) = 0$ whenever $C_i \cap \mathcal{CSC}_n = \emptyset$.

Definition 4.2.1 *The nested multipartite access structure* Γ *involving substructures of the forms (1),(2) and (3') with threshold* $\mathbf{t}$ *(within the prescribed setting) is the set of all participant sets* $\mathcal{V}$ *with* $\exists \mathcal{W} \subset \mathcal{V}$ *such that*

i) $|\mathcal{W}| = t$

ii) $|\mathcal{W} \cap C_i| \geq t_i, \forall i \in \{1, \ldots, m\}$

iii) $|\mathcal{W} \cap (\cup_{n=1}^{j} C_{in})| \geq t_{ij}, \ \forall i \in \{1, \ldots, c_1\}, \ \forall j \in \{1, \ldots, m_i\}$

iv) $|\mathcal{W} \cap (\cup_{n=1}^{j} C_{in})| \geq t_{ij}$, *for at least one* $i \in \{c_1 + 1, \ldots, c_2\}, \ \forall j \in \{1, \ldots, m_i\}$

v) $|\mathcal{W} \cap C_{ij}| \geq t_{ij} \ \forall i \in \{c_2 + 1, \ldots, m\}, \ \forall j \in \{1, \ldots, m_i\}$

vi) $|\mathcal{W} \cap (\mathcal{CSC}_n \cap (\cup_{i=1}^{i=c_2} C_i))| - \sum_{i=1}^{i=c_2} t_{max}(i, n) \geq p_n, \ \forall n \in \{1, \ldots, r\}$

vii) $|\mathcal{W} \cap (\mathcal{CSC}_n \cap (\cup_{i=c_2+1}^{i=m} C_i))| - \sum_{C_{ij} \in (\mathcal{CSC}_n \cap (\cup_{i=c_2+1}^{i=m} C_i)} t_{ij} \geq p_n, \ \forall n \in \{1, \ldots, r\}$

The first two conditions *i,ii* are there to simply assure the total threshold value t and the threshold values t_i on the substructures C_i. Conditions *iii,iv,v* are, on the other hand, the regular requirements representing the characteristics of each substructure. Letting $\ell = \sum_{i=1}^{r} p_i$ denote the additional participants that may be coming from any of the substructures as before, we again partition them as p_n of them are required to be coming from compartments belonging to $\mathcal{CSC}_n$. However, the representation of this condition differs for the hierarchical compartments belonging to (1) or (2) and the compartments belonging to (3'), yielding to the conditions *vi, vii*. One may consider a simpler nested access structure by getting rid of the conditions *vi,vii*. But this time, the control of the dealer on the additional number of participants belonging to arbitrarily defined compartments of distinct substructures would disappear. Let us now describe a scheme for the aforementioned nested access structure.

scheme 1.

1. The dealer generates random polynomials $P_i(x) = \sum_{j=0}^{t_{im}-1} a_{ij}x^j \in \mathbb{F}[x]$ of degree $t_{im} - 1$ for $i \in \{1, \ldots, c_2\}$. The dealer also generates;

-truncated polynomials $P_{ij}(x)$, $1 \leq i \leq c_1$, $1 \leq j \leq m_i$ each with a subset of coefficients obtained from $P_i(x)$ such as, $P_{ij}(x) = \sum_{k=t_{j-1}}^{t_{im}-1} a_{ik}x^k$ where we take $t_0 = 0$ for P_{i1}.

-truncated polynomials $P_{ij}(x)$, $c_1 + 1 \leq i \leq c_2$ each with a subset of coefficients obtained from $P_i(x)$ such as, $P_{ij}(x) = \sum_{k=0}^{t_{ij}-1} a_{ik}x^k$.

-ℓ random coefficients b_{ij}, $1 \leq i \leq r$, $0 \leq j \leq p_i - 1$ and random polynomials $P_{ij}(x) = \sum_{k=0}^{t_{ij}-1} c_{ijk}x^k \in \mathbb{F}_q[x]$, $c_2 + 1 \leq i \leq m$, such that $\deg(P_{ij}(x)) = t_{ij} - 1$.

2. The secret is $s = \sum_{i=1}^{c_2} a_{i0} + \sum_{i=c_2+1}^{m} \sum_{j=1}^{m_i} c_{ij0} + \sum_{i=1}^{r} b_{i0}$.

3. Identify each participant $u_{ijk} \in C_{ij}$ by a unique public point $x_{ijk} \neq 0$, such that no two participants are given the same x_{ijk} value. The private share of the participant $u_{ijk} \in C_{ij}$ is $P_{ij}(x_{ijk}) + \{\sum Q_c(x_{ijk}) : \mathcal{CSC}_c \in \mathcal{CSC}_{C_i}\}$ where $Q_c(x_{ij}) = \sum_{d=0}^{p_c-1} b_{cd} x_{ijk}^{d+t_{ij}+\sum_{e=1}^{c-1} p_e}$, and the exponent of x_{ij} in $Q_1(x)$ is $d + t_{ij}$.

Scheme 1 is essentially a combination of the schemes realizing the substructures of the form (1),(2) and (3') and is obviously ideal as the share size of a participant is equal to that of the secret, where both are elements of a finite field $\mathbb{F}_q$. We omit the proof that Scheme 1 realizes nested multipartite access structure considered in this section and is perfect with a probability $1 - O(q^{-1})$ on a finite field $\mathbb{F}_q$, since the corresponding arguments are essentially similar to the ones considered in the case of selective compartmented access structures.

4.2.2 Examples

Using nested multipartite access structures may allow the dealer design and handle a more sophisticated access structure when compared to any single one of the substructures (1),(2),(3) and (3'). We would like to exemplify some cases.

Example 4.2.2 *Tassa [4] considered the problem of sharing a secret which addresses the simple setting where a bank transfer should be signed by three employees, at least one of whom must be a department manager. Now suppose that the customer who demands the bank transfer has accounts in two distinct branches of the bank, and he wants to transfer money from both of his accounts. Suppose for simplicity that the threshold conditions on each*

bank branch is the same as Tassa's setting, that is, the approval of the transfer requires three employees apiece for each bank branch, one of whom is required to be a department manager therein, summing up to six employees in total. In this setting, applying two instances of Tassa's hierarchical threshold scheme for two branches of banks solves the problem. However, suppose that a further requirement of one additional participant, belonging to any bank branch, is demanded. This time, it is not possible to design an ideal scheme without the help of a nested multipartite access structure. In the setting of a nested access structure described in 4.2.1, the compartments will be C_{11} and C_{12} which represent the participant sets of departmental managers and ordinary employees respectively for the first branch, and C_{21} and C_{22} in a similar fashion for the second branch of the bank. Calling such an authorized set $\mathcal{V}_1$, the scheme may further be designed in a way that the additional participant is required to be a departmental manager in any of the branches, rather than an ordinary employee coming from any of the compartments, forming $\mathcal{V}_2$. The corresponding matrices formed by authorized sets of participants $\mathcal{V}_1$ and $\mathcal{V}_2$ formed by participants $u_{ijk} \in C_{ij}$ with public shares x_{ijk}, $1 \leq i, j \leq 2$, where the additional seventh participant is say from C_{12} for $\mathcal{V}_1$ and from C_{11} for $\mathcal{V}_2$, are illustrated below.

$$M_{\mathcal{V}_1} = \begin{bmatrix} 1 & x_{111} & x_{111}^2 & 0 & 0 & 0 & x_{111}^3 \\ 0 & 1 & x_{121} & 0 & 0 & 0 & x_{121}^2 \\ 0 & 1 & x_{122} & 0 & 0 & 0 & x_{122}^2 \\ 0 & 1 & x_{123} & 0 & 0 & 0 & x_{123}^2 \\ 0 & 0 & 0 & 1 & x_{211} & x_{211}^2 & x_{211}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{221} & x_{221}^2 \\ 0 & 0 & 0 & 0 & 1 & x_{222} & x_{221}^2 \end{bmatrix}$$

$$M_{\mathcal{V}_2} = \begin{bmatrix} 1 & x_{111} & x_{111}^2 & 0 & 0 & 0 & x_{111}^3 \\ 1 & x_{112} & x_{112}^2 & 0 & 0 & 0 & x_{112}^3 \\ 0 & 1 & x_{121} & 0 & 0 & 0 & 0 \\ 0 & 1 & x_{122} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & x_{211} & x_{211}^2 & x_{211}^3 \\ 0 & 0 & 0 & 0 & 1 & x_{221} & 0 \\ 0 & 0 & 0 & 0 & 1 & x_{222} & 0 \end{bmatrix}$$

The unknown vector and the target vector $\mathbf{t}$ *for both the systems will be*

$(a_{10}\, a_{11}\, a_{12}\, a_{20}\, a_{21}\, a_{22}\, b_{10})^t$ *and* $\mathbf{t} = (1\,0\,0\,1\,0\,0\,1)$ *respectively.*

Example 4.2.3 *To illustrate a nested access structure involving a merging of compartmented and hierarchical substructures, this time, consider the following fictitious gloomy scenario of an old father, who is a rich businessman, having many children from his marriages but lying in his bed with a deadly disease, trying to figure out a way of informing his children, his only descendants, on his testament about how to share his wealth. The businessman does not trust any third party or a single entity, to carry this sensitive information. Indeed, he wants his children to be able to learn the distribution of his wealth only when they come together and pool their shares. However, he wants to have some flexibility for some of them who may not be able to participate or does not want the reconstruction of the secret, as a descendant who expects to be given less may not wish so. The father has a number of sons from his first marriage, and sons and daughters from his second. He trusts the elder sons, say forming the set* C_{11} *more when compared to the youngsters* C_{12}*, both of which belonging to his first marriage, yielding to a hierarchy. However, there is no such hierarchy regarding children of his second marriage. Instead, there are two compartments* C_{21} *and* C_{22} *formed by sons and daughters, respectively, with a slight distinction on them, such as having different numbers of thresholds. Let the exact thresholds be* $t_{11} = 2, t_{12} = t_1 = 3, t_{21} = 2, t_{22} = 1, t_2 = 4, t = 8$*. The additional participant in the substructure* C_2 *can be handled by defining* $\mathcal{CSC}_1 = C_{21} \cup C_{22}$*. Let* $\mathcal{CSC}_2 = C_{11} \cup C_{21} \cup C_{22}$ *be associated with the only* $\ell = 1$ *additional participant that may belong to any substructure. Let* s_{ij} *denote the number of participants from compartment* C_{ij} *and let* $s_{11} = 2, s_{12} = 1, s_{21} = 3, s_{22} = 2$ *forming the authorized set* $\mathcal{V}$*. The reconstruction matrix is as follows.*

$$M_{\mathcal{V}} = \begin{bmatrix} 1 & x_{111} & x_{111}^2 & 0 & 0 & 0 & 0 & x_{111}^3 \\ 1 & x_{121} & x_{121}^2 & 0 & 0 & 0 & 0 & x_{121}^3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & x_{211} & 0 & x_{211}^2 & x_{211}^3 \\ 0 & 0 & 0 & 1 & x_{212} & 0 & x_{212}^2 & x_{212}^3 \\ 0 & 0 & 0 & 1 & x_{213} & 0 & x_{213}^2 & x_{213}^3 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_{221} & x_{221}^2 \\ 0 & 0 & 0 & 0 & 0 & 1 & x_{222} & x_{222}^2 \end{bmatrix}$$

The corresponding unknown vector is $(a_{10}\, a_{11}\, a_{12}\, c_{210}\, c_{211}\, c_{220}\, b_{10}\, b_{20})^t$ *and the target vector*

is $\mathbf{t} = (1\,0\,0\,1\,0\,1\,1\,1)$. *The first three rows of* M *belong to participants of* $C_1 = C_{11} \cup C_{12}$, *the next three rows are the ones owned by participants from* C_{21} *and the last two rows correspond to* C_{22}. *The seventh column associated with* b_{10} *is due to the* $t_2 - (t_{21} + t_{22}) = 1$ *additional participant coming from* $CSC_1 = C_2$ *and the last column corresponding to* b_{20} *is due to the* $t - (t_1 + t_2) = 1$ *additional participant who is expected to come from* CSC_2.

4.2.3 Substructures of Other Types

As mentioned earlier, nested access structures may employ building blocks of any linear multipartite access structure as a substructure. If all the substructures exploited are ideal, the nested access structure will eventually be ideal as well.

We gave a sample definition of a nested multipartite access structure involving substructures of the form (1), (2) and (3'). The reconstruction matrices of the corresponding subschemes are involved as submatrices of the reconstruction matrix of emerging from the scheme 1, the one realizing the nested multipartite access structure we consider. Via the techniques we employ, we believe that the necessary adaptations to be performed on the subschemes realizing other kinds of substructures is obvious.

Of course, as a particular case, the substructure to be chosen may be of the type described in [6] as well, which is as follows. $\Gamma = \{\mathcal{V} \subset \mathcal{U} : \exists \mathcal{W} \subset \mathcal{V}, |\mathcal{W} \cap C_i| \geq 0 \text{ for } \ell \text{ indices } i \in \{1, \ldots, m\} \text{ and } |\mathcal{W}| = t\}$. This access structure touches upon an interesting case such as, besides having a total of at least t participants, each authorized subset must involve representatives from at least ℓ distinct compartments instead of satisfying a separate threshold condition on the number of participants from each compartment. Such a requirement is helpful in improving the diversity of coalition. A nice way of handling the above access structure is given in [5], employing bivariate interpolation. If the total threshold condition t is withdrawn, say yielding to Γ', a naive employment of the well-known scheme of Shamir would suffice such that members of the same compartment are given the same share. Indeed, when viewed with the perspective of nested multipartite access structures we present herein, the nested access structure considered in [9] corresponds to the particular case that all the substructures are of the form of Γ' and no CSC is defined upon them and in particular, the size of all the substructures are the same as they are defined to involve same number of compartments.

CHAPTER 5

CONCLUSION

Our contribution in chapter 3 is the consideration of a rich variety of multipartite access structures. A first family coming with a c out of m perspective yields generalizations of the hierarchical access structure of Simmons and the hierarchical threshold access structure of Tassa, as well as some interesting variants of the naive (c, m) access structure in the compartmented case. For the aforementioned access structures, we propose non-ideal schemes, nonetheless having acceptable information rates. Finally, all the proposed schemes are perfect. On the occasional cases that efficiency is not important (ex: for small number of participants), or when perfectness (with probability 1) is more important than efficiency, one may consider to use the schemes we describe. The following table summarizes our results of chapter 3.

(c, m) acc. str.	modification	info. rate
compartmented	- none -	1
	Γ' : k compts. fixed	1
	Γ_1 : t-threshold	$1/2$
	Γ_2 : ℓ-varying	$1/2$
	Γ_3 : doubly thresholded	$1/2$
hierarchical	- none -	$1/m$
	Γ' : highest k levels fixed	$1/(m-k+1)$

Remarks. We would like to note that the variant Γ' of hierarchical (c, m) access structures is perfect with probability 1 for not a random but a monotone allocation of participant identities in a sufficiently large field $\mathbb{F}_q$. We refer the reader to [4] for the details. Similarly for the case of Γ_2, we refer the reader to [6], for issues on perfect realization of the aforementioned ℓ-varying scheme employed in Γ_2. To realize such an ℓ-varying access structure with total threshold value t, introduced in [6], one may alternatively employ the corresponding scheme given in [5], exploiting bivariate interpolation, if a probability of perfectness $1 - O(q^{-1})$ via a random allocation of participant identities on a field $\mathbb{F}_q$ is fine enough. All the other schemes

considered in this study are perfect (with probability 1) for a random allocation of participant identities.

Our contribution in chapter 4 is that, we consider nested multipartite access structures, a generalization of conventional multipartite access structures, which in turn are referred to herein as substructures. Under such a title, we essentially follow an approach regarding the generalization that a compartment may embody other compartments. The substructures are allowed to differ, such as they might be compartmented, hierarchical or indeed any linear multipartite access structure. As an example, we show how to realize a nested multipartite access structure involving the well-known conjunctive and disjunctive hierarchical substructures, and a generalized selective compartmented substructure, that we propose herein. The substructures are combined with a threshold condition on the total number of participants coming from any of them. In this work, we consider only nested multipartite access structures of order 1, such that, an outer compartment, or a substructure, may involve inner compartments, but the inner compartments may not. If we further partition the inner compartments to some others, we obtain nested access structures of order 2. With an analogy to the techniques employed herein, one may define and realize nested multipartite access structures of higher orders, such as order 2 and above. However, it is obvious that as the orders increase, the access structure possibly becomes less realistic and its realization turns out to be less beneficial.

As a final remark, we would like to mention that secure multi-party computation techniques are available for any LSSS [13], such as the schemes we consider throughout this work.

Future work. One may attempt to prove or hopefully disprove the conjecture that we discussed in section 3.3.2, regarding the nonexistence of an efficient, perfect, ideal and linear scheme for (3), perhaps with the involvement of the techniques similar to the ones in [6,8], which is out of the scope of this work. A constructive attempt for (3) might be designing a scheme with a better information rate, if there is any. Indeed, similar arguments can be put forward for the access structures that we consider in the compartmented non-ideal case. On the other hand, we believe that nested multipartite access structures (of especially lower orders such as order 1), have potential to be employed in the embracement of various realistic situations. It might be interesting and motivating to study such possible real-life applications on distinct fields of studies such as wireless sensor networks and e-voting.

REFERENCES

[1] A. Shamir, How to Share a Secret, *Comm. ACM*, vol. 22, no. 11, 1979, pp. 612-613.

[2] G.R. Blakley, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, 1979, American Federation of Information Processing Societies Proceedings 48. 1979, pp. 313-317.

[3] G.J. Simmons, How to (really) share a secret, *Advances in Cryptology - CRYPTO 88*, LNCS 403, 1990, pp. 390-448.

[4] T.Tassa, Hierarchical Threshold Secret Sharing, *J. of Cryptology*, 20, pp. 237-264, 2007.

[5] T.Tassa and N. Dyn, Multipartite Secret Sharing by Bivariate Interpolation, *J. of Cryptology* 22, pp. 227-258, 2009.

[6] J. Herranz, G. Sáez, New Results on Multipartite Access Structures. *IEEE proc. Inf. Secur,* 153, pp. 153-162, 2006.

[7] E.F. Brickell, Some ideal secret sharing schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9, 1989, pp. 105-113.

[8] H. Ghodosi, J. Pieprzyk and R. Safavi-Naini, Secret sharing in multilevel and compartmented groups *ACISP '98: Proceedings of the Third Australasian Conference on Information Security and Privacy*, LNCS 1438, pp. 367-378, 1998.

[9] J. Maucher, Multi Dimensional Compartment Schemes, *Proc. of the 6th IMA Int. Conf. on Cryptography and Coding*, LNCS, Vol. 1355, pp. 233-238, 1997.

[10] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In Proc. of the *IEEE Global Telecom. Conf., Globecom 87*, pages 99-102, 1987. Journal version: Multiple Assignment Scheme for Sharing Secret. *J. of Cryptology*, 6(1), pp. 15-20, 1993.

[11] E. K*ä*sper, V. Nikov, S. Nikova, Strongly Multiplicative Hierarchical Threshold Secret Sharing, *Information Theoretic Security*, LNCS, Vol. 4883. Springer-Verlag Berlin Heidelberg, pp. 148, 2009.

[12] D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes, and Cryptography*, 2, pp. 357-390, 1992.

[13] R. Cramer, I. Damgård and U. Maurer: Efficient General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme. *Proceedings of 19th Annual IACR EUROCRYPT*, Springer Verlag LNCS, vol. 1807, pp. 316-334, May 2000.

[14] E. Ballico, G. Boato, C. Fontanari, and F. Granelli, Hierarchical Secret Sharing in Ad Hoc Networks through Birkhoff Interpolation, *Advances in Computer, Information, and Systems Sci. and Eng.*, pp. 157-164, 2006.

[15] C. Ma and R. Cheng, Key Management Based on Hierarchical Secret Sharing In Ad Hoc Networks, *Inscrypt 2007*, LNCS 4990, Springer-Verlag Berlin Heidelberg, pp. 182-191, 2008.

[16] F. Parvaresh, A. Vardy, Correcting errors beyond the Guruswami-Sudan radius in polynomial time, *Proc. of the 46th Annual IEEE Symp. on Foundations of Comp. Sci. (FOCS'05)*, pp. 285-294, 2005.

[17] K. Kaşkaloğlu and F. Özbudak, On Hierarchical Threshold Access Structures, *Information Assurance and Cyber Defense (IST-091)*, Antalya, Turkey, 2010.

[18] K. Kaşkaloğlu and F. Özbudak, Some Generalized Multipartite Access Structures, A non-ideal Approach, *4th Inter. Inf. Sec. and Crypt. Conf.*, Ankara, Turkey, 2010.

[19] O. Farràs and C. Padró, Ideal Hierarchical Secret Sharing Schemes, *7th IACR Theory of Cryptography Conference, TCC'10*, LNCS, (to appear), 2010.

[20] S. Fehr, Efficient construction of the dual span program. *Manuscript*, May 1999.

[21] Ventzislav S. Nikov, Verifiable Secret Sharing and Applications, PhD Thesis, *Technische Universiteit Eindhoven*, 2005.

[22] A.C. Yao, Protocols for secure computations, *Proceedings of the 23rd Annual IEEE Seymposium on Foundations of Computer Science*, pp. 160-164, 1982.

[23] T. Rabin, M. Ben-Or: Verifiable secret sharing and multiparty protocols with honest majority, *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989.

[24] B.S. Goldwasser, S. Micali, B. Awerbuch, Verifiable Secret Sharing in the Presence of Faults, *Proc. 26th IEEE Symp. on Foundations of Computer Science*, 1985.

[25] R. Ostrovsky, M. Yung, How to withstand mobile virus attack, PODC'92, pp. 51-59, 1992.

[26] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, Proactive secret sharing or: How to cope with perpetual leakage, CRYPTO'95, LNCS 963, Springer-Verlag 1995, pp. 339-352, (extended version 1998).

[27] V. Nikov, S. Nikova, On Proactive Secret Sharing Schemes, LNCS 3357, pp. 308-325, 2005.

[28] H. Krawczyk. Secret sharing made short, *CRYPTO*, 1993.

[29] H. Krawczyk. Distributed fingerprints and secure information dispersal, *PODC* 1993.

[30] C. Cachin. On-line secret sharing. *IMA: Conference on Cryptography and Coding*, Springer, 1995.

[31] V. Vinod, A. Narayanan, K. Srinathan, C. Rangan and K. Kim. On the power of computational secret sharing, *Indocrypt*, 2003.

[32] P. Rogaway, M. Bellare, Robust computational secret sharing and a unified account of classical secret-sharing goals, *Proc. of the 14th ACM conf. on Comp. and Comm. Sec.*, pp. 172-184, 2007.

[33] J. Benaloh, J. Leichter, Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88*. LNCS 403, pp. 27-35, 1990.

[34] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. of Cryptology*, vol. 6, pp. 157-168, 1993.

[35] E. F. Brickell, D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. of Cryptology*, 5(3), pp. 153-166, 1992.

[36] L. Csirmaz. The size of a share must be large. *J. of Cryptology* vol. 10, 223-231, 1997.

[37] T. Galibus and G. Matveev, Generalized Mignotte's sequences over polynomial rings, *Elec. Notes on Theo. Comp. Sci*, 186, pp. 43-48, 2007.

[38] T. Galibus, G. Matveev amd N. Shenets, Some structural and security properties of the modular secret sharing, textitProc. of SYNASC'08, 2008.

[39] İ.N. Bozkurt, K. Kaya, A.A. Selçuk, Secret Sharing for General Access Structures, *4th Inter. Inf. Sec. and Crypt. Conf.*, Ankara, Turkey, 2010.

[40] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro, On the size of shares of secret sharing schemes, *J. of Cryptology*, 6, pp. 157-168, 1993.

[41] M. Naor, A. Wool, Access Control and Signatures via Quorum Secret Sharing, *IEEE Transactions on Parallel and Distributed Systems*, vol. 9,9, pp. 909-922, 1998.

[42] M. Naor and A. Shamir, Visual Cryptography, *Advances in Cryptology, Eurpocrypt'94*, Springer-Verlag, Berlin, pp.1-12, 1995.

[43] C. Blundo, A.D. Santis and M. Naor, Visual Cryptography for grey level images, *Information Processing Letters*, 75, pp. 255-259, 2000.

[44] Y.C. Hou, Visual cryptography for color images, *Pattern Recognition*, 36, pp. 1619-1629, 2003.

[45] C.C. Thien and J.C. Lin, Secret image sharing, *Computers & Graphics*, 26, pp. 765-770, 2002.

[46] C.C. Thien and J.C. Lin, An image-sharing method with user-friendly shadow images, *IEEE Transactions on Circuits and Systems for Video Technology*, 12(13), pp. 1161-1169, 2003.

[47] W.P. Fang, Friendly progressive visual secret sharing, *Pattern Recognition* 41(4), 1410-1414, 2008.

[48] C.C. Chen and Y.W. Chien, Sharing Numerous Images Secretly with Reduced Possessing Load, *Fundamenta Informatiace*, 86, pp. 447-458, 2008.

[49] Y.S. Wu, C.C. Thien and J.C. Lin, Sharing and hiding secret images with size constraint, *Pattern Recognition*, 37(7), pp. 1377-1385, 2004.

[50] C.C. Chen and W.Y. Fu, A Geometry-Based Secret Image Sharing Approach, *J. of Info. Science and Eng.*, 24, pp. 1567-1577, 2008.

[51] W.P. Fang, Friendly progressive visual secret sharing, *Pattern Recognition*, 41(4), pp. 1410-1414, 2008.

[52] S.J. Shyu and Y. Chen, Threshold secret image sharing by Chinese Remainder Theorem, *Proc. of the IEEE Asia-Pacific Services Computing Conf.*, 2008

[53] M. Ulutaş, V. Nabiyev and G. Ulutaş, A new secret image sharing technique based on Asmuth Bloom's scheme, *Proc. of IEEE Appl. of Information and Communication Technologies*, 2009.

[54] M. Mignotte, How to share a secret, *Proc. of the Workshop on Cryptography Burg Feuerstein'82*, v.149 LNCS, pp. 371-375, Springer-Verlag, 1983.

[55] C. Asmuth and J. Bloom, A modular approach to key safeguarding, *IEEE Trans. Information Theory*, 29(2), pp. 208-210, 1983.

[56] B. Schoenmakers, A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting, *Adv. in Cryptology, CRYPTO'99*, v.1666 LNCS, Springer-Verlag, pp .148-164, 1999.

[57] A. DeSantis, Y. Desmedt, Y. Frankel, M. Yung, How to share a function securely, *STOC'94*, 522-533, 1994.

[58] Y. Desmedt, Society and group oriented cryptography: an new concept, *Advances in Cryptography, CRYPTO '87*, Springer-Verlag LNCS 293, pp. 120-127, 1987.

[59] Y. Desmedt and Y. Frankel. Threshold CryptoSystems. *Advances in Cryptography, CRYPTO'89*, Springer-Verlag LNCS 435, pp. 307-315, 1989.

[60] T. Pederson, A threshold crypto-system without a trusted dealer, *Advances in Cryptology, EUROCRYPT '91*, Springer-Verlag LNCS 547, pp. 522-526, 1991.

[61] I. N. Bozkurt, K. Kaya, A. A. Selçuk, Practical Threshold Signatures with Linear Secret Sharing, *Africacrypt'09*, LNCS, Springer-Verlag, 2009.

[62] I. N. Bozkurt, K. Kaya, A. A. Selçuk, A. M. Guloğlu. Threshold Cryptography Based on Blakley Secret Sharing. Information Security and Cryptology, Ankara, Turkey, December 2008.

[63] H. Chen, R. Cramer, Algebraic geometric secret sharing schemes and secure multiparty computation over small fields, *CRYPTO'06*, LNCS 4117, pp. 516-531. Springer, Heidelberg, 2006

[64] H. Chen, R. Cramer, R. de Haan, I. Cascudo Pueyo, Strongly Multiplicative Ramp Schemes from High Degree Rational Points on Curves, *Eurocrypt'08*, LNCS 4965, pp. 451-470, 2008.

[65] M. Iwamoto, H. Yamamoto, Strongly secure ramp secret sharing schemes for general access structures, Hirosuke Yamamoto, *Information Processing Letters*, 97(2), 2006.

[66] G.R. Blakley and C. Meadows, Security of ramp schemes, *Advances in Cryptology-Crypto'84*, LNCS, Vol.196, pp. 242-268, 1984.

[67] Iftene, S., A generalization of Mignotte's secret sharing scheme. *Proceedings of the 6th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pp. 196-201.

[68] S. Iftene, M. Grindei, Weighted Threshold RSA Based on the Chinese Remainder Theorem, *Symbolic and Numeric Algorithms for Scientific Computing* SYNASC 2007, pp. 175-181, 2007

[69] S. Iftene, General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting, *Electronic Notes in Theoretical Computer Science (ENTCS)*, 186, pp. 67-84, 2007.

[70] S. Iftene, S. Ciobaca and M. Grindei, Compartmented Threshold RSA Based on the Chinese Remainder Theorem, *Cryptology ePrint Archive*: 2008/370.

[71] M. Tompa and H. Woll, How to share a secret with cheaters, *J. of Cryptology*, 1, pp. 133-138, 1988.

[72] R. J Mceliece, D. V. Sarwate, On sharing secrets and Reed-Solomon codes, *Communications of the ACM*, 24(9), pp. 583-584, 1981.

[73] R. Cramer, Y. Dodis, S. Fehr, C. Padró, D. Wichs, Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors, *Eurocrypt'08*, LNCS 4965, pp. 471-488, 2008.

[74] Joan Cooper, Secret sharing schemes arising from latin squares, *Bulletin of the ICA*, v. 12, pp. 33-43, 1994.

[75] T.B. Pedersen, Y. Saygın, E.Savaş, Secret sharing vs. encryption based techniques for privacy-preserving data mining, *Joint UNECE/Eurostat work session on statistical data confidentiality*, United Kingdom, pp. 17-19, 2007.

[76] K. Kulesza, Z. Kotulski, Secret sharing for n-colorable graphs with application to public key cryptography, *Proc. of 5th NATO Conference on Military Communication and Information Systems'03,Capturing New CIS Technologies*, Zegrze, 2003.

[77] H.L. Nguyen, RSA Threshold Cryptography, *Thesis*, Dept. of Computer Science, Univ. of Bristol, 2005.

[78] C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, Graph Decompositions and Secret Sharing Schemes, *J. of Cryptology*, 8 (1995), 39 - 64. Preliminary version appeared in LNCS, 658, pp. 1-24, 1993.

[79] K.M. Martin, New secret sharing schemes from old, *J. Comb. Math. Comb. Comp.*, 14, pp. 65-77, 1993.

[80] K.M. Martin, Discrete Structures in the Theory of Secret Sharing, *PhD Thesis*, University of London, 1991.

[81] D.R. Stinson, New general lower bounds on the information rate of secret sharing schemes, *LNCS*, 740, pp. 170-184, 1993.

[82] D.R. Stinson, Decomposition Construction for Secret Sharing Schemes, *IEEE Transactions on Information Theory*, 40, pp. 118-125, 1994.

[83] L. Harn and C. Lin, Detection and identification of cheaters in (t, n) secret sharing scheme, *Des. Codes Cryptogr.*, 52, pp. 15-24, 2009.

[84] Ogata, K Kurosawa, DR Stinson, H Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, *Discrete Mathematics*, vol. 279, Issues 1-3, 28, pp. 383-405, 2004.

[85] Y. P. Deng, L. F. Guo, M. L. Liu, Constructions for Anonymous Secret Sharing Schemes Using Combinatorial Designs, *Acta Mathematicae Applicatae Sinica, English Series*, vol. 23, no. 1, pp. 67-78, 2007.

[86] A. Beimel, Y. Ishai, On the Power of Nonlinear Secret-Sharing, *SIAM Journal on Discrete Mathematics*, vol. 19, issue 1, pp. 258-280, 2005.

[87] Brickell and Davenport, On the Classification of Ideal Secret Sharing Schemes, *J. of Cryptology*, 4, pp. 123-134, 1991.

[88] A. Braeken, V. Nikov, S. Nikova, Error-Set Codes and Related Objects, COCOON 2005, LNCS 3595, pp. 577-585, 2005.

[89] J. He, E. Dawson, Multistage secret sharing based on one-way function, *Electronics Letters*, 30 (19), pp. 1591-1592, 1994.

[90] Y.J. Geng, X.H. Fan, F. Hong, A new multi-secret sharing scheme with multi-policy, *The 9th International Conf. on Advanced Communication Technology*, vol. 3, pp. 1515-1517, 2007.

[91] H. Y. Lin and Y. S. Yeh, Dynamic Multi-Secret Sharing Scheme, *Int. J. Contemp. Math. Sciences*, vol. 3, no. 1, 37 - 42, 2008.

VITA

Kerem Kaşkaloğlu received the B.Sc. degree in Mathematics in 2002 and M.Sc. degree in Cryptography from the Institute of Applied Mathematics in 2004 from Middle East Technical University (METU), in Ankara, Turkey. He worked in METU, at the department of Mathematics, as a research assistant between 2002 and 2004. He has been working as an instructor in Atılım University since 2005. His research interests are coding theory, combinatorial designs, efficient arithmetic on finite fields, cryptographic protocols and secret sharing.

Publications

1. K. Kaşkaloğlu, K. Kaya, A. A. Selçuk, "Threshold Broadcast Encryption With Reduced Complexity", *The 22nd International Symposium on Computer and Information Sciences (ISCIS 2007)*, Ankara, Turkey, 2007.

2. K. Kaşkaloğlu and F. Özbudak, "On Hierarchical Threshold Access Structures", *Information Assurance and Cyber Defense (IST-091)*, Antalya, Turkey, 2010.

3. K. Kaşkaloğlu and F. Özbudak, "Some Generalized Multipartite Access Structures, A non-ideal Approach", *4th Inter. Inf. Sec. and Crypt. Conf.* (ISCTURKEY'10), Ankara, Turkey, 2010.

4. K. Kaşkaloğlu and F. Özbudak, "Nested Multipartite Secret Sharing via Multivariate Interpolation", *(to be submitted)*.