Generalized secret sharing

by

Alexander Dibert

Submitted to

Central European University

Department of Mathematics and its Applications

In partial fulfulment of the requirements for the degree of

Master of Science

Supervisor: Professor László Csirmaz

Budapest, Hungary

2011

Table of Contents

Chapter 1

Introduction

1.1 History

Since its inception, cryptology has been dealing with the problem of sending a secret message to a receiver in such a way that an eavesdropper, who can possibly intercept the communication, does not understand what the original message(plain text) is. The methods used in cryptology have been changing along with technological progress. Julius Caesar is believed to have encrypted his messages with so called *"Caesar cipher"*, simple substitution cipher [19], whereby each letter is replaced by the third-next. At the beginning of the 20^{th} century mechanical devices became sufficiently advanced to be used for the purposes of cryptology. The best known among them is Enigma, the electro-mechanical rotor machine which was used by Germany in World War II. For an overview of cryptology of that period see [13].

Modern cryptology begins with the paper *"Communication Theory of Secrecy Systems"* [21] published by Claude Shannon in 1945 for the Bell lab, in which he discussed the subject from a mathematical point of view. This work was classified and a few papers were published before 1970s. The next breakthrough was made in 1976 by Whitfield Diffie and Martin Hellman in their paper "New Directions in Cryptography" [6], where they suggested means to distribute privately cryptographic keys via public communication channels, the algorithm known as *"Diffie-Hellman key exchange protocol"*. This article gave an impulse to developments in different areas of cryptology. Among them, probably one of the most important is so called *asymmetric key algorithms*, when two different keys are used to encrypt and decrypt the message.

At the same time it was noticed that some problems involve not just a sender, a receiver and a possible eavesdropper, but a group of participants(players). For example, some company might want its managers to be able to sign documents, while it is not desirable to give the signing key to all of them. The solution to this problem could be the *sharing* of the signing key among managers in a way that a qualified set of them is able to reconstruct the key and sign documents, while an unqualified is not. Another example of the same situation is the Root DNS key protection [11]. This solution is called *secret sharing.*

Secret sharing could be used as part of the solution to a problem which seems to be different, namely to *multi-party computation* problem. An example of such problem is the famous *Yao's millionaire problem*[24], when a group of millionaires wants to determine who is the richest among them without revealing how much money each of them has. More generally, in *multi-party computation*(MPC) problem a group of players wants to compute a function on their inputs while preserving these inputs' privacy.

We will discuss *secret sharing* and its applications to MPC in the following sections.

1.2 Secret sharing

Secret sharing was first introduced by Adi Shamir [20] and George Blakley [3] independently in 1979 as one possible way of protecting data from leaking. Informally it allows a so called dealer to distribute the secret among the other participants of the protocol in a way that qualified sets of players can reconstruct it, while unqualified sets get no information about it. Both schemes by Shamir and Blakley are so called *threshold* schemes, when the set of players is qualified if and only if it is big enough. If k over n players are required, then the scheme is called (k, n)*-threshold scheme*.

The set of *participants*, who receive a share will be denoted by P. We always assume that P is not empty, and to avoid certain trivialities, we assume further that is has at least two members. During this thesis we allow P to be infinite as well; for the time being the reader may assume that P is finite. Certain subsets of participants who are expected to recover the secret, are called *qualified* sets of players, while all the other subsets are called *unqualified*. The collection of *qualified* subsets is $\mathcal{A} \subset 2^P$.

Definition 1.1. *Let P, $|P| = n$ be a set of players and $\mathcal{A} \subseteq 2^P$ - the set of qualified subsets of players. $\mathcal{A}$ is called an access structure if it satisfies the following conditions:*

1. *(Monotonicity) If $A \in \mathcal{A}$ and $A \subset A' \subseteq P$, then $A' \in \mathcal{A}$. Intuitively, if a set is allowed to recover the secret, then adding further members to this set should not take away this property.*

2. *(Non-triviality) There is at least one qualified set (and thus $P \in \mathcal{A}$), furthermore no singleton set is in $\mathcal{A}$ (in particular, the empty set is never qualified).*

Here we will give a definition of *perfect secret sharing scheme(PSSS)* in case when the set of possible secrets to be shared is finite.

Definition 1.2. *Let S_0 be a finite set of secrets s_0 with some distribution on it and for $i \in P$ let S_i be a set of shares s_i which could belong to i^{th} player. Perfect secret sharing scheme(PSSS) is a probability mapping from the set of secrets S_0 to the product set of shares $\prod_{i=1}^{n} S_i$ such that:*

1. *(Correctness) If a set of players A is qualified, then they can reconstruct the secret:*

$$\forall A = \{a_1, \ldots, a_{|A|}\} \in \mathcal{A} : \; \exists f_A(x_1, \ldots, x_{|A|}) \; s.t. \; f_A(s_{a_1}, \ldots, s_{a_{|A|}}) = s_0$$

2. *(Security) If a set of players A is unqualified, then the secret s is independent from the set of shares which belongs to players in A.*

Remark 1.1. *In case of finite set of players we can equally define a PSSS as a distribution on the product space of secrets and shares $\prod_{i=0}^{|P|} S_i$.*

Here we supposed the set of secrets to be finite, but later we will allow it to have bigger cardinality. Sometimes (although not necessarily) some of domains S_i can be equipped with an algebraic structure. The basic and one of the most elegant examples of *secret sharing* scheme is *Shamir secret sharing scheme* [20].

Let $P = \{1, \ldots, n\}$, $\mathcal{A} = \{A \subseteq P | \, |A| \geq k\}$ for some fixed k, let S_0 be some finite field F, $|F| > n$ with uniform distribution on it and S_i be equal to F for $i =\in P$.

Scheme 1.1.

1. *Let $F_s^{k-1}[x] \subset F[x]$ be the set of polynomials of degree $k-1$ with coefficients from F and the constant term equal to the secret s_0. $f(x) \in F_s^{k-1}[x]$ is picked up uniformly from $F_s^{k-1}[x]$.*

2. *The share of the i^{th} player is the value of the polynomial $f(x)$ in a point a_i, where*

all a_i are distinct, non zero and known by every player.

$$s_i = f(a_i)$$

To reconstruct the secret, a qualified set of players simply has to reconstruct the polynomial using any type of interpolation and take its constant term. It's easy to see that if the set of players is unqualified, then the set of shares is independent from the secret. Indeed, suppose $t-1$ points (a_i, s_i), $i \leq t-1$, are known by the players. These points together with $(0, s_0)$ point determine the polynomial, which means that there is a bijection between the set of polynomials and the set of secrets. Which means that from the players' point of view the secret has the same distribution as the polynomial chosen by the dealer.

As mentioned above this is an (n, k)-*threshold scheme*, while this restriction is not necessary. Ito, Saito and Nishizeki in [14] presented a generalization of the Shamir scheme which allows to share a secret for any *access structure*. Benaloh and Leichter in [2] showed how to construct a secret sharing scheme using a monotone function and an (n, n)-threshold scheme for any given *access structure*.

Shamir scheme requires the set of secrets S_0 to be a field. A huge research for possibility of *secret sharing*(as well as *MPC*) over a ring or an Abelian group was done during past fifteen years. See for example [8]. In this thesis we discus the *secret sharing* over more general structures, particularly for countable and continuum domains, as well as for infinite number of players.

If we allow players not only to collect information but to be corrupted by an adversary and misbehave in arbitrary way or even ignore the communication, we will face a so called *verifiable secret sharing (VSS)* problem. Informally it can be defined as follows:

Definition 1.3. *VSS is a protocol between the dealer and players, part of whom can be corrupted by an adversary, such that:*

- *If the dealer is honest, then he can distribute the secret in a way that qualified(honest) sets of players can reconstruct the secret independently from the corrupted players' behavior, while adversary doesn't get any information about the secret.*
- *If the dealer is corrupted(and thus the secret is already known by the adversary), then either honest players understand it and escape the protocol or some value is distributed and can be reconstructed by honest players.*

For an overview of VSS see [5] and [9].

1.3 Applications to other cryptographic protocols

There are two main applications of secret sharing: *Multi-party computation* [24] and *Zero-Knowledge Proofs*[18].

The problem of MPC is to enable a set of players to evaluate some type of functions on their private inputs. The correctness of the obtained value should be guaranteed, as well as the privacy of the inputs. Depending on a model, some sets of players can only collect information in an attempt to break the privacy of other players or be corrupted and misbehave in arbitrary way. For an overview see [10].

Here we present a simple example which shows how *secret sharing* schemes could be used as a building block in a construction of an *MPC* protocol.

The first useful observation is that any function over finite set F can be represented as a polynomial, which means that it is enough to be able to add and multiply values from F.

Now suppose that we have a *secret sharing* scheme such that if players have shares for two different secrets s and s', they can securely(without revealing any information) compute shares for $s + s'$ and $s \cdot s'$. To see how Shamir scheme can be modified to be such a scheme and required conditions on an *access structure* see [5]. Also suppose that players can not be corrupted and they follow the protocol correctly. The function is presented as a circuit with two operations: addition and multiplication. The algorithm is as follows:

1. Each player distributes his secret value among all players(including himself) using the secret sharing scheme.
2. Players evaluate the circuit step by step repeating the following operations:
   - If the next step is multiplication of two shared values, the multiplication protocol of the secret sharing scheme starts and each player obtains a share for the product.
   - If the next step is addition of two shared values, the addition protocol of the secret sharing scheme starts and each player obtains a share for the sum.
3. When shares for the final value are obtained, the reconstruction protocol of secret sharing scheme starts.

If the set of players is unqualified, they do not have at least one share for each intermediate value and thus the privacy is guarantied by security of the *secret sharing* scheme.

Zero-knowledge proofs were introduced by Goldwasser, Micali and Rackoff in [18]. In this protocol we have two entities, Prover and Verifier, and a language L. Prover tries to convince Verifier that some element l belongs to L. It is required that:

1. If $l \in L$, Prover should be able to convince honest Verifier of this fact.
2. If $l \notin L$, no cheating Prover can convince honest Verifier with probability greater then $\frac{1}{2}$.
3. If $l \in L$, no cheating Verifier gets any information except this fact.

For an example of how *secret sharing* can be used in ZKP see [1].

1.4 Thesis structure and contribution

This thesis is organized as follows. In chapter 2 we present a definition of secret sharing over countable domains suggested by Chor and Kushilevits [4], then we present our negative result, which is slightly more general than the result by Chor and Kushilevits. Finally, we show several counterexamples which demonstrate an importance of different conditions of our theorem. In chapter 3 we discuss possible definitions of continuum secret sharing and show by a counterintuitive example that the definition by Chor and Kushilevitz [4] should be modified to fit an intuitive idea of *secret sharing.* Later we present the result by Chor and Cushilevitz which shows the existence of *perfect secret sharing* over the real line. We also give a short introduction to the theory of *Lebesgue-Rokhlin probability spaces* [17] and suggest how it can be used for secret sharing over more general secret domains. In chapter 4 we present a nice scheme which allows to share a branch of possibly infinite binary tree. In our scheme several primitives could be computed by players locally without any communication. Finally, in chapter 5 we introduce a new concept of *Perfect uniform non-probabilistic secret sharing* in which we totally avoid the usage of probability. We show an existence of such scheme for arbitrary(infinite) access structure and arbitrary secret domain.

Chapter 2

Countable set of secrets

Secret sharing started with two schemes which are appropriate for a secret chosen from a finite field. A lot of work was done to investigate the possibility of secret sharing over other types of domains. For instance, it is desirable to be able to share a secret from less restrictive algebraic structures such as finite ring or an Abelian group. So called black-box secret sharing schemes allow to share a secret from arbitrary finite field(ring, Abelian group)[8]. Nevertheless, most of this work is done for finite case, while infinite structures are poorly understood. The main result for the infinite secret domains is by Chor and Kushilevitz [4]. We think that research in infinite secret sharing could help to construct efficient schemes for finite case and understand the nature of the secret itself. In this chapter we suppose the set of participants to be finite.

When we want to leave finiteness the first step is to deal with countable sets. In this chapter we revisit the classical result of Chor and Kushilevitz [4]. Roughly speaking it states that a secret sharing scheme which distributes infinitely many secrets cannot have atomic shares. A share is *atomic* if one of its values is received with positive probability. One consequence of the Chor–Kushilevitz theorem is that no perfect secret sharing scheme exists on countably many secrets and shares, i.e. when all the sets S_0 and S_i are countable.

2.1 Definition

When the set of possible secrets is finite we usually have a discrete probability measure on it. Chor and Kushilevitz in [4] suggest a different approach to secret sharing in infinite case and renounce the usage of distribution on the set of secrets. Instead, they look on the secret s_0 as on a given value which has to be shared, and the dealer picks up shares according to a corresponding distribution P_{s_0}. In case of countable set of secrets they use the following definition[4]:

Definition 2.1. *Let S_0 be a countable set of possible secrets, let $\mathcal{A}$ be an access structure on a set of n players, and $\alpha \geq 1$ be a constant. An $(\mathcal{A}, \alpha)$ secret sharing scheme over S_0 is a probabilistic mapping $\Pi : S_0 \to S = \prod\limits_{i \in P} S_i$ from the set of secrets to the set of n-tuples (shares) such that:*

1. *(Correctness) If a set of players A is qualified, then the secret can be reconstructed. That is, for any subset $A \in \mathcal{A}$ there exists a function $f_A : \prod_{i \in A} S_i \to S_0$ such that, for every possible set of shares $(s_1, \ldots, s_n) = \Pi(s_0)$, the secret can be found by $f_A(\{s_i\}_{i \in A}) = s_0$.*

2. *(Security) No unqualified set of shares reveals "too much" partial information about the secret. Formally, for any $A \notin \mathcal{A}$, for every two values of the secret a_1, $a_2 \in S_0$ and for every possible shares $\{s_i\}_{i \in A}$:*

$$\frac{1}{\alpha} \cdot Pr(\{s_i\}_{i \in A} | s_0 = a_1) \leq Pr(\{s_i\}_{i \in A} | s_0 = a_2) \leq \alpha \cdot Pr(\{s_i\}_{i \in A} | s_0 = a_1)$$

In the definition above the parameter α tells us what "too much information" is. If $\alpha = 1$, then the scheme is a perfect secret sharing scheme.

We will use a less restrictive definition. Namely, we do not require α to be unique for all unqualified sets of players and we replace the property 2 by the following:

$2'$ *(Security) For every $A \notin \mathcal{A}$ there exists a positive constant $\alpha_A \geq 1$, such that for every two values of the secret a_1, $a_2 \in S_0$ and for every possible shares $\{s_i\}_{i\in A}$:*

$$\frac{1}{\alpha_A} \cdot Pr(\{s_i\}_{i\in A}|s_0 = a_1) \leq Pr(\{s_i\}_{i\in A}|s_0 = a_2) \leq \alpha_A \cdot Pr(\{s_i\}_{i\in A}|s_0 = a_1)$$

We call such schemes *closely perfect secret sharing schemes.*

2.2 Impossibility of countable secret sharing

In the same paper Chor and Kushilevitz showed that if we require the set of possible shares to be countable as well, then there is no secret sharing scheme scheme. The proof of this statement is based on impossibility of uniform distribution on a countable set. In chapter 5 we will particularly show that such schemes exist in *non-probabilistic secret sharing*, when we completely avoid the probability. We show that almost the same proof as the one by Chor and Kushilevitz works for *closely perfect secret sharing schemes.*

Theorem 2.1. *If we consider a set of possible shares S_i to be countable for every player $i \in P$, then there is no closely perfect secret sharing scheme(independently from a chosen access structure $\mathcal{A}$).*

Proof. First we will show that it is enough to consider just two players, provided that both are required to reconstruct the secret.

Lemma 2.1. *If there exists a scheme F_n for an access structure $\mathcal{A}$ on n players and a secret s_0 picked up from a set S_0, then there exists a scheme F_2 for just two participants when both are required to reconstruct the secret and a secret is picked up from the same set S_0.*

Proof. Let A be any minimal qualified set of players, $\emptyset \neq A_1 \subsetneq A$ and $\emptyset \neq A_2 = A - A_1$(here we suppose that no player can reconstruct the secret alone, otherwise he can simply be excluded from the scheme). Clearly, both A_1 and A_2 are unqualified. First the new scheme F_2 runs the scheme F_n, then the first player gets all shares which in scheme F_n belong to players in A_1 $(s_i,\ i \in A_1)$ and the second player gets shares from A_2 $(s_i,\ i \in A_2)$. $A_1 \cup A_2 = A$ and A is qualified, thus two players can reconstruct the secret together. On the other hand, from scheme F_n(and from $A_1 \notin \mathcal{A}$) we have that for every two values of the secret $a_1,\ a_2 \in S_0$:

$$\frac{1}{\alpha_{A_1}} \cdot Pr(\{s_i\}_{i \in A_1} | s_0 = a_1) \leq Pr(\{s_i\}_{i \in A_1} | s_0 = a_2) \leq \alpha_{A_1} \cdot Pr(\{s_i\}_{i \in A_1} | s_0 = a_1)$$

It implies that the first player does not have "too much information" about the secret. The same holds for A_2 and the second player, and it ends the proof. □

Now it is enough to prove the theorem for two players. Suppose, such scheme exists and let $f(x_1, x_2)$ be a function which reconstructs the secret according to two given shares. For every value of the secret s_0 and pair of shares s_1, s_2 we have a probability that secret s_0 will be distributed as s_1 and s_2. We will denote it $Pr(s_1, s_2 | s_0)$. This probability satisfies the following conditions:

1. If $f(s_1, s_2) \neq s_0$ then $Pr(s_1, s_2 | s_0) = 0$. This means that the function f gives the right value.

2. For any secrets $s_0,\ s_0' \in S_0$ and share $s_1 \in S_1$:

$$Pr(s_1 | s_0) = \sum_{s_2 \in S_2} Pr(s_1, s_2 | s_0) \leq \sum_{s_2 \in S_2} \alpha_1 \cdot Pr(s_1, s_2 | s_0') = \alpha_1 \cdot Pr(s_1 | s_0')$$

3. For any secrets $s_0,\ s'_0 \in S_0$ and share $s_2 \in S_2$:

$$Pr(s_2|s_0) = \sum_{s_1 \in S_1} Pr(s_1, s_2|s_0) \leq \sum_{s_1 \in S_1} \alpha_2 \cdot Pr(s_1, s_2|s'_0) = \alpha_2 \cdot Pr(s_2|s'_0)$$

For any fixed secret s'_0 there exists a pair of shares (s'_1, s'_2) such that $Pr(s'_1, s'_2|s'_0) > 0$ (otherwise by σ-additivity of the probability measure Pr the total probability will be zero, and hence the secret s'_0 could not be shared). Let $\epsilon = Pr(s'_1|s'_0)$ and let $S_2^{s_0} \subset S_2$ be the set of shares s_2 such that $f(s'_1, s_2) = s'_0$, then:

$$\sum_{s_2 \in S_2^{s_0}} Pr(s_2|s_0) = \sum_{s_2 \in S_2^{s_0}} \sum_{s_1 \in S_1} Pr(s_1, s_2|s_0) \geq \sum_{s_2 \in S_2^{s_0}} Pr(s'_1, s_2|s_0) = Pr(s'_1|s_0) \geq \frac{\epsilon}{\alpha_1}$$

The last inequality is by (2). Now note that sets $S_2^{s_0}$ are disjoint and $\bigcup_{s_0 \in S_0} S_2^{s_0} = S_2$. Thus by σ-additivity:

$$1 = \sum_{s_2 \in S_2} Pr(s_2|s'_0) = \sum_{s_0 \in S_0} \sum_{s_2 \in S_2^{s_0}} Pr(s_2|s'_0) \geq \sum_{s_0 \in S_0} \sum_{s_2 \in S_2^{s_0}} \frac{1}{\alpha_2} \cdot Pr(s_2|s_0) =$$

$$\sum_{s_0 \in S_0} \frac{1}{\alpha_2} \sum_{s_2 \in S_2^{s_0}} Pr(s_2|s_0) \geq \sum_{s_0 \in S_0} \frac{\epsilon}{\alpha_1 \cdot \alpha_2} = \infty$$

This gives a contradiction. □

The theorem is interesting by itself and as a consequence we get an important corollary:

Corollary 2.1. *Suppose that a closely perfect secret sharing scheme distributes a secret from an infinite domain. Then some participant $i \in P$ must have more than countably many possible shares.*

Proof. If the set of secrets S_0 is infinite, then it can be restricted to a countable set(the dealer can simply forget about other values). Now if we suppose that every player gets a share from a countable set, then it fits the conditions of theorem 2.1, which says that such scheme does not exist. □

2.3 Counterexamples

In this section we show the importance of conditions in theorem 2.1 and corollary 2.1 by providing some counterexamples.

In contrast to the corollary 2.1, if we allow at least one player to have a share from a continuum set, then such scheme exists.

In this example there are only two participants, a and b. The set S_0 of the secrets is $\mathbb{Z}$, the set of all integers (positive and negative). The share of a is a uniformly distributed random real from the $[0, 1]$ interval. The share of b is an element of $\mathbb{Z}$, such that $j \in \mathbb{Z}$ is chosen with probability $p_j > 0$, where $\sum_{j\in\mathbb{Z}} p_j = 1$.

Scheme 2.1. *First we split* $[0, 1]$ *into countably many disjoint sets indexed by* $\mathbb{Z}$ *as*

$$[0,1] = \bigcup_{k\in\mathbb{Z}}^{*} E_k$$

so that each E_k *has an outer measure* 1.

Suppose that the share of a *is* $\alpha \in [0, 1]$*, and the share of* b *is* $\beta \in \mathbb{Z}$*. Then the secret is* $k + \beta \in \mathbb{Z}$*, where* $k \in \mathbb{Z}$ *is the index of the part of the unit interval in which* α *is.*

In the access structure a and b are unqualified, but $\{a, b\}$ is qualified. It is clear that a and b together can determine the secret. Given any secret $s_0 \in \mathbb{Z}$, the share of the first player a is distributed uniformly on zero-one interval, and the share of the second player has a discrete distribution on $\mathbb{Z}$ where the probability of j is p_j. Hence this is a perfect secret sharing scheme.

Remember that in this chapter we suppose that the set of players is finite. To show the importance of this assumption we provide the following example:

In this scheme participants are indexed by positive natural numbers and an access structure consists of all infinite sets of players. The set of secrets S_0 is $\mathbb{N}^+$ the set of positive natural numbers and each S_i is finite.

Scheme 2.2. *The dealer chooses the secret $s_0 \geq 1$, say with probability $\frac{1}{2^s}$ and a threshold $t > s_0$, so that t is chosen with probability $\frac{1}{2^{t-s_0}}$. Then he computes the share of participant j as follows: If $j < t$ then j's share is a random number between 1 and j (chosen with equal probability). If $j \geq t$, then j's share is s_0.*

We claim that this is a *closely perfect secret sharing scheme.*

Proof. Condition 1 of Definition 2.1 is immediate. If $A \in \mathcal{A}$ then members of A can recover the secret as the limit of their shares.

To check condition $2'$ we first notice that the participant j gets his share from the set $S_j = \{1, \ldots, j\}$. If the secret is $s_0 \geq j$, then j receives every value with probability $\frac{1}{j}$. If $s_0 < j$, then with probability $1/2^{j-s_0}$ the threshold is bigger then j. This implies that j gets every value with probability at least $j^{-1} \cdot 2^{-(j-s_0)}$.

Next, we consider the joint distribution of shares of the first b participants. Denoting $\{1, \ldots, b\}$ by $[b]$, the shares are elements of $S_{[b]} = \prod_{j \in [b]} S_j$. If the secret s_0 is at least b, then every element of $S_{[b]}$ is equally probable (as shares are chosen uniformly and randomly). If the b^{th} share is chosen uniformly(which means that $j < t$), then all smaller shares $1, \ldots, b-1$ are chosen uniformly as well, hence if $s_0 < b$, then with probability at least $2^{-(b-s_0)}$ every share up to b is chosen uniformly. It means that choosing any particular element from $S_{[b]}$ has probability at least $c_b = |S_B|^{-1} \cdot 2^{-(b-s_0)}$ and at most 1, independently of the value of the secret. Therefore for any $s \in S_{[b]}$ and secrets s_0 and s_0',

$$c_b \cdot Pr(s|s_0) \leq Pr(s|s_0') \leq \frac{1}{c_b} \cdot Pr(s|s_0) \tag{2.1}$$

Now let $A \notin \mathcal{A}$ be an unqualified set of players. Then A is finite and consequently $A \subseteq [b]$ for some natural number b. Then by (2.1) property 2' of definition 2.1 is satisfied.

□

It is easy to see that the example above does not work for the "classical" definition 2.1 by Chor and Kushilevitz, as the constants c_b are different and tend to zero.

Chapter 3

Continuum set of secrets

3.1 Definition

It appears that it is not an easy question what is an appropriate definition of *secret sharing* in case of continuum set of secrets. In this section we show that the idea to apply the same definition 1.2, as in finite case, in some sense fails, as well as the definition suggested by Chor and Kushilevitz [4]. Also, we suggest a modification of definition 1.2 to be used for continuum *perfect secret sharing.*

It is a trivial idea to apply the definition of finite perfect secret sharing to infinite case, namely:

Definition 3.1. *Let S_0 be an infinite set of secrets s_0 with some sigma-algebra and probability measure on it, and for $i \in P$ let S_i be the set of shares s_i which could belong to i^{th} player. Perfect secret sharing scheme(PSSS) is a probability mapping from the set of secrets S_0 to the product set of shares $\prod_{i=1}^{n} S_i$ such that:*

1. *(Correctness) If the set of players A is qualified, then they can reconstruct the secret:*

$$\forall A = \{a_1, \dots, a_{|A|}\} \in \mathcal{A} : \; \exists f_A(x_1, \dots, x_{|A|}) \; s.t. \; f_A(s_{a_1}, \dots, s_{a_{|A|}}) = s_0$$

2. *(Privacy) If the set of players A is unqualified, then the secret s is independent from the set of shares which belongs to players in A.*

Unfortunately, this definition fails. In finite case independence of set of shares from the secret implies that, knowing them, one can not reconstruct the value of the secret(which is a natural requirement for the secret sharing), while this does not hold in general for a secret distributed continuously. The reason for this is a complex behavior of not measurable functions.

We show an example for a scheme which satisfies definition 3.1, while an unqualified set of players still can reconstruct the correct value of the secret. The idea which is used in this scheme is by G. Tardos [22].

Let the set of players consist of just two entities, and both are required to reconstruct the secret. The secret and first player's domains are zero-one intervals, while a share of the second player is always equal to 1. Finally, let the secret be distributed uniformly.

$$P = \{1, 2\}, \; \mathcal{A} = \{P\}, \; S_0 = S_1 = [0, 1], \; S_2 = \{1\}, \; s_0 \in_u [0, 1]$$

Scheme 3.1. *Let $f(x)$ be a bijection of $[0, 1]$ interval, such that the outer measure of $G = \{x, f(x)\}$ is equal to 1(existence of such bijection follows from the axiom of choice). For any measurable subset of the unit square $U \subseteq [0, 1]^2$ let $Pr(U \cap G) = Pr(U)$.*

1. *To pick up the secret s_0, we first generate a point in G and take the secret equal to the value of the first coordinate of this point.*

2. *$s_1 = f(s_0)$ or, in other words, the second coordinate of the point.*

3. $s_2 = 1$

Independence of s_0 and s_2 is obvious as s_2 is a constant. The construction gives us independence between uniformly distributed s_0 and $s_1 = f(s_0)$:

$$Pr(s_0 \in U_0,\ s_1 \in U_1) = Pr((s_0, f(s_0)) \in U_0 \times U_1) = |U_0 \times U_1| = |U_0||U_1| =$$

$$Pr(s_0 \in U_0)Pr(s_1 \in U_1)$$

for any measurable $U_0, U_1 \in [0,1]$. The second requirement in definition 3.1 is satisfied. To show that the first player still can reconstruct the secret alone, observe that applying the inverse of the bijection f to his share he gets the secret: $s_0 = f^{-1}(s_1)$. We will call such definitions of secret sharing "*intuitively wrong*".

As mentioned above, existence of such an example is based on properties of unmeasurable functions. Indeed, in Scheme 3.1 function f^{-1}, which reconstructs the secret given the share of the first player, is unmeasurable. At the same time, if we require the recovery function in the definition of secret sharing scheme for continuous domain to be measurable, the definition will become "*intuitively right*".

Proof. Let A be an unqualified set of players and S be the set of shares they know, and let the secret s_0 be independent from S i.e.

$$Pr(s_0 = a, S = B) = Pr(s_0 = a)Pr(S = B)$$

for any $a \in S_0$ and $B \in \prod_{i \in A} S_i$. Suppose, there is a measurable function f_A, which given the set of shares reconstructs the secret. Then

$$Pr(s_0 = a)Pr(S = B) = Pr(s_0 = a, S = B) = Pr(f(B) = a, S = B)$$

which is equal to $Pr(S = B)$ if $f(B) = a$ and to 0 otherwise. This gives us a contradiction.

□

For continuum case in [4] Chor and Kushilevitz replace the second property in definition 2.1 of countable *secret sharing scheme* by the following:

2′ No unqualified set of shares reveals "too much" partial information about the secret. Formally, for any $A \notin \mathcal{A}$, for every two values of the secret a_1, $a_2 \in S_0$, and for any $|A|$-tuple of measurable sets $\{C_i\}$, $C_i \subset S_i$:

$$Pr(\forall i \in A: \ s_i \in C_i | \, s_0 = a_1) = Pr(\forall i \in A: \ s_i \in C_i | \, s_0 = a_2)$$

Using the same idea like in Scheme 3.1, we can show that this definition is "*intuitively wrong*".

Let the set of players consist of three entities and all of them are required to reconstruct the secret. Let the set of secrets and the sets of shares for the first and the second player be zero-one intervals, while the share of the third player is always equal to 1. Finally let the shares for the first two players be distributed uniformly for any value of the secret.

$$P = \{1,2,3\}, \ \mathcal{A} = \{P\}, \ S_i = [0,1], \ i \in 0,1,2, \ S_3 = \{1\}, \ s_1, s_2 \in_u [0,1] \ for \ all \ s_0$$

Scheme 3.2. *For any secret s_0 let $f_{s_0}(x)$ be a bijection of $[0,1]$ interval, such that the outer measure of $G_{s_0} = \{x, f_{s_0}(x)\}$ is equal to 1 and for any $s_0' \neq s_0$ $G_{s_0} \cap G_{s_0'} = \emptyset$(existence of such family of bijection follows from an axiom of choice). For any measurable subset of the unit square $U \subseteq [0,1]^2$ and any secret s_0 let $Pr(U \cap G_{s_0}) = Pr(U)$.*

1. *Given the secret s_0, we pick up a point s from G_{s_0}*

2. *The i^{th} share s_i is i^{th} coordinate of the point s, $i = 1,2$.*

3. *The 3^{rd} share is equal to* 1.

By the construction, all the shares s_i are independent and have the same uniform distribution for every value of the secret s_0. It means that the requirement $(2')$ is satisfied. Sets G_{s_0} are disjoint, which implies that three players together can reconstruct the secret(just by determining for which index the point s_0 $(s_1, s_2, 1)$ is in G_{s_0}), i.e. the first property is satisfied. In the same time it means that the first and the second players can reconstruct the secret as well, while they form an unqualified set of players. This shows us that this definition is *intuitively wrong.*

To construct this example, as well as in Scheme 3.1, we used unmeasurability. Namely, the set to which the secret is mapped is unmeasurable, while in all examples by Chor and Kushilevitz in [4] these sets are measurable.

In this thesis later on we will use corrected definition 3.1 for continuum secret sharing, namely:

Definition 3.2. *Suppose, $P = \{1, \ldots, n\}$ and $\mathcal{A}$ is some access structure on it. Let S_0 be an infinite set of secrets s_0 with some sigma-algebra and probability measure on it, and for $i = \in P$ let S_i be the set of all possible shares s_i which could belong to i^{th} player. Perfect secret sharing scheme(PSSS) is a probability mapping from the set of secrets S_0 to the product set of shares $\prod_{i=1}^{n} S_i$, such that:*

1. *(Correctness) if the set of players A is qualified, then they can reconstruct the secret using a measurable function:*

$$\forall A = \{a_1, \ldots, a_{|A|}\} \in \mathcal{A} : \exists f_A(x_1, \ldots, x_{|A|}) \; s.t. \; f_A(s_{a_1}, \ldots, s_{a_{|A|}}) = s_0$$

   Where f_A is measurable.

2. *(Security) if the set of players A is unqualified, then the secret s is independent from the union of shares which belongs to players in A.*

3.2 Existence over the real line

To show an existence of secret sharing scheme over continuum set, Chor and Kushilevitz presented [4] a (n, n)-threshold scheme for secret picked up uniformly from zero-one interval.

Let the set of players $P = \{1, \dots, n\}$, access structure $\mathcal{A} = \{P\}$. Let the set of secrets, as well as sets of shares for any player S_i, $i = 0, 1, \dots, n$ be equal to zero-one interval and let the secret s_0 be distributed uniformly.

Scheme 3.3.

1. *First $n-1$ shares s_i, $i \leq n-1$ are picked up uniformly from $[0, 1]$.*
2. *The last share $s_n = s_0 - \sum\limits_{i \leq n-1} s_i \,(mod\, 1)$*

All together n players can add up their shares modulo one and obtain the value of the secret, while if at least one of them is missed, then the secret is independent from the set of known shares.

As it was pointed out in the same paper by Chor and Kushilevitz, this scheme can be used like a building block to construct a scheme for arbitrary access structures on n players. There are three common ways to do it: using monotone functions [2], using minimal qualified sets [14], or using maximal unqualified subsets(which is in some sense a dual to the second approach) [16].We present the last one.

Theorem 3.1. *For any access structure on n players there exists a perfect secret sharing scheme over zero-one interval.*

Proof. Let $U = \{U_1, \ldots, U_k\}$ be the set of all maximal unqualified sets of players. Using scheme 3.3 for k players, the dealer distributes the secret into k shares s_i. Each of them corresponds to an element of U. For every player p if $p \notin U_i$, p gets s_i as a part of its share.

If the set of players A is qualified, then for any $U_i \in U$ there is a player p_i such that $p_i \in A$, but $p_i \notin U_i$. Thus A knows all shares s_i and can reconstruct the secret $s_0 = \sum\limits_{i \leq k} s_i \, (mod \, 1)$. If the set of players A is unqualified, then there is at least one $V \in U$, such that $A \subseteq V$. Thus players in A do not know at least one share. The rest follows from security of (n, n)-threshold scheme. □

As we mentioned in the introduction, it is important to be able to compute shares for the sum of two secrets locally. It is easy to see that this scheme gives such opportunity: to obtain a share for a sum of secrets, one simply has to add up corresponding shares.

To show the existence of perfect secret sharing over the real line with any strictly monotone continuous distribution function $\mathcal{F}$ on it, we observe that, after the secret is picked up according to this distribution, one can apply $\mathcal{F}$ to the secret and distribute it as a secret distributed uniformly on zero-one interval. To reconstruct the secret, the qualified set of players first reconstructs its image and applies $\mathcal{F}^{-1}$ to it. Security is guaranteed by ”zero-one” scheme. Namely:

Theorem 3.2. *Let $\mathcal{A}$ be any access structure on a set of n players. Let the set of secrets S_0 be a real line with distribution function $\mathcal{F}$ on it. Suppose that $\mathcal{F}$ is continuous and strictly monotone, then there is a perfect secret sharing scheme for an access structure $\mathcal{A}$ and a secret picked up from S_0.*

Proof. For secret s_0 let $s'_0 = \mathcal{F}(s_0)$. $\mathcal{F}$ is a continuous distribution function, hence s'_0 is distributed uniformly. Now one can apply a scheme for an access structure $\mathcal{A}$ and a secret distributed uniformly(such scheme exists by theorem 3.1). Let s'_i be a share which belongs to i^{th} player in the "subscheme", then $s_i = s'_i$.

1. If A is a qualified set of players, let f'_A be their reconstruction function from the "subscheme". Then $s_0 = \mathcal{F}^{-1}(f'_A(s_i,\ i \in A))$, and hence the secret can be reconstructed by A.

2. If A is unqualified, then $\{s_i,\ i \in A\}$ is independent from s'_0, and hence is independent from $s_0 = \mathcal{F}^{-1}(s'_0)$.

□

To prove a theorem for a wider class of probability spaces, we have to introduce some elements of *Lebesgue-Rokhlin probability space* theory.

3.3 Lebesgue probability space

The theory of *Lebesgue-Rokhlin probablity space*(or *Standard probability space*) was started by von Neuman [23] and Rokhlin [17] in 40s. Informally, a probability space is *Lebesgue-Rokhlin* if it is isomorphic modulo zero set to zero-one interval with Lebesgue measure on it. Most of basic probability spaces has this property[12]. If such isomorphism f exists, one can apply it to the secret and use a secret sharing scheme in zero-one interval, like it was done in theorem 3.2.

In this section we give a formal definition of *Lebesgue-Rokhlin probablity space*, like it is used in [17], and give a criterion of standardness. Finally, we state a theorem about existence of perfect secret sharing over *Lebesgue-Rokhlin probability spaces.*

Definition 3.3. *Probability space $(S, \mathcal{F}, P)$ is separable if there exists a countable set of measurable sets Γ (we will denote the set generated by them as Γ_B, all its elements are obviously measurable), such that:*

1. *For any measurable $A \subset S$ there exists a set B, $A \subset B \subset S$ such that $P(\Delta(A, B)) = 0$, where Δ is a symmetric difference, and $B \in \Gamma_B$.*

2. *For any two points $x, y \in S$ there exists a measurable set $G \in \Gamma$, such that $x \in G$, $y \notin G$ or $y \in G$, $x \notin G$.*

Such Γ is called a basis of probability space.

Now let the space be *separable* and let $\Gamma = \{G_i\}$ be its basis. Let A_i be either G_i of $\overline{G}_i$, and for any point a $\in S$ let $A_i(a)$ be that of G_i and $\overline{G}_i$ which contains a. By the second property of definition 3.3 $\bigcap\limits_{all\ i} A_i$ can not contain more than one point and hence $\bigcap\limits_{all\ i} A_i = \{a\}$

Definition 3.4. *If in notations as above all $\bigcap\limits_{all\ i} A_i$ are not empty, then the space is called complete with basis Γ.*

As it usually happens in measure theory, we are interested in definition 3.4 only modulo zero.

Definition 3.5. *Probability space $(S, \mathcal{F}, P)$ is called complete modulo 0 with basis $\Gamma = \{G_i\}$ if there exists a complete probability space $(S', \mathcal{F}', P')$ with basis $\Gamma' = \{G'_i\}$ and an embedding $E : S \to S'$, such that the image of S is measurable (i.e. $E(S) \in \mathcal{F}'$), $P'(S' - E(S)) = 0$ and $G_i = E^{-1}(G'_i)$.*

It is known that, if a space is *complete modulo* 0 with one of its basis, then it is *complete modulo* 0 with any basis. For the proof of this statement see [17] or [15]. So, we will call them just *complete modulo* 0 spaces.

Now we are ready to define a *Lebesgue-Rokhlin probability space.*

Definition 3.6. *Separable, complete modulo* 0 *probability spaces are called Lebesgue-Rokhlin spaces.*

As we are interested in using zero-one interval instead of Lebesgue-Rokhlin space in a secret sharing scheme, we need a definition of an isomorphism between probability spaces.

Definition 3.7. *Two probability spaces $(S, \mathcal{F}, P)$ and $(S', \mathcal{F}', P')$ are isomorphic(or isomorphic modulo 0) if there exist sets $A \subset S$ and $A' \subset S'$ of measure zero and an isomorphism F between $S - A$ and $S' - A'$. I.e. for any measurable $B \subseteq S - A$ $F(B)$ is measurable and $P(B) = P'(F(B))$. As well as for any measurable $B' \subseteq S' - A'$ $F^{-1}(B')$ is measurable and $P(F^{-1}(B')) = P'(B')$.*

We state the following theorem by Rokhlin and suggest [17] to the reader for a proof.

Theorem 3.3. *Suppose that a Lebesgue-Rokhlin space $(S, \mathcal{F}, P)$ has atoms $\{m_i\}$, then it is isomorphic modulo 0 to an interval of length $1 - \sum_i P(m_i)$ with Lebesgue measure on it and a set of atoms with measures $P(m_i)$(obviously this set can not be bigger than countable).*

Unfortunately, theorem 3.3 gives us isomorphism modulo 0 only. To use this theorem we have to give up the ability of qualified sets of players to reconstruct the secret picked up from some set of measure zero.

Definition 3.8. *Suppose $P = \{1, \ldots, n\}$ and $\mathcal{A}$ is some access structure on it. Let S_0 be an infinite set of secrets s_0 with some sigma-algebra and probability measure on it, and for $i \in P$ let S_i be the set of shares s_i which could belong to i^{th} player. Perfect secret sharing scheme(PSSS) is a probability mapping from the set of secrets S_0 to the product set of shares $\prod_{i=1}^n S_i$ such that:*

1. *(Correctness) If the set of players A is qualified, then with probability one they can reconstruct the secret using a measurable function:*

$$\forall A = \{a_1, \ldots, a_{|A|}\} \in \mathcal{A} : \; \exists f_A(x_1, \ldots, x_{|A|}) \; s.t. \; Pr(f_A(s_{a_1}, \ldots, s_{a_{|A|}}) = s_0) = 1$$

   Where f_A is measurable.

2. (Security) If the set of players A is unqualified, then the secret s is independent from the union of shares which belongs to players in A.

Theorem 3.4. *Let $\mathcal{A}$ be any access structure on a set of n players. Let S_0 be the set of secrets and the probability space $(S_0, \mathcal{F}, P)$ be a Lebesgue-Rokhlin probability space then there is a perfect secret sharing scheme for an access structure $\mathcal{A}$ and a secret picked up from S_0.*

Proof. By theorem 3.3 there is an isomorphism f between $S_0 - A$ and $[0,1] - B$, where A and B have corresponding measure zero. If the secret appeared to be in A, the dealer gives each player a share(or multiple shares if it is required by the corresponding zero-one scheme) distributed uniformly on zero-one interval independently from the secret. If the secret $s_0 \notin A$, then the dealer computes $s'_0 = f(s_0) \in ([0,1] - B)$, B has Lebesgue measure zero, hence s'_0 is distributed uniformly on $[0,1]$ and the dealer may use a zero-one scheme to distribute it.

With probability one the secret did not get into A, and acting like in scheme 3.3 a qualified set of players can reconstruct $s'_0 = f(s_0)$, apply the inverse of f to it(remember that f is an isomorphism) and get the real value of the secret. Hence the correctness property of definition 3.8 is satisfied. If the set of players is unqualified, then, independently from where the secret is, the shares are independent from the secret. Either because of the security of zero-one scheme, if the secret is in $S_0 - A$, or because the shares are distributed uniformly on $[0,1]$ and independent from the secret, if the secret is in A. □

It seems that the converse is true as well.

Conjecture 3.1. *Suppose that there exists a secret sharing scheme(see definition 3.8) for some access structure and a secret picked up from some probability space, then this space is Lebesgue-Rokhlin.*

We suggest this question as a possible direction for further research.

Chapter 4

Binary trees

Binary tree is an important construction as it is widely used in computer science, particularly in compression and coding theory(for example, the Fano code [7]), as well as in probability theory in order to understand the nature of randomness. We think that it is important to be able to share a branch(possibly infinite) of a rooted binary tree.

In this section we present a secret sharing scheme which shares a branch of a rooted binary tree for any access structure on finite set of players. This scheme allows players to compute several primitives securely, namely vertex-wise XOR and alternation merging of two shared branches.

Let G be a rooted binary tree. We will consider it to have all branches of equal(possibly infinite) length and identify every branch with a zero-one string $\{0,1\}^L$, where L is the length of a branch. Finally, let S_0 be the set of all G's branches.

Definition 4.1. *Let r be a zero-one string of any length $l \leq L$. A cone C_r is a set of all branches in S_0 which has r as a prefix(if $L = l = \infty$, then the cone in just one branch).*

In case of infinite branches let $\mathcal{F} \subset 2^{S_0}$ consist of all *cones* $C_r \subseteq S_0$ and their countable unions. Also, let the probability $Pr(C_r)$ be equal to $\frac{1}{2^l}$, where l is a length of a prefix r.

Claim 4.1. *$\mathcal{F}$ is a sigma-algebra.*

Proof. The claim is an easy consequence of two lemmas.

Lemma 4.1. *Let C_1 and C_2 be two cones, then $C_1 \bigcap C_2 \in \{C_1, C_2, \emptyset\}$*

Proof. Let r_1 and r_2 be prefixes of the corresponding cones. Suppose, $C_1 \bigcap C_2$ is not empty, then there exists a branch $s \in C_1 \bigcap C_2$. It means that, without loss of generality, r_1 is a prefix of r_2, and both of them are prefixes of s. If $|r_1| = |r_2|$, then the cones C_1 and C_2 are equal and hence $C_1 \bigcap C_2 = C_1 = C_2$. If $|r_1| < |r_2|$, then $C_2 \subset C_1$ and $C_1 \bigcap C_2 = C_1$ □

As a corollary of the lemma we derive that the countable intersection of elements of $\mathcal{F}$ is still in $\mathcal{F}$.

Lemma 4.2. *The complement of any cone C is in $\mathcal{F}$*

Proof. Let $\overline{C}$ be an empty set and r be an empty string(already passed part of the prefix). We will go from the root of the tree down along the prefix till its end. On every step, when we chose between x_1 and x_2, suppose we chose x_1. Then we do the following:

1. Let r' be equal to r with x_2 added in the end, then put $\overline{C} := \overline{C} \bigcup C_{r'}$

2. Put r equal to r with x_1 added in the end.

The length of the prefix is at most countable, hence $\overline{C}$ is a countable union of cones and it is easy to see that $C \bigcup \overline{C} = S_0$. □

Now, to prove that $\mathcal{F}$ is indeed a sigma-algebra, it is enough to show that the complement of any $f \in \mathcal{F}$ is in $\mathcal{F}$. For all $f \in \mathcal{F}$, $f = \bigcup_{i \in \mathbb{N}} C_i$, the countable union of cones.

$$\overline{f} = \overline{\bigcup_{i \in \mathbb{N}} C_i} = \bigcap_{i \in \mathbb{N}} \overline{C_i}$$

By lemmas 4.1 and 4.2, it is in $\mathcal{F}$ and hence $\mathcal{F}$ is a sigma-algebra.

□

Now we present a scheme for a secret from $(S_0, \mathcal{F}, Pr)$. The same idea applies for finite case. As usual, we start with an (n,n)-threshold scheme. In this scheme shares as well as a secret are branches of the tree.

Scheme 4.1. 1. *The first $n-1$ shares are picked up with the same distribution as the secret and independent from it.*

2. *The last share is taken in a way that bitwise sum modulo two of all shares is equal to the secret.*

To reconstruct the secret, n players together may add up all their shares bitwise and modulo two. First $n-1$ shares are independent from the secret by construction, hence if the last player is missed, then the set of shares known by the players is independent from the secret. Now, without loss of generality, suppose that the first player is missed. Then, for any bit of the secret b_0, suppose $\sum_{i \geq 2} b_i \ (mod\, 2) = b$, where b_i is the corresponding bit of i's share. Then

$$Pr(b_0 = j | b_i,\ i \geq 2) = Pr(XOR(b_1, b) = j)$$

And hence the conditional distribution of the secret, given shares s_i, $i \geq 2$, is the same as distribution of s_1, which by construction is distributed as the secret s_0.

This scheme can be used as a building block for a scheme working with arbitrary access structure. In fact, all solutions from [2][14][16] can be used here.

Most of results presented in this thesis work with infinity, and hence are more theoretical than practical. As it was mentioned above, scheme 4.1 can be used for finite trees as well. The restriction of equal branch length can be avoided by adding some extra vertexes with a blank symbol and replacing all modulo two operations by modulo three(to deal with a new symbol). In the following part of the section we show that several operations on secrets could be computed by players locally, without any communication, which can be useful for the practical MPC purpose.

Namely, suppose that the secrets s_0 and s_0' are shared using scheme 4.1 into shares $\{s_i\}$ and $\{s_i'\}$. It is easy to see that to compute shares for the bitwise sum modulo two of the secrets s_0 and s_0', player i can simply compute the bitwise sum modulo two of his shares s_i and s_i'.

Another primitive which can be computed locally is "alternation", when bits from two secrets alternate to become a double length string. We show an example to make it more clear:

Suppose that the first string s_1 is equal to "abc" and the second s_2 is "xyz", then the alternation of s_1 and s_2 is equal to "$axbycz$".

Now it should be obvious that, to get a share for the alternation of two secrets, a player should simply compute the alternation for his shares.

Chapter 5

Non-probabilistic Secret Sharing

In this chapter we discuss how to generalize secret sharing schemes to the infinite case without introducing probability measures at all. First we take a look at how traditional secret sharing can be rephrased without referring to probabilities at all, which will then motivate our general definition.

5.1 Definitions

A (traditional) secret sharing scheme can be identified with the collection of the possible choices of the dealer. Namely, the dealer simply picks one of these possibilities, which determines what the secret is, and what each participant will receive as a share. Even the more customary setting can be rephrased in this language when the dealer first chooses the secret to be distributed, and then chooses one of the possible set of shares for this particular secret value: merge the two choices into a single one.

As usual, the secret is a value from the domain S_0, and the share of participant $i \in P$ is an element of S_i. Thus the elements of the product space $\widetilde{D} = S_0 \times \prod_{i \in P} S_i$ describe exactly the *dealer's possible choices*. A secret sharing scheme is determined by giving the collection $D \subseteq \widetilde{D}$, the *allowed choices* of the dealer. Given the scheme D, the dealer simply picks an element $d \in D$, and determines the secret as the $d_0 \in S_0$, and the share of participant $i \in P$ will be d_i, the i-th coordinate of d (we will start the numeration of coordinates from zero).

This definition falls short in one respect: it cannot accommodate the situation when different choices should happen with different frequency. This happens, for example, when there is a predetermined distribution on the secrets and the scheme must be secure even if that distribution is known to unqualified subsets. To remedy the situation (which works at least when all probabilities are rational numbers) we allow the set D of choices to be a *multiset*, i.e., a set in which multiple membership is allowed. When the dealer chooses one element from D, he chooses it uniformly (that is, all elements are chosen equally). Consequently, elements in D with high multiplicity will be chosen more frequently than those with low multiplicity.

Now it is quite easy to translate the usual properties of a secret sharing scheme. The multiset $D \subseteq \widetilde{D}$ *distributes all secrets uniformly* if for each value of the secret $s_0 \in S_0$ the multiset of those $d \in D$ which distributes s_0 has the same cardinality independently of the secret s_0:

$$|\{d \in D : d_0 = s_0\}| = |\{d \in D : d_0 = s_0'\}| \quad \text{for each} \;\; s_0, s_0' \in S_0.$$

Given any choice $d \in D$ of the dealer, the set A of participants see the projection of d into the subspace determined by A. We will denote this projection(as a multiset) by $d \upharpoonright A$. It is clear that the subset A cannot distinguish between d and $d' \in D$ whenever their projection onto A are the same, i.e., if $d \upharpoonright A = d' \upharpoonright A$. Now $A \subseteq P$ *can determine the secret* if for any $d, d' \in D$, such that members of A receive the same shares from d and from d', the secrets determined by d and d' are the same. The subset $A \subseteq P$ has *no information* on a (uniformly distributed) secret if for any $d \in D$ the collection of shares they see, namely $d \restriction A$, allows every possible secret with the same cardinality.

In ramp schemes we are concerned with subsets which have some, but *not full information* on the secret. There are several candidate definitions with different strength between *determining* the secret and having *no information* on it:

1. There exists a pair $d, d' \in D$ of the dealer's choices, such that

$$d \restriction A = d' \restriction A \text{ and } d \restriction S_0 \neq d' \restriction S_0$$

   i.e. the subset A does not determine the secret;

2. For any choice d of the dealer there exists a choice d', such that

$$d \restriction A = d' \restriction A, \textit{ and } d \restriction S_0 \neq d' \restriction S_0$$

   i.e. for no choice of the dealer A can determine the secret uniquely;

3. For some $d \in D$, not all secrets occur with the same cardinality in the multiset $\{d'_0 : d' \in D,\ d' \restriction A = d \restriction A\}$;

4. There exists no $d \in D$ for which the multiset $\{d'_0 : d' \in D,\ d' \restriction A = d \restriction A\}$ would contain every secret with the same cardinality.

Observe that 1 and 2 imply that members of A cannot determine the secret, and might have no information of the secret at all. Definitions 3 and 4, on the other hand, imply that A necessarily has some information on the secret, but they also allow that members of A could always determine the secret.

After this discussion, the next definition should be straightforward.

Definition 5.1 (Perfect uniform non-probabilistic secret sharing scheme)**.** Let P be the set of players, and $\mathcal{A}$ be an access structure on P. Let S_0 be the set of possible secrets and S_i be the set of possible shares of player $i \in P$. The multiset $D \subseteq S_0 \times \prod_{i \in P} S_i$ is a *perfect uniform non-probabilistic secret sharing scheme* if

1. (uniformity) Fixing $s_0 \in S_0$, the multiset $\{d \in D : d_0 = s_0\}$ has the same cardinality independently from the secret.

2. (qualified subsets determine the secret) If the set A of the players is qualified, i.e. $A \in \mathcal{A}$, then for any $d, d' \in D$, such that $d \restriction A = d' \restriction A$, the shared secret is the same: $d_0 = d'_0$.

3. (unqualified subsets have no information) If $A \notin \mathcal{A}$, then for any $d \in D$ the multiset $\{d'_0 : d' \in D,\ d' \restriction A = d \restriction A\}$ contains every element of S_0 at the same cardinality.

5.2 Existence for the general case

In this section we show that, in contrast to the results of other chapters of this thesis, perfect non-probabilistic secret sharing schemes do exist for every access structure $\mathcal{A}$, independently from the cardinality of the participants and from $\mathcal{A}$. In fact, we will show that both general constructions from [14] and from [16] for finite access structures generalize to our case. In both constructions the secret space will have two elements (one bit); the share of each participant will be an appropriately chosen (possibly infinitely long) 0–1 sequence.

By executing the same scheme independently κ times, where κ is some (infinite) cardinal, both the length of the secret and the length of shares will be multiplied by κ. Choosing κ infinite and bigger than the longest share of any of the participants, both the secret and all shares will be exactly κ long 0–1 sequences.

The scheme is called *ideal* if the set of secrets and all sets of shares have the same cardinality. Thus, we get the following consequence of our construction:

Corollary 5.1. *Every access structure can be realized by an (infinite) ideal perfect uniform non-probabilistic secret sharing scheme.* □

Before stating and proving our main result, we state two lemmas which generalize the XOR function for infinitely many arguments. Using these lemmas, the standard constructions can easily be generalized as well.

Lemma 5.1. *For each (possibly infinite) set J there is an* XOR*-like function* XOR : $\{0,1\}^J \to \{0,1\}$*, so that changing the argument at any index changes the value of the function as well.*

Proof. For any two zero-one sequences a and b of length J let $L(a,b)$ denote the number of indexes where they are different. We say that the sequences a and b are *equivalent* and write $a \sim b$ if $L(a,b)$ is finite. It is easy to check that $\sim$ is an equivalence relation, for example, transitivity follows from $L(a,c) \leq L(a,b) + L(b,c)$.

Now $\{0,1\}^J$ splits into disjoint equivalence classes. Pick a representative element from each equivalence class and define XOR arbitrarily on that element. From these values XOR can be computed uniquely on other elements of the equivalence class. □

Lemma 5.2. *The* XOR *function defined above is balanced in the sense that for any zero-one sequence $\sigma \in \{0,1\}^J$ and set $A \subsetneq J$ the sets of zero-one sequences*

$$E_i = \{\sigma' \in \{0,1\}^J : \sigma' \restriction A = \sigma \restriction A,\ \mathsf{XOR}(\sigma) = \mathsf{i}\}$$

where $i = 0, 1$ have the same cardinality.

Proof. Pick any index $i \in J - A$ and let f be the function defined on $\{0,1\}^J$, which swaps the value of its argument at the i-th position. By Lemma 5.1 this f is a bijection between E_0 and E_1. □

During the proof of Lemma 5.1 we relied on the Axiom of Choice when we choose representatives from each equivalence class. We could avoid the usage of the axiom of choice by restricting the domain of the XOR function to zero-one sequences which have only finitely many 1's, and then the value of XOR will be the parity the sum of the digits ot its argument. The proof of Theorem 5.1 goes through with this modification. Therefore it does not rely on the axiom of choice.

Lemmas 5.1 and 5.2 actually claim that the scheme where each player gets zero or one and the secret is the XOR of these values is, in fact, a perfect uniform non-probabilistic secret sharing scheme realizing the "all out of P" threshold access structure.

Theorem 5.1. *Let $\mathcal{A}$ be an access structure on a set P of participants. There is a uniform non-probabilistic secret sharing scheme realizing $\mathcal{A}$ with the set of secrets as* $\{0,1\}$.

Proof. We give two proofs for this theorem. In fact, we show that both known constructions from [14] and from [16] generalize to our case as well.

Proof 1. In [14], Ito et al. used the following idea: the secret is a single bit, and for each qualified set $A \in \mathcal{A}$ the secret is distributed independently among the members of A as follows: each $i \in A$ receives a random bit such that the (modulo 2) sum these bits is equal to the secret. Then each participant receives as many bits as many qualified subsets he is in. When P is finite, it is enough to consider *minimal* qualified subsets only. When P is infinite, however, there might be qualified subsets which contain no minimal ones. This is the case, for example, when $\mathcal{A}$ consists of all infinite subsets of P.

For each $A \in \mathcal{A}$ let XOR_A be an XOR-like function on the set $\{0,1\}^A$, as guaranteed by Lemma 5.1. The set of possible shares for player $i \in P$ will be $S_i = \{0,1\}^{\mathcal{A}_i}$, where

$\mathcal{A}_i = \{A \in \mathcal{A} : i \in A\}$, and let the set of the possible choices of the dealer be

$$D = \{d \in \{0,1\} \times \prod_{i \in P} S_i \,:\, \text{for each } A \in \mathcal{A},\ \mathsf{XOR}_A(\langle (d_i)_A : i \in A \rangle) = d_0\} \tag{5.1}$$

taking each element in this set with multiplicity one. As d_i is an element of S_i, it is a vector whose elements are indexed by those qualified subsets which i is a member of. Thus XOR_A is applied to a zero-one vector indexed by the elements of A, as required.

We claim that D is a perfect uniform non-probabilistic secret sharing scheme realizing $\mathcal{A}$ as defined in 5.1. First, it is uniform. Choose a designated player from each qualified subset $A \in \mathcal{A}$. For every $d \in D$ define $f(d)$ as follows: flip the value of the secret (i.e., d_0), moreover for each $i \in P$, flip the A-th value in d_i if and only if i was the player designated to the subset A. As for each $A \in \mathcal{A}$ exactly one element of $\langle (d_i)_A : i \in A \rangle$ was swapped, the condition in (5.1) holds for $f(d)$. Thus f is a bijection between elements in D yielding the secret 0 and elements yielding the secret 1.

Second, qualified subsets can determine the secret: members of $A \in \mathcal{A}$ can recover all elements of the vector $\langle (d_i)_A : i \in A \rangle$. Applying XOR_A to this vector gives the secret, independently of the other shares.

Third, suppose $B \subset P$ is an unqualified subset. Then, as above, for each qualified subset $A \in \mathcal{A}$ designate a player in A *but not in* B. As B is unqualified, such a player always exists. Define the bijection $f : D \to D$ exactly as above, and observe that f does not touch shares of players in B. Consequently, f is also a bijection of the set $\{d' \in D : d' \restriction B = d \restriction B\}$ for any $d \in D$ swapping the value of the secret.

Proof 2. The second construction described in [16] is, in a certain sense, dual to the first one. We distribute the secret into shares indexed by the *non-qualified* subsets, and each participant receives shares belonging to those subsets he is *not a member of.* In this construction an unqualified subset will miss the share which belongs to that particular subset.

Let the set of the secrets be $S_0 = \{0,1\}$, and $H \subseteq S_0 \times \prod_{A \notin \mathcal{A}} \{0,1\}$ be just the set of sequences $\langle \mathsf{XOR}(\sigma), \sigma \rangle$ when σ runs over $\prod_{A \notin \mathcal{A}} \{0,1\}$. We define the scheme by mapping H to the set of shares as follows. If $h \in H$, then d_0 (i.e., the secret) is h_0, and the share of $i \in P$ is $d_i = h \restriction \{A \notin \mathcal{A} : i \notin A\}$. This is again a perfect uniform secret sharing scheme. Uniformity follows from the fact that there is a bijection between H_0 and H_1, where $H_i = \{h \in H : h_0 = i\}$.

Second, if $A \in \mathcal{A}$ is a qualified set, then for every unqualified set B some member of A should *not* be in B (otherwise A would be a subset of B). Consequently, the value of h_B is known by some member of A, and then they can determine the secret as

$$s_0 = \mathsf{XOR}(\langle h_B : B \notin \mathcal{A} \rangle)$$

Third, if B is unqualified, then the bijection of H, which swaps h_0 and h_B, extends to a bijection of D, which swaps the secret, but keeps the share of every member of B intact. □

Chapter 6

Conclusion

In this thesis we discussed *secret sharing* for infinite secret domains. The first part of the thesis is devoted to the result by Chor and Kushilevitz[4]. We proved an impossibility of secret sharing over countable set of secrets and shares. Our result is slightly more general the the one by Chor and Kushilevitz. Also we gave several counterexamples which show an importance of assumptions in our theorem. Later we discussed possible definition of *secret sharing* over continuum set of secrets. Particularly, using the idea by Gabor Tardos, we constructed a scheme that shows that the definition by Chor and Kushilevitz is "intuitively incorrect". Namely, it is possible that an unqualified set of players can reconstruct the secret. We suggested a modified definition and showed that the positive result by Chor and Kushilevitz [4] holds for the new definition. Finally we gave an introduction to *Lebesgue-Rokhlin* probability spaces and showed that a secret from such spaces can be shared. We suggest a further research in this direction. It seems that the converse is true. Namely, if a secret sharing scheme exists for a secret picked up from a probability space, then this space is *Lebesgue-Rokhlin*.

As a short digression we presented a nice scheme for the situation when a secret is a branch of a binary tree(possible infinite). This scheme seems to be useful as it allows to compute several primitives on a secret without any communication between participants.

In the last part of the thesis we presented our concept of *perfect uniform non-probabilistic secret sharing*, in which we avoid the idea of probability and concentrate on cardinalities. We showed that there exists a *perfect uniform non-probabilistic secret sharing* scheme for any secret domain and any access structure(possibly infinite).

Bibliography

[1] G. Di Crescenzo A. De Santios and G. Persiano. Secret sharing and perfect zero knowledge. In *Advances in Cryptology CRYPTO 93*, volume 773 of *Lecture Notes in Computer Science*, pages 73–84. 1994.

[2] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology CRYPTO 88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. 1990.

[3] G. Blakley. Safeguarding cryptographic keys. *Proceedings of the National Computer Conference*, pages 313–317, 1979.

[4] B. Chor and E. Kushilevitz. Secret sharing over infinite domain. *Journal of Cryptology*, 6(2):87–95, June 1993.

[5] R. Cramer. Introduction to secure computation. 2000.

[6] W. Diffie and M. Hellman. New directions in cryptography, 1976.

[7] R.M. Fano. The transmission of information. Technical report, Research Laboratory of Electronics at MIT, 1949.

[8] S. Fehr. *Secure Multi-Player Protocols: Fundamentals, Generality, and Efficiency.* PhD thesis, University of Aarhus, Denmark, 2003.

[9] R. Gennaro. *Theory and Practice of Verifiable Secret Sharing.* PhD thesis, MIT, 1995.

[10] M. Hirt. *Multi-Party Computation: Efficient Protocols, General Adversaries and Voting.* PhD thesis, ETH, Zurich, 2001.

[11] Internet Corporation For Assigned Names and Numbers. http://www.root-dnssec.org/.

[12] K. Ito. *Introduction to probability theory*, chapter 2. Cambridge Univ. Press., 1984.

[13] D. Khan. *The Codebreakers.* The New American Library, Inc., 1973.

[14] A. Saito M. Ito and T. Nishizeki. Secret sharing schemes realizing general access structures. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.

[15] N. Martin and J. England. *Mathematical Theory of Entropy*, chapter 1. Addison-Wesley Publishing Company,Reading, MA, 1981.

[16] U. Maurer. Secure multi-party computation made simple. *Discrete Appl. Math.*, 154:370–381, February 2006.

[17] V. Rokhlin. On the fundamental ideas of measure theory. *Translations (American Mathematical Society) Series 1*, 10:1 – 54, 1962.

[18] S. Micali S. Goldwasser and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208.

[19] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley and Sons, second edition, 1996.

[20] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[21] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[22] G. Tardos. Personal conversation.

[23] J. von Neuman. Einige satze ubermessbare abbildungen. *The Annals of Mathematics*, 33(3):574 – 586, 1932.

[24] A. Yao. Protocols for secure computations. *Foundations of Computer Science, Annual IEEE Symposium on Foundations of Computer Science (FOCS 1982)*, 0:160–164, 1982.