PHD THESIS

Security of CRT-based Secret Sharing Schemes

Supervisor:
Prof. Dr. Ferucio Laurentiu
Țiplea

Author:
Constantin Cătălin
Dragan

September 2013
Abstract

The Chinese Remainder Theorem (CRT) is a very useful tool in many areas of theoretical and practical cryptography. One of these areas is the theory of threshold secret sharing schemes. A \((t+1, n)\)-threshold secret sharing scheme is a method of partitioning a secret among \(n\) users by providing each user with a share of the secret such that any \(t + 1\) users can uniquely reconstruct the secret by pulling together their shares. Several threshold schemes based on CRT are known \([1, 45, 29]\). These schemes use sequences of pairwise co-prime positive integers with special properties. The shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders. The secret can be reconstructed by some sufficient number of shares by using CRT. It is well-known that the CRT-based threshold secret sharing schemes are not perfect (and, therefore, not ideal) but some of them are asymptotically perfect and asymptotically ideal and perfect zero-knowledge if sequences of consecutive primes are used for defining them.

In this thesis we introduce \((k-)\)compact sequences of co-primes and their applications to the security of CRT-based threshold secret sharing schemes is thoroughly investigated. Compact sequences of co-primes may be significantly denser than sequences of consecutive primes of the same length, and their use in the construction of CRT-based threshold secret sharing schemes may lead to better security properties. Concerning the asymptotic idealness property for CRT-based threshold schemes, we have shown there exists a necessary and sufficient condition for the Goldreich-Ron-Sudan (GRS) scheme and Asmuth-Bloom scheme if and only if \((1-)\)compact sequences of co-primes are used. Moreover, the GRS and Asmuth-Bloom schemes based on \(k\)-compact sequences of co-primes are asymptotically perfect and perfect zero-knowledge. The Mignotte scheme is far from being asymptotically perfect and perfect zero-knowledge, no matter the sequences of co-primes used. The information rate of the Mignotte scheme asymptotically goes to 0.

We also consider the construction of a CRT-based scheme, called distributive weighted threshold secret sharing scheme, that satisfies the asymptotic perfectness and perfect zero-knowledge property. As the scheme allows for the share spaces to be arbitrarily large compared to the secret space, the scheme can not be asymptotically ideal.

Keywords:
Acknowledgements

I would like to thank my supervisor Professor Dr. Ferucio Laurențiu Țiplea for his continuous encouragements and suggestions, that led to this thesis.

It is my pleasure to thank my family and friends, and my teachers for supporting me during this important step of my education.

Work supported by the European Social Fund in Romania, under the responsibility of the Managing Authority for the Sectoral Operational Programme for Human Resources Development 2007-2013 [grant POSDRU/CPP 107/DMI 1.5/S/78342]
Contents

1 Introduction 1
   1.1 Introduction .............................................. 1
   1.2 Contributions ............................................. 3
   1.3 Thesis structure .......................................... 5

2 Preliminaries 7
   2.1 Sets ......................................................... 7
   2.2 Number Theory ............................................. 9
      2.2.1 Divisibility of integers ............................... 9
      2.2.2 Prime numbers ....................................... 11
      2.2.3 Greatest common divisor ............................ 15
      2.2.4 The Euclidean Algorithm ............................ 17
      2.2.5 Congruences ......................................... 19
      2.2.6 Chinese Remainder Theorem ....................... 20
      2.2.7 Chinese Remainder Algorithm ...................... 25
      2.2.8 Complexity ........................................... 27
   2.3 Information Theory ....................................... 27
      2.3.1 Probability .......................................... 27
      2.3.2 Entropy .............................................. 35

3 Secret Sharing Schemes 39
   3.1 Introduction ............................................... 39
   3.2 Access Structures ......................................... 41
   3.3 Security concepts ......................................... 44
   3.4 Perfect realizations of access structures ................ 59
   3.5 Information rates .......................................... 64
   3.6 Classification of secret sharing schemes ................. 66
      3.6.1 Threshold secret sharing schemes ................. 66
      3.6.2 Unanimous consent schemes ....................... 68
      3.6.3 Weighted threshold secret sharing schemes ...... 69
      3.6.4 Multilevel secret sharing schemes ............... 71
      3.6.5 Compartmented secret sharing schemes ............ 79

4 CRT-based threshold schemes and their security 85
   4.1 Threshold secret sharing schemes ....................... 86
      4.1.1 Asmuth-Bloom scheme ............................... 86
      4.1.2 Mignotte scheme ...................................... 88
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.3 Goldreich, Ron and Sudan scheme</td>
<td>89</td>
</tr>
<tr>
<td>4.1.4 A Generic CRT-based scheme</td>
<td>91</td>
</tr>
<tr>
<td>4.2 Security properties</td>
<td>92</td>
</tr>
<tr>
<td>4.3 Compact sequences of co-primes</td>
<td>95</td>
</tr>
<tr>
<td>4.3.1 More on security properties</td>
<td>97</td>
</tr>
<tr>
<td>4.3.2 Properties of compact sequences</td>
<td>98</td>
</tr>
<tr>
<td>4.4 Bounding the loss of entropy</td>
<td>101</td>
</tr>
<tr>
<td>4.5 Security of the GRS scheme</td>
<td>103</td>
</tr>
<tr>
<td>4.5.1 Asymptotic idealness</td>
<td>104</td>
</tr>
<tr>
<td>4.5.2 Perfect zero-knowledge</td>
<td>108</td>
</tr>
<tr>
<td>4.6 Security of the Asmuth-Bloom scheme</td>
<td>110</td>
</tr>
<tr>
<td>4.6.1 Asymptotic idealness</td>
<td>112</td>
</tr>
<tr>
<td>4.6.2 Perfect zero-knowledge</td>
<td>119</td>
</tr>
<tr>
<td>4.7 Security of the Mignotte scheme</td>
<td>120</td>
</tr>
<tr>
<td>5 CRT-based weighted schemes and their security</td>
<td>123</td>
</tr>
<tr>
<td>5.1 DWTAS</td>
<td>124</td>
</tr>
<tr>
<td>5.1.1 The access structure</td>
<td>124</td>
</tr>
<tr>
<td>5.1.2 DWTAS do not have ideal realizations</td>
<td>126</td>
</tr>
<tr>
<td>5.2 DWTSSS</td>
<td>128</td>
</tr>
<tr>
<td>5.2.1 Epsilon sequences of co-primes</td>
<td>128</td>
</tr>
<tr>
<td>5.2.2 Distributive weighted threshold scheme</td>
<td>132</td>
</tr>
<tr>
<td>5.3 Security issues of DWTSSS</td>
<td>133</td>
</tr>
<tr>
<td>5.3.1 More on security properties</td>
<td>133</td>
</tr>
<tr>
<td>5.3.2 Asymptotic idealness</td>
<td>135</td>
</tr>
<tr>
<td>5.3.3 Perfect zero-knowledge</td>
<td>136</td>
</tr>
<tr>
<td>6 Conclusion and Future work</td>
<td>137</td>
</tr>
</tbody>
</table>

Published and Submitted Papers                                           139
Chapter 1

Introduction

1.1 Introduction

A secret sharing scheme is a method of partitioning a secret among some participants by providing each participant with a piece of the secret (called a share). Any set of participants that contains sufficient shares such that they can recover the secret is called an authorized set, whereas any set of participants that cannot recover uniquely the secret is called an unauthorized set. Furthermore, any secret sharing scheme should satisfy the following security properties with respect to the secret reconstruction phase:

- **accessibility:** any authorized set of participants can uniquely recover the secret;
- **perfect security:** any unauthorized set of participants should not obtain any partial information on the secret.

Threshold secret sharing schemes (threshold schemes, for short) have independently been proposed for the first time by Shamir [54] and Blakley [9]. The authorized sets considered by a \((t+1,n)\)-threshold scheme have the main characteristic that the number of participants needed to reconstruct the secret can be lower bounded by a fixed threshold \(t + 1\), where \(n\) is the total number of participants. Blakley’s scheme is based on hyperplane intersections, while Shamir’s scheme is based on polynomial interpolation. Other essential types of secret sharing schemes consider in our thesis are:

**Weighted threshold secret sharing schemes** [54, 46, 5] as natural generalizations of threshold secret sharing schemes, where each participant is assigned a weight depending on his importance (role) in the group of all participants. The secret can be reconstructed if and only if the
sum of the weights assigned to a set of participants is greater than or equal to a fixed threshold. This idea was first proposed by Shamir [54] who also suggested a realization of it by using tuples of polynomial values associated to each participant.

**Multilevel secret sharing schemes** [55, 60, 5, 6], where the participants are divided into disjoint levels according to their importance. These levels are totally ordered and participants on lower levels are more important than participants on higher levels. According to the restriction over the number of participants that take part in the recovery of the secret we have *disjunctive multilevel schemes* [55] (DMAS, for short), where the set of participants satisfy the threshold *at some level* \(i\), and *conjunctive multilevel schemes* [60], where the set of participants must satisfy the threshold *for all levels* \(i\).

A novel category of \((t + 1, n)\)-threshold secret sharing schemes based on the Chinese Remainder Theorem (CRT) have independently been proposed by Asmuth and Bloom [1] and Mignotte [45], and later by Goldreich, Ron and Sudan [29] (GRS, for short). The main characteristic of this class of schemes is the use of sequences of pairwise co-prime positive integers with special properties. The shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders. The secret can be uniquely recovered from \(t + 1\) shares, where \(t + 1\) depends on the sequence, by using CRT.

The authors of the CRT-based \((t+1, n)\)-threshold secret sharing schemes in [1, 45] have ensured the security of their schemes by counting the number of possible solutions a group of less than \(t+1\) participants have to try in order to obtain the secret. The security of the threshold scheme in [29] was argued in a rather different way, by showing that the secrets are “indistinguishable” if at most \(t - 1\) shares are known and the sequence of co-prime integers consists of prime numbers of the “same magnitude”.

Following an *information theoretic* approach concerning the study of the security of a CRT-based threshold scheme, Quisquater, Preneel and Vandewalle [51] have introduced two modern concepts: *asymptotic perfectness* and *asymptotic idealness*. Then, they proved that the threshold scheme in [29] is asymptotically ideal (and, therefore, asymptotically perfect) provided that it uses sequences of consecutive primes. Moreover, using an *complexity theoretic* approach, they also proved the scheme in [29] satisfies the perfect zero-knowledge property for consecutive primes.

The results obtained in [51] leave open a series of problems concerning the security of the CRT-based schemes:

**Open problem (OP1):** Does there exist other sequences of co-primes (more compact than sequences of consecutive primes) that can provide the
same level of security or better security for the CRT-based threshold schemes?

**Open problem (OP2)** concerns the security of the Asmuth-Bloom scheme, as the proofs given in [51] for the asymptotic perfectness and asymptotic idealness of the GRS scheme do not lead to similar results for the Asmuth-Bloom scheme.

**Open problem (OP3)** deals with finding a necessary and sufficient condition for the asymptotic idealness of the GRS scheme (or the Asmuth-Bloom scheme).

**Open problem (OP4)** targets the refinement of the loss of entropy\(^1\) for the CRT-based threshold schemes.

**Open problem (OP5)** focuses on the problem of construction of CRT-based schemes for other classes of access structures that satisfy the security properties in [51].

### 1.2 Contributions

Concerning the security arguments previously mentioned, we can note that the statistical difference between the random variables associated to two different secrets can be better bounded from above if the scheme is based on sequences of prime numbers of the same magnitude (in fact, this is the advice of the authors of [29], although they did not define the term “same magnitude”). Sequences of sufficiently large consecutive prime numbers, as it was considered in [51], are examples of sequences of prime numbers of the same magnitude. Moreover, with a suitable definition for the “same magnitude”, one should expect similar results to those developed in [51] for CRT-based threshold schemes based on sequences of co-primes of the same magnitude.

This is in fact the main aim of our thesis. More precisely, in [3] we introduced the concept of a *compact sequence of co-primes* as a formal approach to “integers of the same magnitude”. A compact sequence of co-primes is a sequence of pairwise co-prime positive integers whose elements are members of an interval \((x, x + x^\theta)\), for some integer \(x\) and \(\theta \in (0, 1)\). Additionally, given a sequence of consecutive primes in some interval \((x, x + x^\theta)\), one can find a denser sequence of co-primes in the same interval. This fact leads to better security for CRT-based threshold schemes if they are based on such sequences. Another advantage of using compact sequences of co-primes in the design of CRT-based threshold schemes consists of the fact that it is

---

\(^1\) The loss of entropy is the basis for the definition of asymptotic perfectness and asymptotic idealness, and it will be explained in Section 4.2.
easier to define sequences of large co-primes than sequences of consecutive large primes. One has to fix a security parameter \( x \), to choose \( \theta \in (0, 1) \) as close as possible to 1, and then to generate a sequence of co-primes in \((x, x + x^\theta)\). The co-primality test is faster than the primality test.

Furthermore, in [21, 27] we have noticed that we can assign a certain mobility to the element which defines the secret space, in relation with the rest of the sequence of co-primes. According to this remark, we have extended compact sequences to \( k \)-\textit{compact sequence of co-primes}, in which the element used to define the secret space can be smaller than the sequence, greater than the sequence, or in the middle of the sequence. A \( k \)-\textit{compact} sequence of co-primes contains elements from the interval \((kx - x^\theta, kx + x^\theta)\), for some positive integers \( x, k \) and \( \theta \in (0, 1) \). Then, in [21] with the introduction of \( k \)-compact sequences we adapted the asymptotic idealness (and, therefore, asymptotic perfectness) and perfect zero-knowledge properties to account for the mobility of the secret space.

Concerning the security of the GRS threshold secret sharing scheme based on compact sequences of co-primes, we have shown in [3] that the scheme is asymptotically ideal and perfect zero-knowledge with respect to \((t, \Theta)\)-\textit{compact sequences} \(^2\). Moreover, we have shown that there exists a necessary and sufficient condition concerning the asymptotic idealness of the GRS scheme if and only if \((1-)\text{-compact sequences of co-primes}\) are considered. Additionally, the GRS threshold scheme based on \( k \)-compact sequences of co-primes is asymptotically perfect and perfect zero-knowledge.

Regarding the security of the Asmuth-Bloom scheme based on compact sequences of co-primes, we have shown in [3] that the scheme is asymptotic perfect (with the information rate \(^3\) asymptotically 2) if \( \text{almost-} \Theta \)-\textit{compact sequences} are considered, and is asymptotically ideal with respect to \( \text{quasi-compact sequences} \). In [27] we provided a more suitable bound for the loss of entropy for the Asmuth-Bloom threshold scheme, which can be further extended to the GRS threshold scheme. Then, we proved there exists a necessary and sufficient condition concerning the asymptotic idealness of the Asmuth-Bloom scheme if and only if \((1-)\text{-compact sequences of co-primes}\) are considered. Furthermore, the Asmuth-Bloom scheme based on almost-\( \Theta \) compact sequences or \( \text{quasi-compact sequences or } k \)-compact sequences of co-primes is perfect zero-knowledge.

To our knowledge, the security of the Mignotte scheme has never been studied using modern concepts such as asymptotic perfectness and perfect zero-knowledge. In [3] we proved that the Mignotte scheme based on compact sequences is far from being asymptotically perfect and perfect zero-knowledge.

\(^2\) \((t, \Theta)\)-\textit{compact sequence}, \text{almost-} \Theta \text{-compact and} \text{quasi-} \text{compact are particular cases of compact sequence of co-primes where certain constrains were imposed. The constrains were technical and necessary in proofs in [3].}

\(^3\) The information rate is defined as the fraction of the cardinality of the share space over the cardinality of the secret space.
Chapter 1. Introduction

zero-knowledge. Furthermore, the information rate of the Mignotte scheme asymptotically goes to 0.

With respect to the existence of other CRT-based schemes that satisfy the security properties in [51], in [26] we considered the following example of DMAS with just two levels $U_1$ and $U_2$ and thresholds $t_1 = 2$ and $t_2 = 4$. Assume that $U_1$ consists of directors, and $U_2$ of senior tellers, of a bank. The choice of these parameters tells that a bank vault can be opened by either any two directors or four senior tellers. According to the definition of a DMAS, the bank vault can also be opened by three senior tellers together with one director, but not by two senior tellers together with one director. This is somewhat contrary to our intuition that, according to the choice of the parameters, one director can be replaced by any two senior tellers.

This small example led us to consider multilevel schemes where each participant has associated a weight and where each participant in an authorized set can be replaced by any number of participants whose weights can compensate the weight of that participant. These new multilevel schemes are introduced via weighted threshold schemes and are called distributive weighted threshold secret sharing schemes. Additionally, we proved the scheme is asymptotically perfect and perfect zero-knowledge. As the scheme allows for the share spaces to be arbitrarily large compared to the secret space, the scheme can not be asymptotically ideal.

To summarise, in [3] we have answered OP1 and proposed a partial solution to OP2, in [21] we have given a complete solution to OP1 \(^4\) and OP3, and in [27] we have completed OP2 and OP4. Furthermore, in [26] we offered a partial solution to OP5 as the scheme proposed can not satisfy all the security properties in [51].

1.3 Thesis structure

The thesis is organized in six chapters.

In the introduction we presented a brief overview of the domain, the novelty of the thesis and its structure.

Chapter 2 deals with the introduction of the most basic concepts used throughout our thesis. The main directions are sets (Section 2.1), number theory (Section 2.2) and information theory (Section 2.3). In the first section we give a brief introduction to sets. Whereas in the second section we discuss number theory and provide a detailed overview of the following concepts: divisibility of integers, prime numbers, greatest common divisor, the euclidean algorithm, congruences, Chinese remainder theorem and algorithm, and complexity. In the last section we concentrate on the definitions and properties of the concepts of probability and entropy.

\(^4\) It is our belief that (1-)compact sequences is the largest class of co-primes that satisfy the asymptotic idealness property.
In Chapter 3 we introduce secret sharing schemes. After a short introduction to applications in Section 3.1, we define access structures in Section 3.2 and provide some study on basic operations with them. In Section 3.3 we formally define secret sharing schemes and their security properties using the probabilistic approach from [13, 59, 58] and the information theory approach due to [38, 41, 14]. In Section 3.4 we show there exists perfect realizations of access structures, while in Section 3.5 we measure the efficiency of perfect schemes (idealness property). Last section deals with the classification of schemes based on the type of access structures used.

In Chapter 4 we describe the CRT-based threshold schemes from [1, 45, 29] (Section 4.1), and present the security concepts introduced by Quisquater et al. [51] and their results concerning the security of the threshold scheme in [29] based on consecutive primes (Section 4.2). In the rest of the chapter we deal with our contribution to the Open Problems OP1-OP4. Thus, we propose a generic construction for CRT-based threshold secret sharing schemes (for uniformity presented at the end of Section 4.1) and introduce in Section 4.3 compact sequences of co-primes [3] and \( k \)-compact sequences [21, 27] as the formal approach to “integers of the same magnitude” [29], and study some of their basic properties. In Section 4.4 we provide a more suitable bound [27] for the loss of entropy. In the last three sections (4.5, 4.6 and 4.7) we study the security of the schemes in [29, 1, 45] based on compact sequences and \( k \)-compact sequences of co-primes. Furthermore, for the schemes in [1] and [29] a necessary and sufficient condition is provided with respect to asymptotic idealness.

In Chapter 5 we propose a new secret sharing scheme, called distributive weighted threshold scheme [26]. We prove there exists sequences of co-primes that satisfy the requirements considered by the co-primes used in this scheme. Concerning the security of the distributive weighted threshold scheme, we show that the scheme is asymptotically perfect and perfect zero-knowledge. As the scheme allows for the share spaces to be arbitrarily large compared to the secret space, the scheme can not be asymptotically ideal.

In the last chapter we summaries the results we obtained and provide some interesting future work directions.
Chapter 2

Preliminaries

2.1 Sets

The formal concept of set was one of the most discussed subject in mathematics, as it is the fundamental basis of all mathematical constructions: relation, function, numbers (integers or real), and so forth.

The introduction of this concept is possible through the Zermelo-Fraenkel axiomatic system [19], in which “belongs” (denoted \( \in \)) is a primitive property. We are only interested in some of the basic properties of sets.

**Definition 2.1.1.** [19] Let \( A \) and \( B \) be two sets. The set \( A \) is **equal to** \( B \), denoted \( A = B \), if \( x \) belongs to \( A \) if and only if \( x \) belongs to \( B \). Furthermore, \( A \) and \( B \) are not equal, denoted \( A \neq B \), if there exists \( a \in A \) with \( a \notin B \) or \( b \in B \) with \( b \notin A \).

**Proposition 2.1.2.** [19] Given the sets \( A, B \) and \( C \), the equality of sets satisfies the following properties

1. **reflexivity**: \( A = A \);
2. **symmetry**: if \( A = B \), then \( B = A \);
3. **transitivity**: if \( A = B \) and \( B = C \), then \( A = C \).

**Proof.** The proof is trivial and based on Definition 2.1.1.

**Example 2.1.3.** Consider \( A = \{1, 2, 3\} \), \( B = \{2, 3, 4\} \) and \( C = \{1, 2, 3\} \). Then, \( A = C \) and \( A \neq B \).
Definition 2.1.4. [19] Let $A$ and $B$ be two sets. The set $A$ is a subset of $B$, denoted $A \subseteq B$, if any element from $A$ is an element of $B$. Moreover, the set $A$ is a proper subset, denoted $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Proposition 2.1.5. [19] Let $A, B$ and $C$ be three sets. Then, the following properties hold

1. $A \subseteq A$;
2. if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$;
3. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$;
4. $A \subseteq B$ if and only if $A \subset B$ or $A = B$;
5. if $A \subset B$, then $B \not\subseteq A$;
6. if $A \subset B$ and $B \subseteq C$ or $A \subseteq B$ and $B \subset C$, then $A \subset C$.

Proof. Property (1)-(2): Directly from Definition 2.1.4.

Property (3): Based on Definition 2.1.1, the result follows.

Property (4): Assume $A \subseteq B$. If for any $b \in B$ we have $b \in A$, then $B \subseteq A$. Property (3) leads to $A = B$. Otherwise, there exists $b \in B$ with $b \notin A$, then $A \subset B$ (see Definition 2.1.4).

Conversely, if $A \subset B$ then $A \subseteq B$ (Definition 2.1.4), or if $A = B$ we have $A \subseteq B$ (Property (3)).

Property (5): As $A \subset B$, there exists $b \in B$ such that $b \notin A$. Therefore, $B \not\subseteq A$.

Property (6): Assume $A \subset B$ and $B \subseteq C$. From Properties (2) and (4), we have $A \subseteq C$. As $A \neq B$, then $A \neq C$. Therefore, the result follows. Similarly, one can show that $A \subseteq B$ and $B \subset C$ leads to $A \subset C$. 

Example 2.1.6. Consider $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ and $C = \{1, 2, 3, 4\}$. Then, $A \subset C$ and $B \subset C$.

Let $A, B$ and $U$ be three finite sets. We define the following operations over sets:

The power set of $A$, denoted $\mathcal{P}(A)$, is the set of all subsets of $A$ including $A$ itself and the empty set. Consider $A = \{1, 2\}$. Then, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

The union of $A$ and $B$, denoted $A \cup B$, is the set of all the elements from $A$ or from $B$
\[ A \cup B = \{a \mid a \in A \text{ or } a \in B\} . \]

Let $A = \{1, 2, 3\}$, $B = \{2, 3, 5\}$. Then, $A \cup B = \{1, 2, 3, 5\}$. 

8
Chapter 2. Preliminaries

The intersection of $A$ and $B$, denoted $A \cap B$, is the set of all the elements that are both from $A$ and $B$

$$A \cap B = \{a \mid a \in A \text{ and } a \in B\}.$$

Let $A = \{1, 2, 3\}, B = \{2, 3, 5\}$. Then, $A \cap B = \{2, 3\}$.

The difference of $A$ and $B$, denoted $A/B$ or $A - B$, is the set of all the elements that are only from $A$ and not from $B$. Sometimes, the difference is called relative complement of $B$ in $A$

$$A/B = \{a \mid a \in A \text{ and } a \notin B\}.$$

Let $A = \{1, 2, 3\}, B = \{2, 3, 5\}$. Then, $A/B = \{1\}$ and $B/A = \{5\}$.

The absolute complement (or simply complement) of $A$, denoted $\overline{A}$, is the set of all the elements that are from $U$ and not from $A$

$$\overline{A} = \{a \mid a \in U \text{ and } a \notin A\}.$$

Let $A = \{1, 2, 3\}, B = \{2, 3, 5\}$ and $U = \{1, 2, 3, 4, 5\}$. Then, $\overline{A} = \{4, 5\}$ and $\overline{B} = \{1, 4\}$. Moreover, $U = A \cup \overline{A}$ and $U = B \cup \overline{B}$.

The cartesian product of $A$ and $B$, denoted $A \times B$, is the set of all pairs $(a, b)$, for any $a \in A$ and any $b \in B$

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Let $A = \{1, 2, 3\}, B = \{2, 4\}$. Then, $A \times B = \{(1, 2), (1, 4), (2, 2), (2, 4), (3, 2), (3, 4)\}$ and $B \times A = \{(2, 1), (2, 2), (2, 3), (4, 1), (4, 2), (4, 3)\}$.

In this thesis, we consider the following particular sets:

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ as the set of natural numbers;
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ as the set of integers;
- $\mathbb{R}$ as the set of real numbers,

2.2 Number Theory

2.2.1 Divisibility of integers

Definition 2.2.1. [19] The absolute value of an integer $a$, denoted $|a|$, is defined by

$$|a| = \begin{cases} 
  a, & \text{if } a \geq 0 \\
  -a, & \text{otherwise}
\end{cases}$$

Example 2.2.2. Consider $a = 3, b = -2$ and $c = 0$, then $|a| = a = 3, |b| = -b = 2$ and $|c| = c = 0$. 


Definition 2.2.3. [19] Let \(a\) and \(b\) be integers with \(a \neq 1\) and \(a \leq b\). We say that \(a\) divides \(b\), denoted by \(a \mid b\), if there exists an integer \(c\) such that \(b = ac\). Furthermore, \(a\) is called the divisor of \(b\), and \(b\) the multiple of \(a\). If \(a\) does not divide \(b\), we write \(a \nmid b\).

Example 2.2.4. Consider \(a = 4, b = 5, c = 8\) and \(d = 10\). Then, \(a \mid c\) and \(c \mid d\). However, \(a \nmid b\) and \(a \nmid d\).

Theorem 2.2.5. [19] Let \(a\) and \(b\) be integers with \(b \neq 0\). Then, there exists unique integers \(q\) and \(r\) such that
\[
a = q \cdot b + r
\]
and \(0 \leq r < |b|\).

Proof. For simplicity, we consider \(b > 0\).

Let \(A\) be the set of all positive integers that can be obtained from \(a - bq\), for any \(q \in \mathbb{Z}\):
\[
A = \{a - bq | q \in \mathbb{Z}\} \cap \mathbb{N}.
\]
If \(a < 0\), then \(a - ba \in A\), and if \(a \geq 0\), then \(a \in A\). Therefore, \(A\) is a non-empty set.

Let \(r \in A\) be the smallest number such that \(r \leq s\) for any \(s \in A\). Then, \(r = a - bq\) for some \(q \in \mathbb{Z}\).

Claim 1: \(r\) satisfies \(0 \leq r < b\).

Proof of Claim 1: As \(r \in A\), we have \(r \geq 0\). Now, assume that \(r \geq b\). As \(r > r - b \geq 0\) and \(r - b = a - b(q + 1)\), we have \(r - b \in A\). Therefore, our assumption is false, and \(r < b\).

Claim 2: There exists a unique \(r\) and \(q\) that satisfy \(a = q \cdot b + r\) and \(0 \leq r < b\).

Proof of Claim 2: Assume, by contradiction, there exists \(q, q', r, r' \in \mathbb{Z}\) such that \(a = q \cdot b + r\) and \(a = q' \cdot b + r'\) with \(0 \leq r < b\) and \(0 \leq r' < b\).

If \(q = q'\), then \(r = r'\). Similarly, \(r = r'\) leads to \(q = q'\).

We assume \(q < q'\) and \(r \neq r'\). Then, \(r' = r - b(q' - q)\). As \(r < b\) and \(q' - q > 0\), we have \(r' < 0\). Therefore, our assumption is false, and \(q = q'\) and \(r = r'\).

Based on Claim 1 and Claim 2, the result of the theorem follows.

In the equality \(a = q \cdot b + r\), \(q\) is called quotient and \(r\) the remainder. Moreover, we express them by
\[
q = a \div b, \quad r = a \mod b.
\]

Proposition 2.2.6. [19] Let \(a, b\) and \(c\) be integers. Then, the following properties hold:
Chapter 2. Preliminaries

(1) 0 divides only 0;
(2) \( a \) divides 0 and \( a \);
(3) 1 divides \( a \);
(4) \( a \mid b \) if and only if \( a \mid (-b) \);
(5) if \( a \mid b \) and \( b \mid c \), then \( a \mid c \);
(6) if \( a \mid (b + c) \) and \( a \mid b \), then \( a \mid c \);
(7) if \( a \mid b \), then \( ac \mid bc \). Conversely, if \( c \neq 0 \) and \( ac \mid bc \), then \( a \mid b \);
(8) if \( a \mid b \) and \( a \mid c \), then \( a \mid (\alpha a + \beta b) \) for any \( \alpha, \beta \in \mathbb{Z} \);
(9) if \( a \mid b \) and \( b \neq 0 \), then \( |a| \leq |b| \).

Proof. The proofs are trivial, and based on the fact that for any \( a \mid b \) there exists \( c \) such that \( b = ca \).

2.2.2 Prime numbers

Definition 2.2.7.\cite{19} A positive integer \( p \geq 2 \) is called a prime number if its only positive divisors are \( p \) and 1. Any positive \( m \geq 2 \) that is not prime is called a composite number.

Example 2.2.8. Consider \( a = 4 \) and \( b = 7 \). Then, \( b \) is prime as the only divisors are 1 and 7, and \( a \) is composite as 2 is a divisor.

Definition 2.2.9.\cite{19} Let \( n \geq 2 \). The numbers \( m_1, \ldots, m_n \in \mathbb{Z} \) are called co-primes (or relatively primes) if the only positive divisor is 1. Moreover, the numbers are called pairwise co-primes, if \( m_i \) and \( m_j \) are co-prime, for any \( 1 \leq i < j \leq n \).

We use \((m_1, \ldots, m_n) = 1\) to express that \( m_1, \ldots, m_n \) are co-primes. A detailed justification concerning this notation is given in the next section.

Example 2.2.10. Consider \( a = 4, b = 5, c = 6 \) and \( d = 7 \). Then, \( a \) and \( b \) are co-prime, and \( b \) and \( c \) co-prime. Moreover, \( a, b \) and \( d \) are pairwise co-primes.

Theorem 2.2.11.\cite{19} Let \( n \geq 2 \) be a positive integer and \( m_1, \ldots, m_n \in \mathbb{Z} \).

Then, if and only if there exists \( \alpha_1, \ldots, \alpha_n \in \mathbb{Z} \) such that

\[ \alpha_1 m_1 + \cdots + \alpha_n m_n = 1 . \]

Proof. We prove the converse. Assume there exists \( \alpha_1, \ldots, \alpha_n \in \mathbb{Z} \) such that

\[ \sum_{i=1}^{n} \alpha_i m_i = 1 . \]

Then, \( m_1, \ldots, m_n \) do not have a common divisor \( d \) greater than 1, as \( d \) should divide the sum \( \alpha_1 m_1 + \cdots + \alpha_n m_n \) (meaning \( d \) should divide 1). Therefore, the elements \( m_1, \ldots, m_n \) are relatively prime.
2.2. Number Theory

We prove now the direct implication. Assume that $m_1, \ldots, m_n$ are co-primes. Let $A$ be the set of all the positive values that can be obtained from the sum $\alpha_1m_1 + \cdots + \alpha_nm_n$ for any $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$:

$$A = \{\alpha_1m_1 + \cdots + \alpha_nm_n \mid \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\} \cap \mathbb{N}.$$ 

Let $\alpha_i = m_i$, for any $1 \leq i \leq n$. The set $A$ is not empty, as $m_1^2 + \cdots + m_n^2 = c$ with $c \neq 0$, and $c \in A$.

Consider $d$ the smallest positive integer from $A$ different from 0. As $\alpha_1m_1 + \cdots + \alpha_nm_n = d$, we prove that $d|m_i$ for any $i$.

Based on Theorem 2.2.5, for any $1 \leq i \leq n$ there exists $q_i$ and $r_i$ with $0 \leq r_i < d$ such that

$$m_i = d \cdot q_i + r_i.$$

Then, $r_i$ can also be viewed as

$$r_i = m_i - d \cdot q_i$$

$$= m_i - (\alpha_1m_1 + \cdots + \alpha_nm_n) \cdot q_i$$

$$= (1 - q_i\alpha_i)m_i + \sum_{j=1, j \neq i}^{n} (-q_i\alpha_j)m_j.$$

According to the above form of $r_i$ and the fact that $r_i \geq 0$, we have $r_i \in A$. (Recall the choice of $d$.) Therefore, $r_i = 0$ and $d|m_i$ for any $1 \leq i \leq n$. That leads to $d = 1$. 

**Corollary 2.2.12.** \[19\] Let $n \geq 2$ and $m_1, \ldots, m_n \in \mathbb{Z}$. Then, the following properties hold:

1. if $(b, m_i) = 1$ for any $1 \leq i \leq n$, then $(b, m_1 \cdots m_n) = 1$;
2. if $(b, m_i) = 1$ for some $1 \leq i \leq n$, then $(b, m_1, \ldots, m_n) = 1$;
3. if $m_1, \ldots, m_n$ are pairwise co-prime and $m_i|b$ for any $1 \leq i \leq n$, then $m_1 \cdots m_n|b$;
4. if $(b, m_1) = 1$ and $b|(m_1 \cdots m_n)$, then $b|(m_2 \cdots m_n)$;
5. if $p$ prime and $p|(m_1 \cdots m_n)$, then there exists $1 \leq i \leq n$ with $p|m_i$.

**Proof.** For simplicity, we prove all the properties for $n = 2$. Furthermore, the sequences $\alpha_i$ and $\beta_i$ are introduced based on Theorem 2.2.11, for any $1 \leq i \leq n$.

**Property (1):** There exists $\alpha_1, \alpha_2, \beta_1, \beta_2$ such that

$$\alpha_1m_1 + \beta_1b = 1$$

$$\alpha_2m_2 + \beta_2b = 1.$$

Note that

$$(\alpha_1m_1 + \beta_1b)(\alpha_2m_2 + \beta_2b)$$

$$= 1$$

$$\alpha_1\alpha_2 \cdot m_1m_2 + (\alpha_1m_1\beta_2 + \alpha_2m_2\beta_1 + \beta_1\beta_2)b \cdot b$$

$$= 1.$$

Therefore, based on Theorem 2.2.11, we have $(b, m_1m_2) = 1$. 

12
Chapter 2. Preliminaries

Property (2): Assume $i = 1$. Let $\alpha_1, \beta_1$ such that
$$\alpha_1 m_1 + \beta_1 b = 1.$$  
Using the converse of Theorem 2.2.11 for
$$\alpha_1 m_1 + 0 \cdot m_2 + \beta_1 b = 1,$$
the result easily follows.

Property (3): As $(m_1, m_2) = 1$, there exists $\alpha_1, \alpha_2 \in \mathbb{Z}$ such that
$$\alpha_1 m_1 + \alpha_2 m_2 = 1.$$  
Moreover, from $m_1 | b$ and $m_2 | b$ there exists $\beta_1, \beta_2$ such that
$$b = \beta_1 m_1 = \beta_2 a_2.$$  
Combining the above relations, we have
$$b = \beta_1 m_1 = \beta_1 m_1 \alpha_1 m_1 + \beta_1 m_1 \alpha_2 m_2 = m_1 m_2 (\beta_2 \alpha_1 + \beta_1 \alpha_2).$$
Therefore, $m_1 m_2 | b$.

Property (4): Given $(b, m_1) = 1$, let $\alpha_1, \beta_1 \in \mathbb{Z}$ such that $\alpha_1 m_1 + \beta_1 b = 1$. From $b | (m_1 m_2)$, there exists $\gamma$ such that $m_1 m_2 = b \gamma$.
To prove that $b | m_2$, we consider $m_2$ as
$$a_2 = 1 \cdot m_2 = (\alpha_1 m_1 + \beta_1 b) m_2 = \alpha_1 m_1 m_2 + \beta_1 bm_2 = \alpha_1 b \gamma + \beta_1 bm_2 = b (\alpha_1 \gamma + \beta_1 m_2).$$
Therefore, $b | m_2$.

Property (5): Assume that $p \not| m_i$, for any $1 \leq i \leq n$. As $(p, m_i) = 1$, based on Property (1) we have $(p, m_1 \cdots m_n) = 1$. Which is false, as $p|(m_1 \cdots m_n)$ and $p \geq 2$. Therefore, there exists $1 \leq i \leq n$ such that $p|m_i$.

Definition 2.2.13. [19] Given a natural number $n \geq 2$, we call a decomposition of $n$ any sequences $n_1, \ldots, n_k$ of length $k$, such that
$$n = n_1 \cdots n_k.$$  
The decomposition of a natural number $n \geq 2$ is not necessary unique, as any permutation of the factors can lead to new decomposition. Therefore, we assign the following properties to any decomposition

- $2 \leq n_1 < \cdots < n_k$, for some $k \geq 1$;
- $e_i > 0$ for any $1 \leq i \leq k$. 

13
such that
\[ n = n_1^{e_1} \cdots n_k^{e_k}. \]

If the numbers \( n_i \) are primes, for any \( 1 \leq i \leq k \), then the decomposition of \( n \) is called \textit{decomposition into prime factors}.

**Theorem 2.2.14.** [19] Any natural number \( n \geq 2 \) can be uniquely decomposed in prime factors.

**Proof.** We prove the theorem by considering the following aspects:

- there exists at least a decomposition into prime factors;
- and the decomposition is unique.

**Proof of existence:** Using the following Claim, we prove there exists a decomposition into prime numbers.

**Claim 1:** Any number has a prime divisor.

**Proof of Claim 1:** If \( n \) is prime, then the results of the claim easily follows.

As \( n \) is a composed number, let \( m \) be the smallest divisor of \( n \). We prove that \( m \) is a prime.

Assume that \( m \) is a composed number. Let \( l \) be a divisor of \( m \). Based on the Proposition 2.2.6, if \( l|m \) and \( m|n \), then \( l|n \). Therefore, \( m \) is a prime.

Based on Claim 1, there exists a prime \( p_1 \) such that
\[ n = p_1n_1. \]

Inductively, we prove that for any \( n_i \) there exists a decomposition
\[ n_i = p_{i+1}n_{i+1}. \]
where \( p_{i+1} \) is a prime divisor, for any \( i \geq 1 \). At each step \( n_{i+1} \leq n_i/2 \), as \( p_{i+1} \geq 2 \).

Therefore, the last divisor \( n_k \) must be 1, as for any other divisor Claim 1 is used
\[ n = p_1 \cdots p_k n_k. \]

**Proof of uniqueness:** We prove by contradiction. Assume there exists two decompositions into prime factors \( n = n_1^{e_1} \cdots n_s^{e_s} \) and \( n = q_1^{g_1} \cdots q_t^{g_t} \), where \( p_1 < \cdots < p_s \) and \( q_1 < \cdots < q_t \).

**Claim 2:** \( p_1 = q_1 \) and \( e_1 = g_1 \).

**Proof of Claim 2:** According to Corollary 2.2.12, for \( p_1|n \) there exits 1 \( \leq i \leq t \) such that \( p_1 = q_i \). Assume that \( i > 1 \). Similarly, as \( q_1|n \) there exists 1 \( \leq j \leq s \) such that \( q_1 = p_j \). Recall that \( q_1 < p_1 \) and \( p_1 < p_j \), for all 1 \( < j \leq t \). Our assumption that \( i > 1 \) is false. Therefore, \( i = 1 \) and \( p_1 = q_1 \).

Similarly, one obtains \( e_1 = g_1 \), as \( p_1 < p_j \) and \( q_1 < q_i \), for any 1 \( < j \leq s \) and any 1 \( < i \leq t \).
Inductively, one uses Claim 2 to prove that \( s = t \), \( p_i = q_i \) and \( e_i = g_i \), for all \( 1 \leq i \leq s \).

**Example 2.2.15.** Consider \( n = 19 \) and \( m = 2200 \). Note that \( n \) is prime. Consider the following decompositions for \( m \)
\[
2200 = 2 \cdot 11 \cdot 100 \\
= 2 \cdot 5 \cdot 11 \cdot 20 \\
= 2^3 \cdot 5^2 \cdot 11 .
\]

**Theorem 2.2.16.** [19] There are infinitely prime numbers.

**Proof.** Assume there exists a finite number of primes. Let \( p_1, p_2, \ldots, p_n \) be these primes with \( p_i < p_{i+1} \) for any \( 1 \leq i < n \). Let \( n = p_1 \cdots p_n + 1 \).

According to Theorem 2.2.14, \( n \) can be decomposed into prime factors. Let \( q \) be any of the prime numbers, such that \( q|n \). Furthermore, as the number of primes is finite, \( q \) divides the product of all the primes \( q|(p_1 \cdots p_n) \).

Based on Proposition 2.2.6, we have that \( q|1 \).

Therefore, our assumption is false, and there are infinitely prime numbers.

An increasing sequence \( p_1 < \cdots < p_n \) of prime numbers will be called a sequence of primes. If the primes are consecutive, then it will be called a sequence of consecutive primes. Furthermore, the length of the sequence of primes is \( n \).

Let \( p_1, p_2, \ldots \) stand for the infinite sequence of prime numbers.

Similar to prime numbers, an increasing sequence \( m_1 < \cdots < m_n \) of positive integers, where \( n \geq 1 \), is called a sequence of co-primes if \( (m_i, m_j) = 1 \) for any \( 0 \leq i, j \leq n \) with \( i \neq j \). Moreover, any sequence of primes is a sequence of co-primes.

### 2.2.3 Greatest common divisor

**Definition 2.2.17.** [19] Given \( a \) and \( b \) two integers, the greatest common divisor is the largest positive integer \( c \) that divides both \( a \) and \( b \).

The greatest common divisor is denoted by \( \gcd(a, b) \), for any \( a \) and \( b \). For simplicity, when there is no possibility of confusion it is also denoted by \( (a, b) \). Furthermore, the numbers \( m_1, \ldots, m_n \) are co-primes if and only if \( (m_1, \ldots, m_n) = 1 \).

**Proposition 2.2.18.** [19] Given \( m_1, \ldots, m_n \), for some \( n \geq 2 \), then

1. \( (0, m_1, \ldots, m_n) = (m_1, \ldots, m_n) \); 
2. \( (0, m_1) = |m_1|, \) if \( m_1 \neq 0 \); 
3. \( (m_1, m_2) = (m_2, m_1 \mod m_2), \) if \( m_2 \neq 0 \).
Proof. Property (1)-(2): Recall from Proposition 2.2.6 that \( m \) divides 0, for any \( m \geq 1 \). Therefore, the result easily follows.

Property (3): According to Theorem 2.2.5, there exists \( q \) and \( 0 \leq r < a_2 \) such that \( m_1 = qm_2 + r \). Let \( c = (m_1, m_2) \). As \( c|m_1 \), we have \( c|r \) and \( c|(m_2, r) \).

Let \((m_2, r) = d \). As \( m_1 = qm_2 + r \), we have \( d|m_1 \) and \( d|(m_1, m_2) \). Therefore, we have \( (m_1, m_2)|(m_2, r) \) and \((m_2, r)|(m_1, m_2) \). The result of the theorem follows.

\[ \Box \]

**Theorem 2.2.19.** [19] Let \( n \geq 2 \) and \( m_1, \ldots, m_n \in \mathbb{Z} \). Then, there exists \( \alpha_1, \ldots, \alpha_n \) such that

\[ (m_1, \ldots, m_n) = \alpha_1 m_1 + \cdots + \alpha_n m_n . \]

**Proof.** Let \( d = (m_1, \ldots, m_n) \). Compute \( m'_i = m_i / d \), for all \( 1 \leq i \leq n \). According to Theorem 2.2.11 over the elements \( m'_1, \ldots, m'_n \), the result follows.

\[ \Box \]

**Corollary 2.2.20.** [19] Let \( n \geq 2 \) and \( m_1, \ldots, m_n \in \mathbb{Z} \) with \( m_i \neq 0 \) for some \( 1 \leq i \leq n \). Then, for any \( b \in \mathbb{Z} \) the equation

\[ m_1 x_1 + \cdots + m_n x_n = b \quad (2.1) \]

with the unknowns \( x_1, \ldots, x_n \) admits solutions in \( \mathbb{Z} \) if and only if \((m_1, \ldots, m_n) \) divides \( b \).

**Proof.** Assume that the equation (2.1) has solutions in \( \mathbb{Z} \), and \( \alpha_1, \ldots, \alpha_n \) is one of these solutions. Any common divisor of \( m_1, \ldots, m_n \) is also a divisor of \( \alpha_1 m_1 + \cdots + \alpha_n m_n \). Therefore, \((m_1, \ldots, m_n)|b\).

Let \((m_1, \ldots, m_n) = d \). Conversely, assume that \( d|b \). So, there exists \( k \) and \( \alpha_1, \ldots, \alpha_n \) such that \( b = kd \) and \( \alpha_1 m_1 + \cdots + \alpha_n m_n = d \). Then, one can easily see that \( x_i = k \alpha_i \), for all \( 1 \leq i \leq n \), is a solution to (2.1).

\[ \Box \]

**Definition 2.2.21.** [19] Given \( a \) and \( b \), the least common multiple is the smallest positive integer \( c \) such that \( a|c \) and \( b|c \).

The least common multiple is denoted by \( \text{lcm}[a, b] \), for any \( a \) and \( b \). For simplicity, when there is no possibility of confusion it is also denoted by \([a, b]\).

**Theorem 2.2.22.** [19] Let \( a, b \) be two positive numbers. Then,

\[ ab = (a, b)[a, b] . \]

**Proof.** If \( a \) or \( b \) are 0, the result follows.

Consider now \( a \neq 0 \) and \( b \neq 0 \). Let \( d = (a, b) \). There exists \( a', b' \in \mathbb{Z} \) such that \( a = da' \) and \( b = db' \) with \((a', b') = 1 \).

From \( a|[a, b] \) and \( b'|[a, b] \), we have \( ab'|[a, b] \). Equivalent to \( da'b'|[a, b] \). As \( a|da'b' \) and \( b|da'b' \), we have \([a, b] = da'b' \) (Definition 2.2.21).

Therefore, the result is easily obtained.

\[ \Box \]
Example 2.2.23. Consider $a = 10$ and $b = 16$. Then, $(a, b) = 2$ and $[a, b] = 80$. Therefore,

$$160 = 2 \cdot 80.$$ 

2.2.4 The Euclidean Algorithm

In this subsection we present an algorithmic approach to computing the greatest common divisor of two numbers.

Let $0 \leq b \leq a$. Without loss of generality, consider that at least one number is different from 0.

Case 1: $a = b$ or $b = 0$. Then, $(a, b) = 0$.

Case 2: $0 < b < a$. Note that $(a, b) = (b, r)$, if there exist $q$ and $0 \leq r < b$ such that $a = b \cdot q + r$. (see Proposition 2.2.18) Therefore, one can repeat this process till the last remainder that is different from 0.

The above approach [19] is called the Euclidean Algorithm (see Algorithm 1) and consists of the following steps:

$$r_i = r_{i+1}q_{i+2} + r_{i+2}, \quad 0 < r_{i+2} < r_{i+1} \quad (2.2)$$

for all $-1 \leq i \leq n - 1$, where $r_{-1} = a$, $r_0 = b$ and $r_{n+2} = 0$.

Therefore,

$$(a, b) = (r_{-1}, r_0) = (r_0, r_1) = \cdots = (r_n, 0) = r_n.$$ 

**Algorithm 1:** The Euclidean Algorithm

```
input : a and b ;
output: (a, b);
begin
    while b ≠ 0 do
        compute t = b;
        compute b = a mod t;
        compute a = t ;
    end
    print The greatest common divisor is a;
end
```

Example 2.2.24. Euclidean Algorithm for $(10,5)$

Step 1: $5 \neq 0$, so $(10, 5) = (5, 0)$.

Step 2: $0 = 0$, so $(5, 0) = 5$. Therefore, $(10, 5) = 5$.

Euclidean Algorithm for $(7,13)$

Step 1: $13 \neq 0$, so $(7, 13) = (13, 7)$. 

17
Step 2: $7 \neq 0$, so $(13, 7) = (7, 6)$.
Step 3: $6 \neq 0$, so $(7, 6) = (6, 1)$.
Step 4: $1 \neq 0$, so $(6, 1) = (1, 0)$.
Step 5: $0 = 0$, so $(1, 0) = 1$. Therefore, $(7, 13) = 1$.

As we have seen in Theorem 2.2.19, the greatest common divisor of $a$ and $b$ can be expressed by a linear combination of them

$$(a, b) = \alpha a + \beta b,$$

for some $\alpha$ and $\beta$.

In Algorithm 1 at each step one can obtain a linear combination of the remainders involved. For each element $x$, we assign $V_x = (\alpha, \beta)$ such that $\alpha a + \beta b = x$.

Let $V_{r-1} = V_a = (1, 0)$ and $V_{r_0} = V_b = (0, 1)$. For $r_{i+2}$, we assign

$$V_{r_{i+2}} = V_{r_i} - q_i \cdot V_{r_{i+1}},$$

where $r_i, r_{i+1}, r_{i+2}$ and $q_i$ are as those in equation (2.2), for any $0 \leq i \leq n-2$.

This approach is called the extended Euclidean Algorithm (see Algorithm 2). For simplicity, we use $V_{r_i}$ in the algorithm, for all $-1 \leq i \leq n$.

---

**Algorithm 2:** The Extended Euclidean Algorithm

```
input : a and b ;
output: ax + by = (a, b) where V_{r_i} = (x, y) ;

begin
  compute $V_{r-1} = (1, 0)$ and $V_{r_0} = (0, 1)$;
  compute $i = -1$;
  while $b \neq 0$ do
    compute $q = a \div b$;
    compute $r_{i+2} = a \mod b$;
    compute $a = b$ and $b = r_{i+2}$ ;
    compute $V_{r_{i+2}} = V_{r_i} - q \cdot V_{r_{i+1}}$;
    compute $i = i + 1$ ;
  end
  print the coefficients are $V_{r_i}$;
end
```

---

**Example 2.2.25.** Extended Euclidean Algorithm for $(7, 13)$

Step 1: $V_7 = (0, 1)$ and $V_{13} = (0, 1)$.

Step 2: As $13 \neq 0$, we have $q = 0$ and $r_1 = 13$. So, $(7, 13) = (13, 7)$ and $V_{13} = V_7 - 0 \cdot V_7$.

Step 3: As $7 \neq 0$, we have $q = 1$, $r_2 = 6$. So, $(13, 7) = (7, 6)$ and $V_6 = V_{13} - 1 \cdot V_7 = (-1, 1)$. 

18
Chapter 2. Preliminaries

Step 4: As 6 \neq 0, we have q = 1, r_3 = 1. So, (7, 6) = (6, 1) and V_1 = V_7 - 1 \cdot V_6 = (2, -1).

Step 5: As 1 \neq 0, we have q = 6, r_4 = 0. So, (6, 1) = (1, 0) and V_0 = V_6 - 6 \cdot V_1 = (-13, 7).

Step 6: As 0 = 0, we have (1, 0) = 1 and V_1 = (2, -1).

Therefore, (7, 13) = 1, and 7 \cdot 2 - 1 \cdot 13 = 1.

2.2.5 Congruences

Definition 2.2.26. [19] Let m be a positive integer. Given a, b \in \mathbb{Z}, we define the congruence modulo m over \mathbb{Z}, denoted \equiv_m, by

\[ a \equiv_m b, \]

if and only if \( m \mid (a - b) \).

If a \equiv_m b, then we say that a and b are congruent modulo m, and denote this fact by a \equiv b \mod m. For simplicity, sometimes we use a = b \mod m.

Proposition 2.2.27. [19] Let a, b, c, d, m and m' be positive integers. Then, the following properties are satisfied:

1. if a \equiv_m b, then (a, m) = (b, m);
2. if a \equiv_m b and c \equiv_m d, then a + c \equiv_m b + d, a - c \equiv_m b - d and ac \equiv_m bd;
3. if ac \equiv_{mc} bc and c \neq 0, then a \equiv_m b;
4. if a \equiv_{mm'} b, then a \equiv_m b and a \equiv_{m'} b.

Proof. Property (1): As a \equiv_m b, according to Definition 2.2.26, we have m \mid (a - b). There exists a positive integer k such that a - b = km. Then,

\[ (a, m) = (b + km, m) = (b, m). \]

The last equality is based on Proposition 2.2.18.

Property (2): We prove only a + c \equiv_m b + d, as the rest are similar to this property. From a \equiv_m b and c \equiv_m d we have m \mid (a - b) and m \mid (c - d). Therefore, m \mid ((a + c) - (b + d)). According to Definition 2.2.26, we have a + c \equiv_m b + d.

Property (3): Using Definition 2.2.26, we have mc \mid (ac - bc). Let k exists such that ac - bc = mkc. As c \neq 0, one obtains a - b = mk. Therefore, the result follows.

Property (4): a \equiv_{mm'} b leads to mm' \mid (a - b). So, there exists k such that a - b = mm'k. According to Definition 2.2.26, we have m' \mid (a - b). □

Let \( \mathbb{Z}_m \) denote the set of all congruence classes modulo m, for some m \geq 1. Note that \( \mathbb{Z}_m = \{0, 1, \ldots, m - 1\} \).
2.2. Number Theory

Theorem 2.2.28. [65] Let \( m \) be a positive integer. Then, the congruence modulo \( m \) is

(1) reflexive: \( a \equiv a \mod m \) for any \( a \in \mathbb{Z} \);
(2) symmetric: if \( a \equiv b \mod m \), then \( b \equiv a \mod m \), for any \( a, b \in \mathbb{Z} \);
(3) transitive: if \( a \equiv b \mod m \) and \( b \equiv c \mod m \), then \( a \equiv c \mod m \), for any \( a, b, c \in \mathbb{Z} \);

Proof. The properties can easily be obtain from Proposition 2.2.27

Definition 2.2.29. [65] Let \( m \) be a positive integer. Given \( b \in \mathbb{Z}_m \), the multiplicative inverse \( 1/b \mod m \), denoted \( b^{-1} \), satisfies the following relation

\[ b \cdot b^{-1} = 1 \mod m . \]

Theorem 2.2.30. [65] Let \( m \) be a positive integer. Given \( b \in \mathbb{Z}_m \), the multiplicative inverse \( b^{-1} \mod m \) exists if and only if \( (b,m) = 1 \).

Proof. Assume that for a given \( b \) there exists \( b^{-1} \) such that \( b \cdot b^{-1} = 1 \mod m \). Let \( k \) exists such that \( b \cdot b^{-1} + km = 1 \). According to Corollary 2.2.20, \( (b,m)|1 \). Therefore, \( (b,m) = 1 \).

We prove now that there exists \( b^{-1} \). According to the extended Euclidean Algorithm 2, there exists \( \alpha, \beta \in \mathbb{Z} \) such that \( \alpha b + \beta m = 1 \). Therefore, \( \alpha b = 1 \mod m \). Consider \( b^{-1} = \alpha \mod m \), and the result follows.

2.2.6 Chinese Remainder Theorem

Theorem 2.2.31. [19] Let \( a, b, m \in \mathbb{Z} \) with \( m \geq 1 \). Then, the equation

\[ ax \equiv b \mod m \]  \hspace{1cm} (2.3)

is solvable in \( \mathbb{Z} \) if and only if \( (a,m)|b \). Moreover, if it is solvable, then it has exactly \( (a,m) \) solution in \( \mathbb{Z}_m \) which are of the form

\[ x_i = \left( x_0 + i \cdot \frac{m}{(a,m)} \right) \mod m \]

where \( x_0 \) is an arbitrary integer solution, and \( 0 \leq i \leq (a,m) \).

Proof. Consider Algorithm 3. Therefore, one obtains solution \( x_0 \) and the subsequent \( x_i \) solutions, for any \( 0 \leq i \leq (a,m) \).

Example 2.2.32. Consider the equation

\[ 3x = 6 \mod 9 . \]

Clearly \( x_0 = 2 \) is a solution. As \( (3,9) = 3 \), the equation admits the following solutions \( \{2, 5, 8\} \).
input : $a, b \in \mathbb{Z}$ and $m \geq 1$;
output: all solution modulo $m$ of $ax \equiv b \mod m$;
begin
compute $\gcd(a, m) := \alpha a + \beta b$;
if $\gcd(a, m)$ divides $b$ then
    $b' = b/\gcd(a, m)$;
    $x_0 = \alpha b'$;
    for $i=0$ to $\gcd(a, m) - 1$ do
        compute $x_i = (x_0 + i \cdot m/\gcd(a, m)) \mod m$ ;
        print $x_i$;
    end
end
print no integer solution available;
end

Algorithm 3: Solving linear congruential equations

Consider the equation

$3x = 5 \mod 9$.

As $(3, 9) = 3$ and $3 \nmid 5$, the equation has no solution.

Theorem 2.2.33 (CRT). [19] Given a finit non-empty set $I$ of positive integers and given the integers $b_i$ and $m_i$ for all $i \in I$, the Chinese Remainder Theorem states that the system of congruences

$$x \equiv b_i \mod m_i, \forall i \in I$$

has a unique solution modulo $\prod_{i \in I} m_i$, if $m_i$ and $m_j$ are co-prime for any $i, j \in I$ with $i \neq j$.

Proof. The above theorem states that given the system (2.4), there exists a single solution modulo $\prod_{i \in I} m_i$. Therefore, we prove the following aspects:

- there exists at least a solution for the system;
- and the uniqueness of the solution in $\mathbb{Z}\prod_{i \in I} m_i$.

Proof of existence: Let $M = \prod_{i \in I} m_i$ and $c_i = M/m_i$ for all $i \in I$. As $(m_i, m_j) = 1$, we can assume that $m_i$ and $c_i$ are co-prime, for all $i \neq j$.

According to Theorem 2.2.31, the following equation

$$c_i x \equiv b_i \mod m_i$$

admits solutions, for any $i \in I$. Let $x_i$ be one of those solutions.

One can easy note that

$$x = \sum_{i \in I} c_i x_i.$$
Therefore, \( x \mod M \) is a solution in \( \mathbb{Z}_M \).

Note that \( x_i \) can be viewed as \( x_i = b_i \cdot c_i^{-1} \mod m_i \). Thus, the solution of the system is
\[
x = \sum_{i \in I} b_i c_i (c_i^{-1} \mod m_i).
\]

**Proof of uniqueness:** Let \( x \) be a solution for the system (2.4). We prove, that for any other solution \( y \) of the system the following relation takes place
\[
x = y \mod M.
\]

As \( x \) is a solution to the system (2.4), then \( x \) is a solution to each of the following equations
\[
x = b_i \mod m_i \ \forall i \in I.
\]
Similarly, \( y \) is a solution to the same equations
\[
y = b_i \mod m_i \ \forall i \in I.
\]
Therefore,
\[
x = y \mod m_i \ \forall i \in I.
\]

As \( m_i \) and \( m_j \) are co-prime for any \( i,j \in I \) with \( i \neq j \), we can conclude that \( x = y \mod M \).

**Example 2.2.34.** Consider the following system
\[
\begin{align*}
x &= 3 \mod 5 \\
x &= 4 \mod 7 \\
x &= 5 \mod 9.
\end{align*}
\]
Let \( M = 5 \cdot 7 \cdot 9 = 315 \). Then,
\[
\begin{align*}
c_1^{-1} &= 63^{-1} = 3^{-1} = 2 \mod 5 \\
c_2^{-1} &= 45^{-1} = 3^{-1} = 5 \mod 7 \\
c_3^{-1} &= 35^{-1} = 8^{-1} = 8 \mod 9.
\end{align*}
\]
The solution is
\[
\begin{align*}
x &= 3 \cdot 63 \cdot 2 + 4 \cdot 45 \cdot 5 + 5 \cdot 35 \cdot 8 \mod 315 \\
&= 2678 \mod 315 = 158.
\end{align*}
\]
The previous theorem can be extended to the following variant.

**Corollary 2.2.35.** [19] Given a finit non-empty set \( I \) of positive integers and given the integers \( a_i, b_i \) and \( m_i \) such that \((a_i, m_i) = 1\), for all \( i \in I\), the following system of congruences
\[
a_i x \equiv b_i \mod m_i, \ \forall i \in I
\]
has a unique solution modulo \( \prod_{i \in I} m_i \), if \( m_i \) and \( m_j \) are co-prime for any \( i,j \in I \) with \( i \neq j \).
Proof. As \((a_i, m_i) = 1\), there exists \(a_i^{-1}\) mod \(m_i\) such that \(a_i \cdot a_i^{-1} \equiv 1\) mod \(m_i\), for all \(i \in I\). Therefore, the system (2.5) is equivalent to
\[
x \equiv a_i^{-1}b_i \text{ mod } m_i, \quad \forall i \in I.
\]
According to Theorem 2.2.33, the above system admits a unique solution modulo \(\prod_{i \in I} m_i\).

The following theorem was proposed by Ore [48] as an extension of the standard Chinese remainder theorem to deal with the case of moduli that are not relatively prime.

**Theorem 2.2.36.** [19] Given a finit non-empty set \(I\) of posible integers and given the integers \(b_i\) and \(m_i\) for all \(i \in I\), the following system of congruences
\[
x \equiv b_i \text{ mod } m_i, \quad \forall i \in I \tag{2.6}
\]
admits solutions if and only if \(b_i = b_j\) mod \((m_i, m_j)\) for all \(i, j \in I\) with \(i \neq j\). Moreover, the system has a unique solution modulo \(\text{lcm}[\prod_{i \in I} m_i]\).

**Proof.** For simplicity, we prove the theorem for the particular case \(|I| = 2\).

**Proof of existence:** Assume that the system (2.6) admits a solution \(x\). We prove that \(b_1 = b_2\) mod \((m_1, m_2)\).

As \(x\) is a solution to the system (2.6), we have
\[
x \equiv b_1 \text{ mod } m_1,
\]
\[
x \equiv b_2 \text{ mod } m_2.
\]
From the above equations, it follows that
\[
x \equiv b_1 \text{ mod } (m_1, m_2),
\]
\[
x \equiv b_2 \text{ mod } (m_1, m_2).
\]
Therefore,
\[
b_1 \equiv b_2 \text{ mod } (m_1, m_2).
\]

Now, we prove the converse. Assume that \(b_1 = b_2\) mod \((m_1, m_2)\). So, there exits \(c \in \mathbb{Z}^*\) such that \((b_1 - b_2) \cdot c = (m_1, m_2)\).

According to Theorem 2.2.31, the system
\[
x \equiv b_2 \text{ mod } m_2
\]
admits solutions that take the following form \(x = b_2 + y \cdot m_2\) for \(y \in \mathbb{Z}\).

System (2.6) admits solution if there exists \(y \in \mathbb{Z}\) such that
\[
b_2 + y \cdot m_2 \equiv b_1 \text{ mod } m_1.
\]
Equivalent to \(ym_2 = (b_1 - b_2) \text{ mod } m_1\).

For simplicity, let \(m_2 = m_2' \cdot (m_1, m_2)\) and \(m_1 = m_1' \cdot (m_1, m_2)\). As there exists \(c \in \mathbb{Z}\), according to Theorem 2.2.31, there exists \(y\) given by
\[
y = c(m_2')^{-1} \text{ mod } m_1'
\]
2.2. Number Theory

Proof of uniqueness: Assume that for the system (2.6), there exits two different solution \( x_1, x_2 \) modulo \([m_1, m_2]\) such that

\[
x_1 \neq x_2 \mod [m_1, m_2]
\]

As both solution must verify every equation of the system we have

\[
x_1 = x_2 \mod m_1 \quad x_1 = x_2 \mod m_2
\]

That implies \( x_1 \equiv x_2 \mod [m_1, m_2] \). Therefore, our assumption is false, and there exits only one solution for the system (2.6).

Theorem 2.2.37. [19] Let \( I \) be a finite non-empty set of positive integers, \( m_i \) for all \( i \in I \) a sequence of co-prime integers and \( f(x) \) a polynomial with integer coefficients. Then, \( a \in \mathbb{Z} \) is a solution for the system

\[
f(x) \equiv 0 \mod \prod_{i \in I} m_i
\]

if and only if \( b \) is a solution to every equation

\[
f(x) \equiv 0 \mod m_i, \quad \forall i \in I.
\]

Moreover, the number of solutions in \( \mathbb{Z} \prod_{i \in I} m_i \) for (2.7) is equal to the product of the number of equation in \( \mathbb{Z}_{m_i} \) for (2.8).

Proof. For simplicity, let \( M = \prod_{i \in I} m_i \).

Proof of existence: Assume \( b \) is a solution to the system (2.7). We prove that \( b \) is a solution for (2.8).

As \( b \) is a solution to (2.7), there exists \( c \in \mathbb{Z} \) such that \( f(b) = c \cdot M \). Equivalent to \( f(b) = c_i \cdot m_i \), where \( c_i = cM/m_i \). Therefore,

\[
f(b) \equiv 0 \mod m_i, \quad \forall i \in I.
\]

meaning, \( b \) is also a solution for the system (2.8).

We prove now the converse. Assume that \( b \) is a solution to the system (2.8). Based on Theorem 2.2.33, then \( b \) is also a solution for (2.7).

Proof of number of solutions: Based on the proof of existence, we have that \( b \) is a solution for (2.7) if and only if \( b \) is a solution for (2.8). Therefore, the result follows.

Theorem 2.2.38 (P1-CRT). [15] Let \( I \) be a finite non-empty set of positive integers and \( m_i \) for all \( i \in I \) a sequence of co-prime integers. Given the polynomials \( f_i(x) \in \mathbb{Z}_{m_i} \) for all \( i \in I \), there exists a unique polynomial \( f(x) \in \mathbb{Z} \prod_{i \in I} m_i \) such that

\[
f(x) \equiv f_i(x) \mod m_i, \quad \forall i \in I.
\]
Proof. Let \( t_i \) be the degree of polynomial \( f_i \) for all \( i \in I \). We artificially increase the degree of each polynomial to \( t \), where \( t = \max \{ t_i \mid \forall i \in I \} \). For each \( f_i = a_{i,t_i}x^{t_i} + \cdots + a_{i,1}x + a_{i,0} \), let

\[
\overline{f_i}(x) = \sum_{j=0}^{t} a_{i,j}x^j \mod m_i, \quad \forall i \in I,
\]

where \( a_{i,j} = 0 \) for all \( t_i < j \leq t \).

Let \( a_j \in \mathbb{Z}_{\prod_{i \in I} m_i} \) be the unique solution, obtained by CRT, over the system

\[
x = a_{i,j} \mod m_i, \quad \forall i \in I.
\]

Therefore, the polynomial \( f(x) = \sum_{i=0}^{t} a_i x^i \) is unique due to the uses of CRT.

\[\square\]

**Theorem 2.2.39** (P2-CRT). [24] Let \( I \) be a finite non-empty set of possible integers and \( m \geq 1 \) a positive integer. Given the polynomials \( f_i(x), m_i(x) \in \mathbb{Z}_m[x] \) for all \( i \in I \), there exists a unique polynomial \( f(x) \in \mathbb{Z}_{\prod_{i \in I} m_i(x)} \) such that

\[
f(x) \equiv f_i(x) \mod m_i(x), \quad \forall i \in I.
\]

**Proof.** We adapt the proof of Theorem 2.2.33, with the following differences:

- replace \( M \) with \( M(x) = \prod_{i \in I} m_i(x) \);
- substitute \( c_i \) with \( c_i = M(x)/m_i(x) \);
- and compute the solution \( f(x) = \sum_{i \in I} f_i(x)c_i(x)(c_i^{-1}(x) \mod m_i(x)) \mod M(x) \).

\[\square\]

### 2.2.7 Chinese Remainder Algorithm

Given a finite non-empty set \( I \) of possible integers and given the integers \( b_i \) and \( m_i \) for all \( i \in I \), consider the following system of congruences

\[
x \equiv b_i \mod m_i, \quad \forall i \in I
\]

(2.10)

If the integers \( m_i \), for all \( i \in I \), are pairwise co-prime, then a method for computing the solution is given in Algorithm 4 [24]. Otherwise, a generalized approach is given in Algorithm 5 [24].

Note that for finding the elements \( c_i \), for all \( i \in I \), the extended Euclidian Algorithm was used.
2.2. Number Theory

The system (2.10) with \((m_i, m_j) = 1, \forall i, j \in I\) with \(i \neq j\); find the unique solution \(x\) modulo \(\prod_{i \in I} m_i\).

**Algorithm 4:** The non-iterative Ore CRA

```plaintext
input : the system (2.10) with \((m_i, m_j) = 1, \forall i, j \in I\) with \(i \neq j\);
output: the unique solution \(x\) modulo \(\prod_{i \in I} m_i\);
begin
    compute \(M = \prod_{i \in I} m_i\);
    compute \(x = 0\);
    for each \(i\) in \(I\) do
        compute \(M_i = M/m_i\);
        compute \(c_i = M_i^{-1} \mod m_i\);
        compute \(x = x + b_i c_i M_i\);
    end
    print the solution \(x\);
end
```

**Algorithm 5:** The generalized Ore CRA

```plaintext
input : system (2.10) with \(b_i = b_j \mod (m_i, m_j), \forall i, j \in I\) with \(i \neq j\);
output: the unique solution \(x\) modulo \([m_i | i \in I]\);
begin
    compute \(M = [m_i | i \in I]\);
    compute \(x = 0\);
    for each \(i\) in \(I\) do
        compute \(M_i = M/m_i\);
    end
    compute \(c_i\) for all \(i\) in \(I\) such that \(\sum_{i \in I} c_i M_i = 1\);
    for each \(i\) in \(I\) do
        compute \(x = x + b_i c_i M_i\);
    end
    print the solution \(x\);
end
```
2.2.8 Complexity

When one describes an algorithm two things must be taken into consideration: correctness (the result is the one desired) and complexity (the efficiency of the operations used). In this thesis we are only interested in the dominant factor of the complexity of an algorithm, focusing on the estimation of the algorithm’s running time. This is called an asymptotic analysis, which is usually discussed in terms of the $O$ notation.

Given a function $f$ from the set of positive integers $\mathbb{N}$ into the set of positive real numbers $\mathbb{R}_+$, denote by $O(f)$ the set

$O(f) = \{g : \mathbb{N} \rightarrow \mathbb{R}_+ | (\exists c > 0)(\exists n_0 \in \mathbb{N})(\forall n \geq n_0)(g(n) \leq cf(n))\}$.

2.3 Information Theory

2.3.1 Probability

Consider the following experiment: the throw of a dice. There are 6 possible outcomes $\{1, 2, 3, 4, 5, 6\}$, each corresponding to one of the faces of the dice. Let $w_i$ be the element (or outcome) that signifies “face $i$”. Then, $\Omega = \{w_1, \ldots, w_6\}$ is the finite space of elements associated to the rolling of a dice. Any subset $A \subseteq \Omega$ is called an event. Furthermore, let $\phi$ be the the impossible event and $\Omega$ be the certain event.

Definition 2.3.1. [32] A probability measure over $\Omega$ is a function $P : \mathcal{P}(\Omega) \rightarrow [0, 1]$, that satisfies:

- $P(\Omega) = 1$,
- and $P(A \cup B) = P(A) + P(B)$, $\forall A, B \subseteq \Omega$ with $A \cap B = \phi$.

From now on, $(\Omega, P)$ will be called a (finite) space of probabilities.

Proposition 2.3.2. [32] Let $(\Omega, P)$ be a (finite) space of probabilities. Given $A, B \subseteq \Omega$, the following properties hold

1. $P(\emptyset) = 0$;
2. $P(A) \geq 0$;
3. $P(\overline{A}) = 1 - P(A)$;
4. $P(A) \leq P(B)$ if $A \subset B$;
5. $P(A/B) = P(A) - P(A \cap B)$;
6. $P(A \cup B) = P(A) + P(B) + P(A \cap B)$.
2.3. Information Theory

Proof. For simplicity, as each property is proven using Definition 2.3.1, we do not use the phrase “according to Definition 2.3.1” in each proof.

Property (1): As \( \Omega \cup \emptyset = \Omega \) and \( \Omega \cap \emptyset = \emptyset \), we have
\[
P(\Omega \cup \emptyset) = P(\Omega) + P(\emptyset)
\]
Therefore, the result easily follows.

Property (2): Using Definition 2.3.1, the property is trivial.

Property (3): Let \( A \subseteq \Omega \), and \( \overline{A} = \Omega - A \). Therefore,
\[
P(\Omega) = P(A) + P(\overline{A})
\]
Equivalent to \( P(\overline{A}) = 1 - P(A) \).

Property (4): As \( A \subseteq B \), let \( C \subseteq \Omega \) such that \( A \cup C = B \). Therefore,
\[
P(B) = P(A) + P(C)
\]
Based on property (2), the result follows.

Property (5): Let \( C, D \subseteq \Omega \) such that \( A \cap B = C \) and \( A = C \cup D \). As \( A/B = D \), we have
\[
P(A) = P(C) + P(D)
\]
Equivalent to \( P(D) = P(A) - P(C) \).

Property (6): Note that \( A \cup B = A \cup (B/A) \). As \( A \cap (B/A) = \emptyset \), we have
\[
P(A \cup B) = P(A) + P(B/A)
\]
Using property (5) for \( P(B - A) = P(B) - P(B \cap A) \), the result is obtained.

Definition 2.3.3. [32] Let \( \Omega = \{w_1, \ldots, w_n\} \) be a (finite) space of elements. A probability distribution over \( \Omega \) is a function \( p: \Omega \rightarrow [0,1] \) with
\[
\sum_{w \in \Omega} p(w) = 1
\]
One may notice there exits a correlation between a probability distribution and a probability measure over the same space of elements \( \Omega \).

Theorem 2.3.4. [20, 18] Let \( \Omega \) be a (finite) space of elements. For any \( a \in \Omega \), let
\[
P(\{a\}) = p(a)
\] (2.11)
Then, \( P \) induces a probability measure over \( \Omega \) if and only if \( p \) induces a probability distribution over \( \Omega \).

Proof. The proof is based on relation (2.11).

Therefore, \((\Omega, p)\) is also a (finite) space of probabilities.
Chapter 2. Preliminaries

Independent events

Definition 2.3.5. [32, 42] Let $(\Omega, P)$ be a (finite) space of probabilities. Given $A, B \subseteq \Omega$, $A$ and $B$ are independent events if

$$P(A \cap B) = P(A) \cdot P(B).$$

Definition 2.3.6. [42] Two events $A$ and $B$ are mutually exclusive if their intersection is empty

$$A \cap B = \emptyset.$$

Example 2.3.7. Consider a drawer that has only five socks, each of a different color: blue, brown, red, white and black. After we extract a sock we return it to the drawer. The probability of extracting two red socks is

$$P(\text{red and red}) = P(\text{red}) \cdot P(\text{red}),$$

which is $1/25$.

The events considered in example 2.3.7, are not mutually exclusive.

Example 2.3.8. Consider a deck of cards, without Jokers. There are 52 cards in the deck with 4 of each kind. After we extract a card we return it to the deck. The probability of extracting jack and 10 is

$$P(\text{jack and 8}) = P(\text{jack}) \cdot P(8),$$

which is $1/169$.

The events considered in example 2.3.8, are mutually exclusive.

Proposition 2.3.9. [20, 18] Let $(\Omega, P)$ be a (finite) space of probabilities, and $A \subseteq \Omega$ an event. The following properties hold

(1) $A$ and $\emptyset$ are independent events;

(2) $A$ and $\Omega$ are independent events.

Proof. We prove each property using Definition 2.3.5.

Property (1): As $A \cap \emptyset = \emptyset$, we have $P(A \cap \emptyset) = P(\emptyset) = 0$. Moreover, $P(A) \cdot P(\emptyset) = 0$. Therefore, the result follows.

Property (2): As $A \cap \Omega = A$, we have $P(A \cap \Omega) = P(A)$. Furthermore, $P(A) \cdot P(\Omega) = P(A)$. Therefore,

$$P(A \cap \Omega) = P(A) \cdot P(\Omega).$$

□
Theorem 2.3.10. [20, 18] There exists finite probability spaces where independent events are not necessarily mutually exclusive.

Proof. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities, and \(A, B \subseteq \Omega\) such that \(A \cap B = x\) with \(x \neq \emptyset\). For simplicity, let \(A = a \cup x\) and \(B = b \cup x\) with \(a \cap b = \emptyset\). Therefore, \(P(A \cap B) = P(x)\) and \(P(A) = P(a) + P(x)\), and \(P(B) = P(b) + P(x)\).

Using Definition 2.3.5, we have

\[
P(A \cap B) = P(A) \cdot P(B) = (P(a) + P(x)) \cdot (P(b) + P(x)).
\]

Equivalent to the following equation in \(P(x)\):

\[
P(x)^2 + (P(a) + P(b) - 1)P(x) + P(a)P(b) = 0.
\]

For the equation to admit real solutions, we must have

\[
\Delta_1 = (P(a) + P(b) - 1)^2 - 4P(a)P(b) \geq 0. \tag{2.12}
\]

Treating (2.12) as an equation in \(P(a)\), one obtains

\[
\Delta_2 = (P(b) + 1)^2 - 4(P(b)^2 - 2P(b) + 1) = 4P(b).
\]

The solutions for \(\Delta_2\) are \(P(a) = (\sqrt{P(b)} - 1)^2\) and \(P(a) = (\sqrt{P(b)} + 1)^2\).

For \(0 \leq P(a) \leq (\sqrt{P(b)} - 1)^2\), one obtains \(\Delta_1 \geq 0\). Therefore, there are independent events that are not mutually exclusive.

Example 2.3.11. Consider a drawer with only four socks, each of a different color: red, blue, green and yellow. After we extract a sock we return it to the drawer. Let \(A = \{\text{red, blue}\}\) be the event in which the red and blue sock were extracted from the drawer. The red sock was extracted, and return to the drawer. Then, the blue sock was extracted. Therefore, the probability of \(A\) is 1/2. Similarly, let \(B = \{\text{blue, green}\}\) be the event in which the blue and green sock were extracted.

Let \(x = \text{blue}, a = \text{red}\) and \(b = \text{green}\). Based on Theorem 2.3.10, we have

\[
\frac{1}{4} = P(a) \leq (\sqrt{P(b)} - 1)^2 = \frac{1}{4}.
\]

Then, the events are independent.

One can easily check this fact by computing \(P(A \cap B)\) and \(P(A) \cdot P(B)\).

Proposition 2.3.12. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities, and \(A, B \subseteq \Omega\) two independent events. The following properties hold:

1. \(A\) and \(B\) are independent events;
2. \(A\) and \(\overline{B}\) are independent events;
3. \(\overline{A}\) and \(B\) are independent events.
Chapter 2. Preliminaries

Proof. As $A$ and $B$ are independent, we have $P(A \cap B) = P(A) \cdot P(B)$.

Property (1): Remark that $A \cap B = (\Omega/A) \cap B = B/A$. Therefore, $P(\overline{A} \cap B) = P(B/A)$. Using Proposition 2.3.2 we obtain

$$P(\overline{A}) \cdot P(B) = (1 - P(A)) \cdot P(B)$$
$$= P(B) - P(A) \cdot P(B)$$
$$= P(B) - P(B \cup A)$$
$$= P(B/A) .$$

The result follows.

Property (2): As $A \cap B = A \cap (\Omega/B) = A/B$, we have $P(A \cap B) = P(A/B)$. From Proposition 2.3.2 we obtain

$$P(A) \cdot P(\overline{B}) = P(A) \cdot (1 - P(B))$$
$$= P(A) - P(A) \cdot P(B)$$
$$= P(A) - P(A \cup B)$$
$$= P(A/B) .$$

The result follows.

Property (3): From $\overline{A} \cap \overline{B} = (\Omega/A) \cap (\Omega/B) = \Omega/(A \cup B)$, we have $P(\overline{A} \cap \overline{B}) = P(\Omega/(A \cup B)) = 1 - P(A \cup B)$. According to Proposition 2.3.2, we obtain

$$P(\overline{A}) \cdot P(\overline{B}) = (1 - P(A)) \cdot (1 - P(B))$$
$$= 1 - P(A) - P(B) + P(A) \cdot P(B)$$
$$= 1 - (P(A) + P(B) - P(A) \cdot P(B))$$
$$= 1 - P(A \cup B) .$$

The result follows. □

Conditional Probability

Definition 2.3.13. [32] Let $(\Omega, P)$ be a (finite) space of probabilities. Given $A, B \subseteq \Omega$ with $P(B) > 0$, the conditional probability of $A$ given $B$, denoted $P(A \mid B)$, is

$$P(A \mid B) = \frac{P(A \cup B)}{P(B)} .$$

If event $B$ does not take place ($P(B) = 0$), then one can not talk about the conditional probability of obtaining $A$ given $B$.

Proposition 2.3.14 (Bayes Formula). [32] Let $(\Omega, P)$ be a (finite) space of probabilities. Given $A, B \subseteq \Omega$ with $P(A) \cdot P(B) > 0$, then the following
property holds
\[ P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}. \]

**Example 2.3.15.** Let \( \Omega = \{1, 2, 3, 4, 5, 6\} \) be the possible outcomes of throwing a dice. Given the events \( A = \{2, 3\} \) and \( B = \{3, 4, 5\} \), the conditional probability of \( A \) given \( B \) is
\[ P(A \mid B) = \frac{P(A \cup B)}{P(B)} = \frac{\frac{5}{6}}{\frac{3}{6}} = \frac{1}{3}. \]

Similarly, \( P(B \mid A) = 1/2 \). Thus, one may check the values involved in the Bayes formula
\[ P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}. \]

**Proposition 2.3.16.** [32, 42] Let \( (\Omega, P) \) be a (finite) space of probabilities. Given \( A, B, C \subseteq \Omega \) with \( P(A) \cdot P(B) \cdot P(C) > 0 \), then the following properties hold
\[ (1) A \text{ and } B \text{ are independent events if and only if } P(A \mid B) = P(A); \]
\[ (2) P(A \mid B) = P(A) \text{ if and only if } P(B \mid A) = P(B); \]
\[ (3) P(A \cap B \cap C) = P(A \mid (B \cap C)) \cdot P(B \mid C) \cdot P(C); \]
\[ (4) H_1, \ldots, H_n \text{ partition of } \Omega, \text{ then } P(A) = \sum_{i=1}^{n} P(A \mid H_i) \cdot P(H_i). \]

**Proof.** We prove each property.

Property (1): We prove the direct implication. Assume \( A \) and \( B \) are independent events with \( P(B) > 0 \). From Definition 2.3.5, we have \( P(A \cap B) = P(A) \cdot P(B) \). Therefore, the conditional probability is
\[ P(A \mid B) = \frac{P(A \cup B)}{P(B)} = \frac{P(A) \cdot P(B)}{P(B)} = P(A). \]

We prove the converse. Assume \( P(A \mid B) = P(A) \). According to Definition 2.3.13, we have
\[ P(A \mid B) = \frac{P(A \cup B)}{P(B)} = \frac{P(A) \cdot P(B)}{P(B)} = P(A). \]

The result follows.

Property (2): Assume \( P(A \mid B) = P(A) \). Using Bayes Formula, we have
\[ P(B \mid A) = \frac{P(A \mid B) \cdot P(B)}{P(A)} = \frac{P(A) \cdot P(B)}{P(A)} = P(B). \]

Conversely, assume \( P(B \mid A) = P(B) \). From Bayes Formula, we have
\[ P(A \mid B) = \frac{P(A \mid B) \cdot P(A)}{P(B)} = \frac{P(B) \cdot P(A)}{P(B)} = P(A). \]
The result follows.

Property (3): The conditional probability of $A$ given by $B \cap C$ is

$$P(A \mid (B \cap C)) = \frac{P(A \cap B \cap C)}{P(B \cap C)}.$$ 

Moreover, the conditional probability of $C$ given by $B$ is

$$P(B \mid C) = \frac{P(B \cap C)}{P(C)}.$$ 

According to the above relations, the result follows.

Property (4): The conditional probability of $A$ given by $H_i$ is

$$P(A \mid H_i) = \frac{P(A \cap H_i)}{P(H_i)}.$$ 

Therefore,

$$P(A \mid H_i) \cdot P(H_i) = P(A \cap H_i).$$

As $H_1, \ldots, H_n$ are a partition of $\Omega$, we have $(A \cap H_i) \cap (A \cap H_j) = \emptyset$ for any $1 \leq i < j \leq n$. According to Proposition 2.3.2, we have

$$\sum_{i=1}^{n} P(A \cap H_i) = P \left( A \cap \bigcup_{i=1}^{n} H_i \right) = P(A \cap \Omega) = P(A).$$

Random variables

**Definition 2.3.17.** [34, 32, 42] Let $(\Omega, P)$ be a (finite) space of probabilities and $V$ a finite set of values. A random variable is a function $X : \Omega \to V$ from the set of all finite elements $\Omega$ to the set of values $V$, such that for any element $a \in V$ there exists an event $A \subseteq \Omega$ with

$$X(A) = a.$$ 

Furthermore, $X^{-1}(a) \in \Omega$ for any $a \in V$.

The probability of $x \in V$ is given by the probability of all the outcomes in $w \in \Omega$ with $X(w) = x$. Therefore,

$$P(X = x) = P(X^{-1}(\{x\})) = P(\{w \in \Omega \mid X(w) = x\}).$$

**Example 2.3.18.** Let $\Omega = \{1, 2, 3, 4, 5, 6\}$ be the possible outcomes of throwing a dice. Consider $X$ the random variable that takes the value 1 if the outcome is odd and the value 2 if the outcome is even, and $Y$ that takes the value 0 for outcomes $\{1, 2\}$ and 1 for outcomes $\{3, 4, 5, 6\}$. Then, $V_X = \{1, 2\}$, $V_Y = \{0, 1\}$ and

$$P(X = 1) = \frac{1}{2}, P(X = 2) = \frac{1}{2},$$

$$P(Y = 0) = \frac{1}{3}, P(Y = 1) = \frac{2}{3}.$$
2.3. Information Theory

**Definition 2.3.19.** [34] Let \((\Omega, P)\) be a (finite) space of probabilities with \(X : \Omega \to V\) a random variable and \(a \in V\) an arbitrary value. The random variable with values greater than \(a\), denoted \(X \geq a\), is the set of all the outcomes \(w \in \Omega\) with \(X(w) \geq a\).

Let \((\Omega, P)\) be a (finite) space of probabilities and \(X : \Omega \to V\) a random variable. The random variable with values (strict) lesser than \(a \in V\), denoted \(X < a\), is defined similar to \(X \geq a\) by the set all the outcomes \(w \in \Omega\) with \(X(w) < a\).

From a probabilistic point of view we have

\[
P(X \geq a) = \sum_{b \in V, b \geq a} P(X = b)
\]

\[
P(X < a) = \sum_{b \in V, b < a} P(X = b).
\]

**Example 2.3.20.** Let \(\Omega = \{1, 2, 3, 4, 5, 6\}\) be the possible outcomes of throwing a dice, and \(X\) the random variable associated to the outcomes. Then, \(V = \{1, 2, 3, 4, 5, 6\}\) and

\[
P(X \geq 4) = P(X = 4) + P(X = 5) + P(X = 6) = \frac{1}{2}
\]

\[
P(X < 4) = P(X = 1) + P(X = 2) + P(X = 3) = \frac{1}{2}.
\]

**Proposition 2.3.21.** [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities with \(X : \Omega \to V\) a random variable. Then,

\[
P(X < a) + P(X \geq a) = 1,
\]

for any \(a \in V\).

**Proof.** According to Definition 2.3.17 and 2.3.19, we have

\[
P(X < a) + P(X \geq a) = \sum_{b \in V, b < a} P(X = b) + \sum_{b \in V, b \geq a} P(X = b)
\]

\[
= \sum_{b \in V} P(X = b)
\]

\[
= \sum_{b \in V} P(\{w \in \Omega \mid X(w) = b\})
\]

\[
= P(\bigcup_{b \in V} \{w \in \Omega \mid X(w) = b\})
\]

\[
= P(\Omega)
\]

\[
= 1.
\]

\(\Box\)
2.3.2 Entropy

The entropy of a random variable measures the uncertainty level concerning the values of the random variable. When the probability of a random variable is 0 or 1, the uncertainty level is 0.

**Definition 2.3.22.** [17] Let \((\Omega, P)\) be a (finite) space of probabilities and \(X\) a random variable over the set \(V\). The entropy of \(X\), denoted \(H(X)\), is defined by:

\[
H(X) = - \sum_{x \in V} P(X = x) \log P(X = x).
\]

**Proposition 2.3.23** (Gibbs inequality). [20, 18] Let \(0 \leq p_i, q_i \leq 1\) with \(\sum_{i=1}^n p_i = 1\) and \(\sum_{i=1}^n q_i \leq 1\), for all \(1 \leq i \leq n\) and some \(n \geq 1\). Given \(b > 1\), then

\[
\sum_{i=1}^n p_i \log_b \frac{1}{p_i} \leq \sum_{i=1}^n p_i \log_b \frac{1}{q_i}.
\]

**Proof.** As \(\log_b x \leq x - 1\) (equal if \(x = 1\)), we have

\[
\log_b \frac{q_i}{p_i} \leq \frac{q_i}{p_i} - 1
\]

for any \(1 \leq i \leq n\) with \(p_i \neq 0\).

Thus, one obtains

\[
p_i \left( \log_b \frac{1}{p_i} - \log_b \frac{1}{q_i} \right) \leq q_i - p_i
\]

\[
p_i \log_b \frac{1}{p_i} \leq p_i \log_b \frac{1}{q_i} + (q_i - p_i),
\]

for any \(1 \leq i \leq n\). Note that the above relations hold, even for \(p_i = 0\).

Applying the sum after \(i\), we have

\[
\sum_{i=1}^n p_i \log_b \frac{1}{p_i} \leq \sum_{i=1}^n p_i \log_b \frac{1}{q_i} + \sum_{i=1}^n (q_i - p_i).
\]

As \(\sum_{i=1}^n (q_i - p_i) \leq 0\), the result easily follows.

Furthermore, the equality is obtained when \(p_i = q_i\), for any \(1 \leq i \leq n\).

**Proposition 2.3.24.** [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities and \(X\) a random variable over the set \(V\). Then, the following properties hold

1. \(0 \leq H(X) \leq \log |V|\);
2. \(H(X) = 0\) if and only if there exists \(x \in V\) such that \(P(X = x) = 1\);
3. \(H(X) = \log |V|\) if and only if \(P(X = x) = 1/|V|\) for any \(x \in V\).
2.3. Information Theory

Proof. Property (1) follows directly from the Gibbs inequality, where \( p_i = P(X = x) \) for any \( x \in V \) and \( q_i = 1/|V| \).

Property (2): According to Definition 2.3.22, \( H(X) = 0 \) if and only if \( P(X = x) \log \left(1/P(X = x)\right) = 0 \) for any \( x \in V \). Therefore, the result follows.

Property (3): According to the Gibbs inequality from Property (1), the equality is satisfied if \( p_i = q_i \). Thus, \( P(X = x) = 1/|V| \).

Joint entropy

The definition for the entropy of a single random variable, can be extended to a pair of random variables. Before we can discuss the joint entropy, we must first prove that the random variables induce a probability distribution.

Proposition 2.3.25. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities, and \( X, Y \) two random variables with \( X : \Omega \rightarrow V_1 \) and \( Y : \Omega \rightarrow V_2 \). Then,

\[
\sum_{x \in V_1, y \in V_2} P(X = x, Y = y) = 1.
\]

Proof. Starting from the left side of the relation above we have:

\[
\sum_{x \in V_1, y \in V_2} P(X = x, Y = y) = \sum_{x \in V_1} \sum_{y \in V_2} P(X = x, Y = y) = \sum_{x \in V_1} \sum_{y \in V_2} P(X^{-1}\{x\} \cap Y^{-1}\{y\}) .
\]

As the sets \( X^{-1}\{x\} \cap Y^{-1}\{y_1\} \) and \( X^{-1}\{x\} \cap Y^{-1}\{y_2\} \) are disjoint for \( y_1 \neq y_2 \), the above sum becomes:

\[
\sum_{x \in V_1, y \in V_2} P(X = x, Y = y) = \sum_{x \in V_1} P(X^{-1}\{x\} \cap \bigcup_{y \in V_2} Y^{-1}\{y\})
\]

Using the fact that \( \Omega = \bigcup_{y \in V_2} Y^{-1}\{y\} \), we have:

\[
\sum_{x \in V_1, y \in V_2} P(X = x, Y = y) = \sum_{x \in V_1} P(X^{-1}\{x\} \cap \Omega) = \sum_{x \in V_1} P(X^{-1}\{x\}).
\]

As \( \sum_{x \in V_1} P(X^{-1}\{x\}) = 1 \), the joint variables induce a probability distribution.

Definition 2.3.26. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities, and \( X, Y \) two random variables with \( X : \Omega \rightarrow V_1 \) and \( Y : \Omega \rightarrow V_2 \). The joint entropy \( H(X,Y) \) is defined as:

\[
H(X,Y) = - \sum_{x \in V_1, y \in V_2} P(X = x, Y = y) \log P(X = x, Y = y).
\]
Lemma 2.3.27. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities and \(X, Y\) two random variables over the sets \(V_1\) and \(V_2\). Given \(x \in V_1\) an arbitrary point, then
\[
\sum_{y \in V_2} P(X = x, Y = y) = P(X = x).
\]

Proof. Using the same line of proof given in Proposition 2.3.25 for the probability distribution of the joint entropy, we have
\[
\sum_{y \in V_2} P(X = x, Y = y) = \sum_{y \in V_2} P(X^{-1}\{x\}, Y^{-1}\{y\})
\]
\[
= P(X^{-1}\{x\} \cap (\bigcup_{y \in V_2} Y^{-1}\{y\}))
\]
\[
= P(X^{-1}\{x\}).
\]

Therefore, the result follows. \(\square\)

Conditional entropy

Based on the discussion for the joint entropy, we can define the conditional entropy of a random variable given another random variable.

Definition 2.3.28. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities and \(X, Y\) two random variables over the sets \(V_1\) and \(V_2\). The conditional entropy of \(X\) given an arbitrary \(y \in V_2\) is:
\[
H(X | Y = y) = \sum_{x \in V_1} P(X = x | Y = y) \log \frac{1}{P(X = x | Y = y)}.
\]

Definition 2.3.29. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities, and \(X, Y\) two random variables over the sets \(V_1\) and \(V_2\). The conditional entropy of \(X\) given \(Y\) is
\[
H(X | Y) = \sum_{y \in V_2} P(Y = y) H(X | Y = y).
\]

Proposition 2.3.30. [20, 18] Let \((\Omega, P)\) be a (finite) space of probabilities, and \(X, Y\) two random variables over the sets \(V_1\) and \(V_2\). The conditional entropy satisfies the following properties:

1. \(H(X | Y) \geq 0;\)
2. \(H(X | X) = 0;\)
3. \(H(X | Y) = \sum_{x \in V_1, y \in V_2} P(X = x, Y = y) \log \frac{P(Y = y)}{P(X = x, Y = y)};\)
4. \(H(X | Y) = H(X, Y) - H(Y);\)
5. \(H(X, Y | Z) = H(X | Y, Z) + H(Y | Z);\)
6. \(H(X, Y | Z) = H(X, Y | Z) + H(X | Z).\)
Proof. Properties (1)-(2), result directly from using Definition 2.3.28 and 2.3.29.

Property (3): The conditional entropy of $X$ given by $Y$ is

$$H(X \mid Y) = \sum_{y \in V_2} P(Y = y) H(X \mid Y = y)$$

$$= \sum_{y \in V_2} P(Y = y) \left( \sum_{x \in V_1} P(X = x \mid Y = y) \log \frac{1}{P(X = x \mid Y = y)} \right)$$

$$= \sum_{x \in V_1, y \in V_2} P(Y = y) P(X = x \mid Y = y) \log \frac{1}{P(X = x \mid Y = y)} .$$

As $P(X = x \mid Y = y) = P(X = x, Y = y)P(Y = y)$, the result follows.

Property (4): Using Property (3), we have

$$H(X \mid Y) = \sum_{x \in V_1, y \in V_2} P(X = x, Y = y) \log \frac{P(Y = y)}{P(X = x, Y = y)}$$

As

$$\log \frac{P(Y = y)}{P(X = x, Y = y)} = \log P(Y = y) + \log \frac{1}{P(X = x, Y = y)} ,$$

we have:

$$H(X \mid Y) = \sum_{x \in V_1, y \in V_2} P(X = x, Y = y) \log \frac{1}{P(X = x, Y = y)}$$

$$+ \sum_{x \in V_1, y \in V_2} P(X = x, Y = y) \log P(Y = y)$$

$$= H(X, Y) + \sum_{x \in V_1, y \in V_2} P(X = x, Y = y) \log P(Y = y)$$

$$= H(X, Y) - \sum_{y \in V_2} P(Y = y) \log \frac{1}{P(Y = y)} .$$

Therefore, $H(X \mid Y) = H(X, Y) - H(Y)$.

Property (5): From Property (4), we have

$$H(X, Y \mid Z) = H(X, Y, Z) - H(Y, Z)$$

$$H(X \mid Y, Z) = H(X, Y, Z) - H(Z) .$$

Equivalent to

$$H(X, Y \mid Z) + H(Y, Z) = H(X \mid Y, Z) + H(Z) .$$

Using Property (4) again for $H(Y \mid Z) = H(Y, Z) - H(Z)$, the result follows.

Property (6): Following a method similar to Property (5), we obtain the same result. $\square$
Chapter 3

Secret Sharing Schemes

3.1 Introduction

Secret sharing schemes are methods of splitting information (usually a cryptographic key) to a group of participants such that an authorized group\(^1\) of participants can recover uniquely the information. Introduced as method to store critical information, secret sharing schemes have extended their applicability to several other applications: Byzantine agreement\([52, 50]\), secure multiparty computation\([7, 16, 50, 35]\), threshold cryptography\([22, 30, 35]\), access control\([47]\), attribute-based encryption\([31]\), generalized oblivious transfer\([61]\), authenticated group key transfer protocol\([33]\), visual cryptography\([57, 37]\). In what follows we provide a brief introduction to some of them.

\(^1\) An authorized group consists of a sufficient number of participants such that the recovery of information is possible, whereas an unauthorized group of participants do not ideally obtain even a part of the information. More details are available in the next section.
Authenticated Group Key Transfer Protocol [33] In authenticated group key transfer protocol the communication between participants of the same group is established by a common secret key that ensures the confidentiality and authentication of the message. That is, no message can be read by any other than the intended receiver. Moreover, any message can not be altered during communication and can be traced to a specific sender.

Considering secret sharing schemes, there are two known approaches in group key transfer protocols: key predistribution scheme with offline trusted authority, and key generation center with online trusted authority. In a key predistribution scheme, at each initialization the trusted authority becomes online and distributes shares to all the participants from a certain group. For the recovery process, any authorized set of participants combine their shares to restore the common key. The main drawback of this approach is the large number of shares each participant has to hold. In a key generation center, as the trusted authority is always online, it can generate session keys for each participant. Moreover, the transport of these keys are done secretly by encryption with the key shared with each participant during registration.

Threshold Cryptography [22] As it is mentioned in [30], “in many real-life situations, we don’t believe that any given person can be trusted, and we may even suspect that a big fraction of all people are dishonest, yet it is reasonable to assume that the majority of people are trustworthy. Similarly, in on-line transactions, we may doubt that a given server can be trusted, but we hope that the majority of servers are working properly.”

Similar to secret sharing schemes, threshold cryptography secures the information by distributing it among a set of servers. Therefore,

- any sufficient large group of servers recover the secret,
- and any group of corrupt servers should not be able to reconstruct the secret.

A group of cooperating servers can perform cryptographic operations such as decryption or digital signing in such a way that no unauthorized group of servers would be able to perform this operation by themselves, nor would they be able to prevent the other servers from performing the operation when it is required.

Secure Multiparty Computation [66] In secure multiparty computation (SMC) there exits a group of parties who do not trust each other, but have to compute some function of common interest without disclosing their respective inputs. A particular case of SMC, called the two-party computation problem, is the Millionaire’s problem proposed by Yao [66]. Two participants want to know which one of them is richer without having to reveal their actual wealth. The most simple and natural solution is to reveal
their wealth to a third party (trusted authority), who can easily determine
the richer between the two. As in real-life scenarios we do not always have
access to a trusted authority, a protocol is used to simulate one.

### 3.2 Access Structures

Let $U$ be a non-empty finite set, whose elements are called *participants*
(or users). An *access structure over* $U$ is essentially a collection of sets of
participants. The main characteristic of such sets is that they are closed
under inclusion as in the definition below.

**Definition 3.2.1.** [36] Given a non-empty finite set $U$, an *access structure* $(AS)$ over $U$ is a set $\Gamma \subseteq \mathcal{P}(U)$ which satisfies the following monotonicity
property:

$$(\forall A \in \Gamma) \left( (\forall B \in \mathcal{P}(U)) (A \subseteq B) \Rightarrow B \in \Gamma \right).$$

The elements of an access structures are called *authorized sets*, and the
rest are called *unauthorized sets* (or *adversary sets*).

An access structure $\Gamma$ can also be specified by its set of *minimal autho-
rized sets* $\Gamma_0$, given by:

$$\Gamma_0 = \{ A \in \Gamma | (\forall B \subset A) (B \notin \Gamma) \}.$$

We refer to $\Gamma_0$ as the *basis* of the access structure $\Gamma$.

**Definition 3.2.2.** Given a non-empty finite set $U$, an *unauthorized access
structure* over $U$ is a set $\bar{\Gamma} \subseteq \mathcal{P}(U)$, which satisfies the following monotonicity
property:

$$(\forall A \in \bar{\Gamma}) \left( (\forall B \in \mathcal{P}(U)) (A \subset B) \Rightarrow B \in \bar{\Gamma} \right).$$

Note that $\bar{\Gamma} = \mathcal{P}(U) - \Gamma$.

The unauthorized access structure $\bar{\Gamma}$ can be defined, similar to $\Gamma$, by its
set of *maximal unauthorized sets*:

$$\bar{\Gamma}_0 = \{ A \in \bar{\Gamma} | (\forall B \in \mathcal{P}(U)) (A \subset B) \Rightarrow B \notin \bar{\Gamma} \}.$$

**Example 3.2.3.** Consider $U = \{1,2,3,4\}$ and $\Gamma = \{\{1,4\}, \{1,2,3\}, \{1,2,4\},$
$\{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}$. We have:

$$\Gamma_0 = \{\{1,4\}, \{1,2,3\}, \{1,3,4\}, \{2,3,4\}\};$$

$$\bar{\Gamma} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{2,3\}, \{2,4\}, \{3,4\}\};$$

$$\bar{\Gamma}_0 = \{\{1,2\}, \{2,3\}, \{2,4\}, \{3,4\}\}.$$

We present some operations with access structures. The following defi-
nitions are adapted from [43, 44].

---

---

$^2$Beneloh et al. [8] called such sets *monotone access structures*
Definition 3.2.4. [44] Let $U$ be a non-empty finite set and $\Gamma$ be an access structure over $U$. The dual access structure associated to $\Gamma$, denoted $\Gamma^*$, is the set:

$$\Gamma^* = \{ A \in \mathcal{P}(U) | \overline{A} \notin \Gamma \}.$$

Basically, given the set $A$ from an unauthorized access structure $\Gamma$, the complementary set $A$ belongs to $\Gamma^*$. For any set $B \in \mathcal{P}(U)$ with $A \subseteq B$, we have $\overline{B} \subseteq \overline{A}$.

The set $\Gamma^*$, described in Definition 3.2.4, is an access structure over $U$:

$$\forall A \in \Gamma^* \left( (\forall B \in \mathcal{P}(U)) (A \subseteq B) \Rightarrow B \in \Gamma^* \right).$$

Another concept regarding access structures is that of restriction to a given set $C$. Intuitively, it means that only the sets that do not contain elements from $C$ are considered.

Definition 3.2.5. [44] Let $\Gamma$ be an access structure over $U$, $C$ a subset of $U$ and $\overline{U} = U - C$. The restriction of $\Gamma$ to the set $C$, denoted $\Gamma|_C$, is the set:

$$\Gamma|_C = \{ A \in \Gamma | A \notin \overline{U} \}.$$

The set $\Gamma|_C$, described in Definition 3.2.5, is an access structure over $\overline{U}$:

$$\forall A \in \Gamma|_C \left( (\forall B \in \mathcal{P}(\overline{U})) (A \subseteq B) \Rightarrow B \in \Gamma|_C \right).$$

Definition 3.2.6. [44] Let $\Gamma$ be an access structure over $U$, $C$ a subset of $U$ and $\overline{U} = U - C$. The contraction of $\Gamma$ with respect to $C$, denoted $\Gamma \cdot C$, is the set:

$$\Gamma \cdot C = \{ A \in \mathcal{P}(\overline{U}) | A \cup C \in \Gamma \}.$$

The contraction of an access structure with respect to a given set $C$ is obtained by the elimination of the participants in $C$ from any set that belongs to the given access structure. For any set $A, B \in \mathcal{P}(\overline{U})$ with $A \subseteq B$ and $(A \cup C) \in \Gamma$, we have $(B \cup C) \in \Gamma$ (according to Definition 3.2.1).

The set $\Gamma \cdot C$, described in Definition 3.2.6, is an access structure over $\overline{U}$:

$$\forall A \in \Gamma \cdot C \left( (\forall B \in \mathcal{P}(\overline{U})) (A \subseteq B) \Rightarrow B \in \Gamma \cdot C \right).$$

Example 3.2.7. Consider $U = \{1, 2, 3, 4\}$, $\Gamma = \{\{1, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$ and $C = \{2, 3\}$. We have:

$$\Gamma|_C = \{\{1, 4\}\};$$

$$\Gamma \cdot C = \{\{1\}, \{4\}, \{1, 4\}\}.$$

---

Definition 3.2.1 was used to obtain $B \in \Gamma$, for any $A \in \Gamma$ with $A \subseteq B$.  

42
Definition 3.2.8. [44] Let $\Gamma_1$, $\Gamma_2$ be access structures over $U_1$, and $U_2$ respectively, and $C$ a subset of $U_1$. The insertion of $\Gamma_2$ in $\Gamma_1$ with respect to $C$, denoted $\Gamma_1(C\rightarrow \Gamma_2)$, is the set:

$$\Gamma_1(C\rightarrow \Gamma_2) = \{ A \in U | A \in \Gamma_1 \lor ((A \cap U_1) \cup C \in \Gamma_1 \land (A \cap U_2) \in \Gamma_2) \},$$

where $U = (U_1 - C) \cup U_2$.

Intuitively, the insertion of an other access structure $\Gamma_2$ in $\Gamma_1$ is done by replacing the elements of $C$ with authorized sets from $\Gamma_2$. Any set $A \in \Gamma_1$ also satisfies $(A \cap U_1) \cup C \in \Gamma_1$. However, the converse is not necessary true, as there may exist minimal authorized sets that do contain $C$. Given the sets $A, B \in \mathcal{P}(U)$ with $A \subseteq B$ and $(A \cap U_1) \cup C \in \Gamma_1$, we have $(B \cap U_1) \cup C \in \Gamma_1$ (according to Definition 3.2.1). Similarly, for $(B \cap U_2) \in \Gamma_2$.

The set $\Gamma_1(C\rightarrow \Gamma_2)$, described in Definition 3.2.8, is an access structure over $U$:

$$(\forall A \in \Gamma_1(C\rightarrow \Gamma_2))(\forall B \in \mathcal{P}(U))(A \subseteq B) \Rightarrow B \in \Gamma_1(C\rightarrow \Gamma_2).$$

A particular case of this concept, where the set $C$ consists of only participant $u$, is that of the composition of $\Gamma_1$ and $\Gamma_2$ via $u$ [4]:

$$\Gamma_c = \{ A \in U | A \in \Gamma_1 \lor ((A \cap U_1) \cup \{u\} \in \Gamma_1 \land (A \cap U_2) \in \Gamma_2) \},$$

where $U = U_1 \cup U_2 - \{u\}$.

Example 3.2.9. Consider $U_1 = \{1, 2, 3, 4\}$ and $U_2 = \{a, b, c\}$ with the access structures $\Gamma_1 = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$, and $\Gamma_2 = \{\{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$ respectively. Let $C = \{1, 2\}$ and $u = 3$. We have:

$$U = \{3, 4, a, b, c\};$$

$$\Gamma_1(B\rightarrow \Gamma_2) = \{\{3, a, b\}, \{3, b, c\}, \{3, a, c\}, \{4, a, b\}, \{4, b, c\}, \{4, a, c\}, \{3, a, b, c\}, \{4, a, b, c\}, \{3, 4, a, b\}, \{3, 4, b, c\}, \{3, 4, a, c\}, \{3, 4, a, b, c\}\};$$

$$U_c = \{1, 2, 4, a, b, c\};$$

$$\Gamma_c = \{\{1, 2, a, b\}, \{1, 2, b, c\}, \{1, 2, a, c\}, \{1, 2, 4\}, \{1, 2, 4, a, b\}, \{1, 2, 4, b, c\}, \{1, 2, 4, a, c\}, \{1, 4, a, b\}, \{1, 4, b, c\}, \{1, 4, a, c\}, \{1, 4, a, b, c\}, \{2, 4, a, b\}, \{2, 4, b, c\}, \{2, 4, a, c\}, \{2, 4, a, b, c\}\}.$$

Two particular cases of insertion are that of the sum and product of two access structures.

Definition 3.2.10. [44] Let $\Gamma_1$ and $\Gamma_2$ be two access structures over $U_1$ and $U_2$, respectively. The sum of $\Gamma_1$ and $\Gamma_2$, denoted $\Gamma_1 + \Gamma_2$, is the set:

$$\Gamma_1 + \Gamma_2 = \{ A \in U_1 \cap U_2 | (A \cup U_1 \in \Gamma_1) \lor (A \cup U_2 \in \Gamma_2) \}.$$
3.3. Security concepts

**Definition 3.2.11.** [44] Let $\Gamma_1$ be an access structure over $U_1$, and $\Gamma_2$ be an access structure over $U_2$ respectively. The *product* of $\Gamma_1$ and $\Gamma_2$, denoted $\Gamma_1 \cdot \Gamma_2$, is the set:

$$\Gamma_1 \cdot \Gamma_2 = \{ A \in U_1 \cap U_2 \mid (A \cup U_1 \in \Gamma_1) \land (A \cup U_2 \in \Gamma_2) \} .$$

The above two concepts can easily be obtained from insertion, as

$$\Gamma_1 + \Gamma_2 = (\{\{a\}, \{b\}, \{a, b\}\} (\{a\} \rightarrow \Gamma_1) (\{b\} \rightarrow \Gamma_2)$$

$$\Gamma_1 \cdot \Gamma_2 = (\{\{a, b\}\} (\{a\} \rightarrow \Gamma_1) (\{b\} \rightarrow \Gamma_2)$$

for any $a, b \notin U_1 \cap U_2$.

**Example 3.2.12.** Consider $U_1 = \{1, 2, 3\}$ and $U_2 = \{a, b\}$ with the following access structures $\Gamma_1 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$, and $\Gamma_2 = \{\{a\}, \{b\}, \{a, b\}\}$ respectively. We have:

$$\Gamma_1 + \Gamma_2 = \{\{1, 2\}, \{1, 2, a\}, \{1, 2, b\}, \{1, 2, a, b\}, \{1, 3\}, \{1, 3, a\}, \{1, 3, b\}, \{1, 3, a, b\}, \{2, 3\}, \{2, 3, a\}, \{2, 3, b\}, \{2, 3, a, b\}, \{1, 2, 3\}, \{1, 2, 3, a\}, \{1, 2, 3, b\}, \{1, 2, 3, a, b\}\};$$

$$\Gamma_1 \cdot \Gamma_2 = \{\{1, 2, a\}, \{1, 2, b\}, \{1, 2, a, b\}, \{1, 3, a\}, \{1, 3, b\}, \{1, 3, a, b\}, \{2, 3, a\}, \{2, 3, b\}, \{2, 3, a, b\}, \{1, 2, 3, a\}, \{1, 2, 3, b\}, \{1, 2, 3, a, b\}\} .$$

**Definition 3.2.13.** [5] Given a non-empty finite set $U$, an *tripartite access structure* (TAS) over $U$ is a tuple $(A, B, C, m, d, t, \Gamma)$, where $A$, $B$ and $C$ are disjoint sets, $A$ and $C$ are nonempty, $U = A \cup B \cup C$, $m \geq t$, and $\Gamma$ is either $\Delta_1$ or $\Delta_2$ as given below:

$$\Delta_1 = \{X \subseteq U \mid |X| \geq m \land |X \cap (B \cup C)| \geq m - d \lor |X \cap C| \geq t\}$$

$$\Delta_2 = \{X \subseteq U \mid |X| \geq m \land |X \cap C| \geq m - d \lor |X \cap (B \cup C)| \geq t\}$$

3.3 Security concepts

We have informally defined in Chapter 1 the fundamental aspects of a secret sharing scheme. In this section we present two approaches that formally describe secret sharing schemes from a mathematical point of view. Then, extend it to include (perfect) schemes that realize a given access structure.

The first approach, a probabilistic one, is due to Brickell and Stinson [13] (later refined by Stinson in [59, 58]). It considers any scheme as a set of distribution rules, where a rule is a method through which a secret is shared. The second one, based on information theory, is due to Karmen et al. [38] and Kothari [41] (later refined by Capocelli et al. [14]). It views secret sharing schemes as a collection of random variables for which the recovery of the secret is measured by entropy.

The approach we follow is the one in [20, 18] with the permission of Prof. dr. F.L. Tiplea (due to the fact that both [20] and [18] are unpublished yet).
Chapter 3. Secret Sharing Schemes

Definition 3.3.1. [58] A distribution rule is a function $f : U \rightarrow S_1 \times \cdots \times S_n$ from the set of participants $U$ to the share spaces $S_1, \ldots, S_n$, such that $f(i) \in S_i$ for all $i \in U$, where $n$ denotes the cardinality of $U$.

Essentially, a distribution rule represents a possible distribution of shares to the participants of $U$. Therefore, each participant $i \in U$ takes shares only from the share space assigned to it $S_i$.

For each secret $s$ from the secret space $S$, let $F_s$ denote the set of distribution rule assigned to $s$.

The set of all distribution rules $F$ is given by

$$F = \bigcup_{s \in S} F_s.$$ 

For simplicity, we denote $(S_i, i \in U)$ the share spaces assigned to a set $U$.

Definition 3.3.2. [13] A secret sharing scheme over a set $U$ of participants is a triple $(S, (S_i, i \in U), F)$, where $S$ is a set of master secrets, $S_i$ is the share space of $i \in U$, and $F$ is the set of all distribution rules.

For any set $A \subseteq U$, we define the restriction of a rule $f$ to $A$, denoted $f|_A$, as the function $f|_A : A \rightarrow \bigcup_{i \in A} S_i$ with

$$f|_A(i) = f(i), \forall i \in A.$$ 

Karnin, Green and Hellman have proposed in [38] the following secret sharing scheme:

Karnin-Green-Hellman (KGH) scheme

parameter

consider $U$ the set of $n$ participants, and $m$ a positive integer such that $m > n$;

setup

define the secret space and share spaces as $\mathbb{Z}_m$;

secret and share spaces

given a secret $s$, randomly generate $n-1$ distinct elements $a_1, \ldots, a_{n-1} \in \mathbb{Z}_m$, and compute

$$a_n = s - (a_1 + \cdots + a_{n-1}) \mod m.$$ 

Then, share $s$ by $s_i = a_i \mod m$, for any $1 \leq i \leq n$.

secret reconstruction

currently all the participants are needed for the recovery of the secret, as $s$ can be uniquely obtain by computing

$$s = \sum_{i=1}^{n} s_i \mod m.$$ 

45
3.3. Security concepts

The KGH scheme can be described using the formalism of Definition 3.3.2. The set $U = \{1, 2, \ldots, n\}$ contains $n$ participants, and the secret and share spaces are defined as

$$S = S_i = \mathbb{Z}_m,$$

for any $1 \leq i \leq n$ and some $m > n$.

Given the secret $s \in S$, any distribution rule $f$ for $s$ is of the form

$$f = (a_1, a_2, \ldots, a_n)$$

where $a_1, a_2, \ldots, a_n \in \mathbb{Z}_m$ such that $a_1 + a_2 + \cdots + a_n = s \mod m$.

**Example 3.3.3.** Let $(\mathbb{Z}_3, (\mathbb{Z}_3, \mathbb{Z}_3), F)$ be an instance of the KGH scheme over the set $U = \{P_1, P_2\}$. However, the sharing and recovery phase are not taken into consideration. The set of all distribution rules is given in Table 3.1.

As there is no restriction over the rules, the same rules are found in each $F_s$. Therefore,

$$F = F_s = \{f_1, \ldots, f_9\},$$

for any $s \in \mathbb{Z}_3$.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Secret</th>
<th>$P_1$</th>
<th>$P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_1$</td>
<td>$s$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$f_2$</td>
<td>$s$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$f_3$</td>
<td>$s$</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$f_4$</td>
<td>$s$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$f_5$</td>
<td>$s$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$f_6$</td>
<td>$s$</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$f_7$</td>
<td>$s$</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$f_8$</td>
<td>$s$</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$f_9$</td>
<td>$s$</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Definition 3.3.4.** [59] A secret sharing scheme $(S, (S_i, i \in U), F)$ realizes the access structure $\Gamma$ over $U$ if the following property is satisfied:

$$((\forall s, s' \in S)(s \neq s'))((\forall f \in F_s)(\forall f' \in F_{s'})((\forall A \in \Gamma) \Rightarrow f|_A \neq f'|_A)).$$

The above definition states that two different secrets $s, s' \in S$ cannot be shared identically to the same authorized set $A \in \Gamma$. In other words,

Ito et al. [36] first proposed and proved that there exists secret sharing schemes that realizes a given access structure. However, to the best of our knowledge, Stinson formalized this property using distribution rules in [59].

46
the secret is recover uniquely by a single distribution rule regardless of the authorized set used.

**Example 3.3.5.** Let \((\mathbb{Z}_3, (\mathbb{Z}_4, \mathbb{Z}_3), F)\) be an instance of the KGH scheme over the set \(U = \{P_1, P_2\}\). The set of all distribution rules is given in Table 3.2.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Secret</th>
<th>(P_1)</th>
<th>(P_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f_1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(f_2)</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>(f_3)</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>(f_4)</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(f_5)</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>(f_6)</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>(f_7)</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>(f_8)</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(f_9)</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

The sharing and recovery phase define the access structure:

\[ \Gamma = \{\{P_1, P_2\}\}. \]

All participants are needed for the recovery.

Compared to Example 3.3.3, the rules of each secret \(s\) are restricted by the access structure \(\Gamma\):

\[ F_0 = \{f_1, f_2, f_3\} \]
\[ F_1 = \{f_4, f_5, f_6\} \]
\[ F_2 = \{f_7, f_8, f_9\} \]
\[ F = F_0 \cup F_1 \cup F_2. \]

Given a secret sharing scheme \((S, (S_i, i \in U), F)\), we associate the following probabilities:

- \(P_S\) the probability distribution for the secret space \(S\);
- \(P_{f,s}\) the probability of choosing \(f \in F_s\) (usually, \(P_{f,s}\) is uniform);
- and \(P\) the probability associated to the share vector \(y \in S_A\) with

\[ P(y) = \sum_{s \in S} P_S(s) \cdot \sum_{f \in F_s, \ f|A=y} P_{f,s}(f). \]

(For a set \(A \subseteq U\), we consider \(S_A = \cup_{i \in A} S_i\) the set of all share vectors associated to \(A\), and the share vector \(y\) a element of \(S_A\).)
3.3. Security concepts

For simplicity, we remove the indices $S$ and $(f, s)$ and only use $P$ when discussing the probability of the elements from the secret space or the distribution rule set.

**Proposition 3.3.6.** [20, 18] The probability $P$ induces a probability distribution over the set of all share vectors associated to $A$.

**Proof.** A share vector is a rule restricted to a set. Therefore, the conditional probability of any $y$ given by some $s \in S$ is the probability of all the rules from $F_s$ restricted to $A$:

$$P(y | s) = \sum_{f \in F_s, f|A=y} P(f).$$

For some $s \in S$, the sum of all the conditional probability $P(y | s)$ after $y \in S_A$ is 1.

The probability of $y$ is

$$P(y) = \sum_{s \in S} P(s) P(y | s).$$

According to Proposition 2.3.16, the result follows.

**Example 3.3.7.** Let $(\mathbb{Z}_3, (\mathbb{Z}_3, \mathbb{Z}_3), F)$ be an instance of the KGH scheme over the set $U = \{P_1, P_2\}$. The set of all distribution rules is given in Table 3.2.

The secret space has 3 secrets, and for each secret there are 3 distribution rules. Then, the probabilities involved in this scheme are defined as follows:

$$P(s) = \frac{1}{3}, \quad \forall s \in S \quad \text{and} \quad P(f) = \frac{1}{3}, \quad \forall f \in F_s.$$

The conditional probability of the share vector $y \in S_U$ given by $s$, is presented in Table 3.3. The probability $P(y)$ is $1/9$, for any $y \in S_U$.

<table>
<thead>
<tr>
<th>$s$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1/3</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1/3</td>
<td>1/3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1/3</td>
<td>1/3</td>
</tr>
</tbody>
</table>

Table 3.3: The probability $P(y | s)$

\[
\begin{array}{cccccccc}
 s & y & (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) & (2,0) \\
\hline
 0 & 1/3 & 0 & 0 & 0 & 1/3 & 0 & 1/3 & 0 \\
 1 & 0 & 1/3 & 0 & 1/3 & 0 & 0 & 0 & 1/3 \\
 2 & 0 & 0 & 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\
\end{array}
\]

Let $A = \{P_1\}$ and $S_A = \{0, 1, 2\}$. Then, the probability $P(y)$ is $1/3$ for any $y \in S_A$. 48
Chapter 3. Secret Sharing Schemes

In secret sharing schemes there may exist sets \( A \in U \) and share vectors \( y \in S_A \) such that \( P(y) = 0 \). If \( P(y) > 0 \), then there exists \( s \in S \) and \( f \in F_s \) such that \( f|_A = y \).

**Remark 3.3.8.** For a secret sharing scheme, we assume a strict positive distribution over the secret space. Meaning, each secret is shared.

The following result strengthens Definition 3.3.4 by showing that for any secret sharing scheme that realizes a given access structure and for any secret, there exists a single distribution rule.

**Proposition 3.3.9.** Let \((S, (S_i | i \in U), F)\) be a secret sharing scheme that realizes the access structure \( \Gamma \). Then, for any secret \( s \in S \), there exists a single rule \( f \in F \) such that \( f|_A = y \), for any \( A \in \Gamma \) and any \( y \in S_A \) with \( P(y) > 0 \).

**Proof.** Let \( s' \in S \) and \( f \in F_{s'} \). We prove \( f \) is unique with respect to \( f|_A = y \), for any \( A \in \Gamma \) and any \( y \in S_A \).

Assume there exists \( f' \neq f \) such that \( f'|_A = y \), for any \( A \in \Gamma \) and any \( y \in S_A \). Thus, \( f|_A = f'|_A \) for any \( A \in \Gamma \).

Given \( A = U \), we have \( f = f' \) (according to Definition 3.2.1). Therefore, our assumption is false and there exists a single \( f \) in \( F_{s'} \).

According to Definition 3.3.4, there exist no other rules \( f' \in F - F_{s'} \) such that \( f'|_A = y \). The result follows. \( \square \)

In a secret sharing scheme that realizes a given access structure, any authorized set recovers the same secret. In [58] Stinson ensured the uniqueness of the secret for any authorized set through distribution rules (see Definition 3.3.4). Meaning, for any secret there exists a single distribution rule (see Proposition 3.3.9).

Blundo et al. [10] have remarked that the converse is also true. For any authorized set there exists only one secret obtain from the shares involved. In the following theorem we prove the results are equivalent.

**Theorem 3.3.10.** [20, 18] A \((S, (S_i | i \in U), F)\) secret sharing scheme realizes the access structure \( \Gamma \) if and only if
\[
(\forall A \in \Gamma) \left( (\forall y \in S_A)(P(y) > 0) \Rightarrow (\exists s \in S)(P(s | y) = 1) \right).
\]

**Proof.** [20, 18] Let \( A \in \Gamma \) and \( y \in S_A \), with \( P(y) > 0 \).

We prove that there exists a single \( s \in S \) such that \( P(y | s) = 1 \). Assume the scheme \((S, (S_i | i \in U), F)\) realizes the access structure \( \Gamma \).

Based on Proposition 3.3.9, for any \( s' \in S \) there exists a single \( f \in F_{s'} \) with \( f|_A = y \). According to Definition 3.3.4, \( s' \) is also unique. Moreover, \( P(y | s) = 0 \) for any \( s \in S \) with \( s \neq s' \).
Recall that $P(y)$ is defined as

$$P(y) = \sum_{s \in S} P(s)P(y|s).$$

As $P(y|s) = 0$, for any $s \in S$ with $s \neq s'$, we have

$$P(y) = P(s')P(y|s').$$

Therefore, using Bayes formula (see Proposition 2.3.14) there exists only one $s' \in S$ such that

$$P(s'|y) = 1.$$  

We prove now the converse. Assume there exists only one secret $s' \in S$ such that $P(s'|y) = 1$.

Based on Bayes formula (Proposition 2.3.14), we obtain the following equality

$$\frac{P(y|s')P(s')}{P(y)} = 1.$$  

As $P(y) > 0$, it implies there exists a rule $f \in F_{s'}$ such that $f|_A = y$.

Regarding $P(y)$, on one hand it is defined as

$$P(y) = P(s')P(y|s') + \sum_{s \in S - \{s'} P(s)P(y|s),$$

on the other hand it is defined as

$$P(y) = P(s')P(y|s').$$

From $P(y|s) = 0$, for any $s \in S$ with $s \neq s'$, we have for any two different secrets $s, s' \in S$, and for any rules $f \in F_s$ and $f' \in F_{s'}$ that $f|_A \neq f'|_A$.

Therefore, the scheme realizes the access structure.

**Definition 3.3.11.** [13] Let $(S,(S_i, i \in U), F)$ be a secret sharing scheme that realizes the access structure $\Gamma$. The scheme $(S,(S_i, i \in U), F)$ is a perfect secret sharing scheme if the following property is satisfied

$$(\forall B \notin \Gamma) \ ((\forall y \in S_B)(P(y) > 0)) \ (\forall s \in S) \Rightarrow P(s|y) = P(s).$$

From a probabilistic point of view, the knowledge given by any unauthorized set $B$, thru the shares $y$, is the same as having no information at all.

**Proposition 3.3.12.** [20, 18] For any perfect secret sharing schemes, the probability of any share vector is strict positive.

**Proof.** Let $(S,(S_i, i \in U), F)$ be a perfect secret sharing scheme that realizes the access structure $\Gamma$, $A \subseteq U$ and $y \in S_A$. We prove that $P(y) > 0$. 

50
Chapter 3. Secret Sharing Schemes

Assume that $y$ is not shared by any secret $s \in S$. Then, $P(s \mid y) = 0$ for any $s \in S$. Based on Definition 3.3.11, we have $P(s) = 0$. Our assumption is false, as there is a strict positive distribution over the secret space (according to Remark 3.3.8).

Therefore, $P(y) > 0$.

The condition imposed by perfect secret sharing schemes can be subjected to Bayes formula (Proposition 2.3.14), such that $P(s \mid y) = P(y) \cdot \frac{P(s)}{P(y)}$.

The share vector of an unauthorized set can be obtain from any secret.

Example 3.3.13. Let $(\mathbb{Z}_3, (\mathbb{Z}_3, \mathbb{Z}_3), F)$ be an instance of the KGH scheme over the set $U = \{P_1, P_2\}$. The set of distribution rules is given in Table 3.2.

We prove that the scheme is perfect.

Let $B = \{P_1\}$. Recall that $P(y \mid s)$ is the probability of all the rules $f \in F_s$ that have $f \mid B = y$. In our case, $f \mid B$ means that $f(1) = y$ and $f(2)$ can take any value from $\mathbb{Z}_3$.

For any $y \in S_B$ and for any $s \in \mathbb{Z}_3$, there exists only one rule from $F_s$ such that $f \mid B = y$. Thus, $P(y \mid s) = 1/3$.

As $P(y)$ is

$$P(y) = \sum_{s \in \mathbb{Z}_3} P(s) P(y \mid s),$$

we have $P(y) = 1/3$ for any $y \in S_B$.

Therefore, $P(y) = P(y \mid s)$ for any $s \in \mathbb{Z}_3$ and $y \in S_B$.

Similarly, for $B = \{P_2\}$, one obtains $P(y) = P(y \mid s)$ for any $s \in \mathbb{Z}_3$ and $y \in S_B$.

Theorem 3.3.14. [20, 18] Let $(S, (S_i, i \in U), F)$ be a secret sharing scheme that realizes the access structure $\Gamma$. Then, the scheme $(S, (S_i, i \in U), F)$ is perfect and $(\forall s, s' \in S)(|F_s| = |F_{s'}|)$ if and only if

$$(\forall B \not\in \Gamma) ((\forall y \in S_B)(P(y > 0))$$

there exists a constant $\lambda_{B,y}$ that depends on $B$ and $y$ such that for any $s \in S$ we have $|\{f \in F_s \mid f \mid B = y\}| = \lambda_{B,y}^5$.

Proof. [20, 18] Let $B \in \Gamma$ and $y \in S_B$, with $P(y) > 0$. The constant $\lambda_{B,y}$, can also be defined by the following relation

$$|\{f \in F_s \mid f \mid B = y\}| = |\{f \in F_{s'} \mid f \mid B = y\}|,$$

for any two different secrets $s, s' \in S$.

5 The condition was introduced by Brickell and Davenport [12] using finite matrices, and later extended by Brickell and Stinson [13, 59] to distribution rules.
3.3. Security concepts

We prove that the number of rules restricted by $B$ and equal to $y$ is the same regardless of the secret involved. Assume that $(S, (S_i, i \in U), F)$ is a perfect secret sharing scheme. Using Bayes formula (Proposition 2.3.14), for any $s \in S$, we have

$$P(y \mid s) = P(y) .$$

Condition that can be extend to

$$P(y \mid s) = P(y \mid s') ,$$

for any $s, s' \in S$. Therefore, for any $s, s' \in S$:

$$\frac{|\{f \in F_s \mid f \mid B = y\}|}{|F_s|} = \frac{|\{f \in F_{s'} \mid f \mid B = y\}|}{|F_{s'}|} .$$

As the space $F$ is under a uniform distribution ($|F_s| = |F_{s'}|$ for any $s, s' \in S$), the result of the theorem easily follows

$$|\{f \in F_s \mid f \mid B = y\}| = |\{f \in F_{s'} \mid f \mid B = y\}| .$$

We prove now the converse. Assume for any $s \in S$, there exists $\lambda_{B,y}$ such that

$$|\{f \in F_s \mid f \mid B = y\}| = \lambda_{B,y} .$$

For $B = \emptyset$ and $y = \emptyset$ (see Proposition 3.3.12 for $P(y) > 0$), we have

$$|\{f \in F_s \mid f \mid \emptyset = \emptyset\}| = \lambda_{\emptyset,\emptyset} , \forall s \in S .$$

The element on the left side of the above equality is $F_s$. Thus, we can extend our result to

$$|F_s| = |F_{s'}| ,$$

for any $s, s' \in S$.

For any $s \in S$, the conditional probability $P(y \mid s)$ is the number of rules that restricted by $B$ give $y$, over the total number of rules generated by $s$:

$$P(y \mid s) = \frac{|\{f \in F_s \mid f \mid B = y\}|}{|F_s|} = \frac{\lambda_{B,y}}{\lambda_{\emptyset,\emptyset}} .$$

As $P(s)$ induces a probability distribution over the secret space, the probability of the share vector $y$ is of form

$$P(y) = \sum_{s \in S} P(s) \cdot P(y \mid s) = \sum_{s \in S} \frac{\lambda_{B,y}}{\lambda_{\emptyset,\emptyset}} \cdot \sum_{s \in S} P(s) = \frac{\lambda_{B,y}}{\lambda_{\emptyset,\emptyset}} .$$

From $P(y \mid s) = P(y)$, and based on Definition 3.3.11 the secret sharing scheme $(S, (S_i, i \in U), F)$ is perfect. \qed
Theorem 3.3.15. [58] The KGH secret sharing scheme is perfect.

Proof. [20, 18] Let \((S, (S_i, i \in U), F)\) be a instance of the KGH secret sharing scheme, where \(|U| = n\) and \(S = S_i = \mathbb{Z}_m\), for any \(1 \leq i \leq n\) and for some prime \(m > n\). Using Theorem 3.3.14, the \((S, (S_i, i \in U), F)\) is perfect if and only if for any \(B \not\in \Gamma\) and any \(y \in S_B\) the following relation holds:

\[
|\{f \in F_s | f|_B = y\}| = |\{f' \in F_{s'} | f|_B = y\}|,
\]

for any \(s, s' \in S\).

Let \(B \not\in \Gamma\) and \(y \in S_B\) with \(P(y) > 0\). We prove there exists a bijection between the sets \(M_s = \{f \in F_s | f|_B = y\}\) and \(M_{s'} = \{f' \in F_{s'} | f|_B = y\}\).

Let \(\varphi\) be a function from \(M_s\) to \(M_{s'}\) with

\[
\varphi(f) = f',
\]

such that \(f'(i) = f(i)\) for any \(1 \leq i \leq n-1\) and \(f'(n) = s' - s + f(n) \mod m\).

Note that

\[
\begin{align*}
    f(1) + \cdots + f(n) &= s \mod m, \\
    f'(1) + \cdots + f'(n) &= s' \mod m.
\end{align*}
\]

We prove \(\varphi\) is injective. Let \(f_1, f_2\) be two different rules such that \(f_1(i) = f_2(i)\) for any \(i \in B\), and \(f_1(j) \neq f_2(j)\) for some \(j \in U - B\).

As \(f'_1 = \varphi(f_1)\) and \(f'_2 = \varphi(f_2)\), it is clear that \(f'_1(j) \neq f'_2(j)\) for some \(j \in U\). Therefore, the function \(\varphi\) is injective.

We prove now \(\varphi\) is surjective. Let \(f' \in M_{s'}\), one can easily build \(f \in M_s\) replacing \(s'\) with \(s\) for the \(n\)-th share and keeping the rest of the shares the same:

\[
f(i) = f'(i)
\]

for any \(1 \leq i < n\), and \(f(n) = s' - s + f'(n)\). So, \(\varphi(f) = f'\).

In conclusion, \(\varphi\) is bijective, and the result easily follows. \(\square\)

Shamir has proposed in [54] the following secret sharing scheme:

**Shamir scheme**

- **setup** consider \(U\) a set of \(n\) participants, and \(t \leq n\) the security parameter for which any authorizes set \(A\) satisfies \(|A| \geq t\);
- **secret and share spaces** define the secret space and share spaces as \(\mathbb{Z}_m\), for some prime \(m > n\);
- **secret sharing** given a secret \(s\), randomly generate \(t - 1\) distinct elements \(a_1, \ldots, a_{t-1} \in \mathbb{Z}_m\), and compute the polynomial \(q(x) = a_{t-1}x^{t-1} + \cdots + a_1x + s \mod m\). Then, share \(s\) to participant \(i\) by \(s_i = q(i) \mod m\) for any \(1 \leq i \leq n\).
3.3. Security concepts

**secret** any set \( A \subseteq U \) of participants with \( |A| \geq t \) can recover
**reconstruction** the secret uniquely by Lagrange’s interpolation over the
shares \( s_i \) for all \( i \in A \)

\[
s = \sum_{i \in A} \left( s_i \cdot \prod_{j \in A - \{i\}} \frac{j}{j - i} \right) \mod m .
\]

The Shamir scheme can be described using the formalism of Definition
3.3.2. The set \( U = \{1, 2, \ldots, n\} \) contains \( n \) participants, and the secret and
share spaces are defined as

\[
S = S_i = \mathbb{Z}_m, \text{ for any } 1 \leq i \leq n \text{ and some } m > n.
\]

Given the secret \( s \in S \), any distribution rule \( f \) for \( s \) is of form

\[
f = (s, a_1, a_2, \ldots, a_t),
\]

where \( a_1, a_2, \ldots, a_t \) are randomly generated from \( \mathbb{Z}_m \).

**Theorem 3.3.16.** [58] The Shamir secret sharing scheme is perfect.

**Proof.** [20, 18] Let \((S, (S_i, i \in U), F)\) be a instance of the Shamir secret
sharing scheme with \( |U| = n \) and \( S = S_i = \mathbb{Z}_m, \) for any \( 1 \leq i \leq n \) and some \( m > n \).

We prove that \((S, (S_i, i \in U), F)\) is perfect. According to Definition
3.3.11 a secret sharing scheme is perfect if for any \( B \notin \Gamma \) and any \( y \in S_B \)
the following relation takes place

\[
P(y \mid s) = P(y).
\]

Let \( B \notin \Gamma \) (meaning, \( |B| < t \)) and \( y \in S_B \).

**Case 1:** \( |B| = t - 1 \). \( P(y \mid s) \) is the probability of choosing a polynomial that
has the free coefficient \( s \) and passes \((t - 1)\) points given by \( y \), over the total
number of polynomials with the free coefficient equal to \( s \)

\[
P(y \mid s) = \frac{1}{m^{t-1}}.
\]

(There exists only one polynomial that has the free coefficient \( s \) and passes
thru \( y \), and there are \( m^{t-1} \) values of \( y \) in \( S_B \).)

The probability \( P(y) \) is given by the number of polynomials that passes
thru \( y \), for each \( s \in S \), over the total number of polynomials

\[
P(y) = \frac{m}{m^t}.
\]

Thus, \( P(y \mid s) = P(y) \) for any \( B \notin \Gamma \) with \( |B| = t - 1 \).

---

6 To the best of our knowledge, a complete proof over the perfectness of the Shamir
scheme can only be found in [20].
Lemma 3.3.17. \cite{28} If the coefficient $a_{t-1}$ is taken from $\mathbb{Z}_m^*$ (thus avoiding 0), then the Shamir scheme is not perfect.

Proof. Let $(S, (S_i, i \in U), F)$ be a instance of the Shamir secret sharing scheme with $|U| = n$ and $S = S_i = \mathbb{Z}_m$, for any $1 \leq i \leq n$ and for some prime $m > n$. Moreover, let $q(x)$ be the polynomial used to share $s \in S$:

$$q(x) = a_{t-1}x^{t-1} + \cdots + a_1x + s \mod m.$$ 

To simplify the proof, let $s_1, \ldots, s_{t-1}$ be the shares of $(t-1)$ random participants and $g(x)$ the uniquely deduced polynomial

$$g(x) = a'_{t-2}x^{t-2} + \cdots + a'_1x + s' \mod m,$$

with $g(i) = s_i$ (or $q(i)$) for any $1 \leq i \leq t-1$.

Applying $q(x_i) - g(x_i)$ for each $1 \leq i \leq t-1$ where $x_i = i$, we have the following system of equations:

$$(s - s') + (a_1 - a'_1)x_1 + \cdots + (a_{t-2} - a'_{t-2})x_1^{t-2} + a_{t-1}x_1^{t-1} = 0$$

$$\cdots$$

$$(s - s') + (a_1 - a'_1)x_{t-1} + \cdots + (a_{t-2} - a'_{t-2})x_{t-1}^{t-2} + a_{t-1}x_{t-1}^{t-1} = 0$$

If $s = s'$ mod $m$, then the resulting system has a non-empty Vandermonde determinant, which implies a unique solution. Let $a_{t-1} = 0$ and $a_i = a'_i$ for any $1 \leq i \leq t - 2$ be a solution of the system. Based on the previous remark this solution is unique with respect to $a_{t-1} = 0$. In this case an unauthorized set could obtain the secret, and thus making the scheme not perfect.

Restricting $a_{t-1}$ to $\mathbb{Z}_m^*$ (avoiding 0) does not lead to a unique solution in the above system. However, it affects the perfectness of the secret sharing scheme.

Let $y$ be the share vector used to obtain the polynomial $g(x)$, defined as above. According to our restriction, we have $P(y) = 0$ as there exists no secret $s$ with a distribution rule that leads to $y$.

Recall that in a perfect secret sharing scheme $P(y) > 0$, for any share vector $y$ (see Proposition 3.3.12). Therefore, the result follows.
Remark 3.3.18. Any constraint on the coefficients used by the polynomial in the Shamir scheme \cite{54} leads to the loss of perfectness. By a constraint on coefficients we mean, for instance:

- \(a_i \neq 0\) or
- \(a_i \neq a_j\) for some \(i \neq j\).

Another approach used to describe (or introduce) secret sharing schemes is that of entropy. Approach that can be further extended to include (perfect) schemes that realize an access structure.

Let \((S, (S_i, i \in U), F)\) be a secret sharing scheme as defined in Definition 3.3.2. We introduce the following random variables associated to such a scheme:

- \(X\) that takes values into the secret space \(S\),
- \(Y_i\) that takes values into the share space \(S_i\), for any \(i \in U\), and \(Y_I\) that takes values into the combined share space \(\bigcup_{i \in I} S_i\), for any \(I \subseteq U\),
- and \(F_s\) that takes values into the rules space \(F_s\), for any secret \(s \in S\).

**Definition 3.3.19.** \cite{38} A secret sharing scheme over a set \(U\) of participants is a tuple \((X, (Y_i, i \in U), (F_s, s \in S))\), where the random variables are defined as above.

Recall that the entropy (Section 2.3.2) measures the uncertainty level concerning the recovery of the secret. Therefore, for any authorized set there should exists no uncertainty regarding such an event, whereas for any unauthorized the uncertainty level should be maximal as the knowledge of any number of shares should have no impact on the recovery of the secret.

**Definition 3.3.20.** \cite{38} A \((X, (Y_i, i \in U), (F_s, s \in S))\) secret sharing scheme realizes the access structure \(\Gamma\) if

\[
(\forall A \in \Gamma) \left( H(X | Y_A) = 0 \right). 
\]

**Definition 3.3.21.** \cite{38} A \((X, (Y_i, i \in U), (F_s, s \in S))\) is a perfect secret sharing scheme if it realizes the access structure \(\Gamma\) and

\[
(\forall B \notin \Gamma) \left( H(X | Y_B) = H(X) \right). 
\]

Perfect secret sharing schemes can also be defined by replacing the expression realizes an access structure with the property involved. Thus, \((X, (Y_i, i \in U), (F_s, s \in S))\) is a perfect secret sharing scheme if the following properties are satisfied:

1. \((\forall A \in \Gamma) \left( H(X | Y_A) = 0 \right)\);
2. \((\forall B \notin \Gamma) \left( H(X | Y_B) = H(X) \right)\).
Previously we defined (perfect) secret sharing schemes that realize a given access structure using entropy. In what follows we prove that the conditions involved are sufficient to ensure the correctness of the definitions. A remark concerning the proofs in the following lemmas is given by Capocelli et al. [14], but the complete proofs can be found in [20].

Lemma 3.3.22. [14] A \( (X, (Y_i, i \in U), (F_s, s \in S)) \) secret sharing scheme realizes \( \Gamma \) if and only if
\[
(\forall A \in \Gamma) \left( H(X \mid Y_A) = 0 \right)
\]

Proof. [20, 18] For any random variables \( X \) and \( Y_A \) and the element \( y \), the conditional entropy (see Section 2.3.2) is defined as
\[
H(X \mid Y_A) = \sum_{y \in S_A} H(X \mid Y_A = y) P(Y_A = y)
\]
\[
H(X \mid Y_A = y) = -\sum_{s \in S} P(X = s \mid Y_A = y) \log P(X = s \mid Y_A = y)
\]

We prove that the conditional entropy \( H(X \mid Y_A) \) is 0 for any \( A \in \Gamma \). Assume that the scheme \( (X, (Y_i, i \in U), (F_s, s \in S)) \) realizes the access structure \( \Gamma \). Based on Theorem 3.3.10, for any \( A \in \Gamma \) and for any \( y \in S_A \) there exists a unique \( s' \in S \) such that \( P(X = s' \mid Y_A = y) = 1 \). Moreover, \( P(X = s \mid Y_A = y) = 0 \) for any other \( s \in S \) with \( s \neq s' \).

Therefore, the conditional entropy is
\[
H(X \mid Y_A = y) = -\sum_{s \in S} P(X = s \mid Y_A = y) \log P(X = s \mid Y_A = y) = 0
\]
and
\[
H(X \mid Y_A) = \sum_{y \in S_A} H(X \mid Y_A = y) P(Y_A = y) = 0
\]

(the convention \( 0 \log 0 = 0 \) was used.) Thus, the result follows.

Assume the converse is true, that for any \( A \in \Gamma \) the conditional entropy \( H(X \mid Y_A) \) is 0. We prove the scheme \( (X, (Y_i, i \in U), (F_s, s \in S)) \) realizes the access structure \( \Gamma \).

Based on the definition of the conditional entropy \( H(X \mid Y_A) \), we have that
\[
H(X \mid Y_A = y) P(Y_A = y) = 0
\]
for any \( y \in S_A \).

As \( P(Y_A = y) > 0 \) for any \( y \in S_A \), the conclusion is that \( H(X \mid Y_A = y) = 0 \). Therefore, there exists a unique \( s' \in S \) for any given \( y \in S_A \) such that \( P(X = s' \mid Y_A = y) = 1 \).

Based on Theorem 3.3.10 the scheme realizes the access structure \( \Gamma \). \( \square \)
Lemma 3.3.23. [14] \((X, (Y_i, i \in U), (F_s, s \in S))\) is a perfect secret sharing scheme that realizes \(\Gamma\) if and only if
\[
\begin{align*}
(1) & \quad (\forall A \in \Gamma) \left( H(X \mid Y_A) = 0 \right); \\
(2) & \quad (\forall B \notin \Gamma) \left( H(X \mid Y_B) = H(X) \right).
\end{align*}
\]

Proof. [20, 18] From Lemma 3.3.22 we have the equivalence concerning the realization of the access structure \(\Gamma\). Thus, condition (1) is satisfied.

Recall that \(H(X \mid Y_B) = H(X)\) for any two random variable \(X\) and \(Y_B\) if and only if \(X\) and \(Y_B\) are independent.

Thus, we have to prove that the \((X, (Y_i, i \in U), (F_s, s \in S))\) scheme is perfect if and only if
\[
P(X = s \mid Y_B = y) = P(X = s)
\]
for any \(B \notin \Gamma\), any \(y \in Y_B\) and for any \(s \in X\) with \(P(Y_B = y) > 0\).

Result that corresponds to the Definition 3.3.11 of perfectness. □

Lemma 3.3.24. [14] Let \((X, (Y_i, i \in U), (F_s, s \in S))\) be a perfect secret sharing scheme that realizes the access structure \(\Gamma\), then
\[
H(Y_C \mid Y_B) = H(X) + H(Y_C \mid Y_B, X),
\]
for any \(B \notin \Gamma\) and \(C \subseteq U\) with \(C \cup B \in \Gamma\).

Proof. Recall the following conditional entropies from Section 2.3.2 (Proposition 2.3.30):
\[
\begin{align*}
H(Y_C, X \mid Y_B) &= H(Y_C \mid X, Y_B) + H(X \mid Y_B) \\
H(Y_C, X \mid Y_B) &= H(X \mid Y_C, Y_B) + H(Y_C \mid Y_B).
\end{align*}
\]

Equalizing the above relations, we have
\[
H(Y_C \mid X, Y_B) + H(X \mid Y_B) = H(X \mid Y_C, Y_B) + H(Y_C \mid Y_B).
\]

As the scheme is perfect, we have \(H(X \mid Y_B) = H(X)\) and \(H(X \mid Y_C, Y_B) = 0\) (Definition 3.3.21).

Therefore, the result of the lemma is easily obtained. □

Corollary 3.3.25. [38] Let \((X, (Y_i, i \in U), (F_s, s \in S))\) be a perfect secret sharing scheme that realizes \(\Gamma\). Then, for any \(i \in U\) the following property holds
\[
H(Y_i) \geq H(X).
\]

Proof. Let \(B \notin \Gamma\) such that \(B \cup \{i\} \in \Gamma\). Using Lemma 3.3.24 for \(C = \{i\}\) and \(B\), we obtain
\[
H(Y_i \mid Y_B) = H(X) + H(Y_i \mid Y_B, X).
\]

As \(H(Y_i \mid Y_B) \leq H(Y_i)\) (see Proposition 2.3.30), the result easily follows. □
3.4 Perfect realizations of access structures

In this section we show that for any access structure there exists a perfect secret sharing scheme that realizes it. The idea, proposed by Beneloh et al. [8], is to construct an monotone boolean circuit.

**Definition 3.4.1.** [63] Let $U$ be a set of $n$ boolean variables $x_1, \ldots, x_n$. A boolean formula $\varphi$ over $U$ is constructed recursively as

$$\varphi ::= i \mid (\varphi \lor \varphi) \mid (\varphi \land \varphi) \mid (\neg \varphi)$$

for any $i \in U$.

We associate to a set of boolean variables $U$, the following assignation $\gamma : U \to \{0, 1\}$ such that $\gamma(i)$ gives the truth value of the variable $i$, for any $i \in U$. Meaning, $\gamma(i)$ is 1 if $i$ belongs to the assignation, and 0 otherwise.

Moreover, one can establish an order between two assignations, by assigning the following inequality $0 < 1$ to the false (0) and true (1) values. Given $\gamma$ an assignation over $U$, we define $\gamma'$ larger than $\gamma$ ($\gamma \leq \gamma'$) by

$$\gamma(x_i) \leq \gamma'(x_i),$$

for any $i \in U$.

Furthermore, assignations can be extended to include boolean formulas. Given the boolean formula $\varphi$, we evaluate $\gamma(\varphi)$ by

- $\gamma(x_i)$ if $\varphi = x_i$ for any $i \in U$;
- $\gamma(\varphi_1) \lor \gamma(\varphi_2)$ for any $\varphi = \varphi_1 \lor \varphi_2$;
- $\gamma(\varphi_1) \land \gamma(\varphi_2)$ for any $\varphi = \varphi_1 \land \varphi_2$;
- $\neg \gamma(\varphi_1)$ for any $\varphi = \neg \varphi_1$.

**Remark 3.4.2.** Any boolean formula $\varphi$ over $U$ that does not contain negations is monotone.

**Proposition 3.4.3.** [63] Let $\varphi$ be a monotone boolean formula. Then, for any assignations $\gamma_1, \gamma_2$ with $\gamma_1 \leq \gamma_2$ we have:

$$\gamma_1(\varphi) \leq \gamma_2(\varphi) .$$

**Proof.** All the elements that are true in $\gamma_1$ are also true in $\gamma_2$, and all the elements that are false in $\gamma_1$ may be true in $\gamma_2$. Therefore, the result is easily obtain.

**Example 3.4.4.** Let $\varphi = (x_1 \land x_2 \land x_3) \lor (x_2 \land x_4) \lor (x_1 \land x_3 \land x_4)$. For $\gamma(x_1) = \gamma(x_2) = 1$ and $\gamma(x_3) = 0$, we have $\gamma(\varphi) = 0$. For $\gamma'(x_1) = \gamma'(x_2) = \gamma'(x_4) = 1$ and $\gamma'(x_3) = 0$, we have $\gamma(\varphi) = 1$.

Moreover, $\gamma(\varphi) < \gamma'(\varphi)$.
For the evaluation of the boolean formulas, boolean circuits are used.

**Definition 3.4.5.** [63] Let $U$ be a set of boolean variables. A boolean circuit, denoted $C$, over $U$ is a finite directed acyclic graph that satisfies the following properties:

- any $i \in U$, that have no input arcs are labeled $i$, are called input nodes;
- there exists only one node with no output arcs, called output node;
- any intermediary nodes, that have both input and output arcs, are labeled $\land$, $\lor$ or $\neg$;
- any node is found on a path from a output node to a input node.

Similar to boolean formulas, a monoton boolean circuit does not contain nodes labeled with negations. Moreover, assignations can be further extended to include boolean circuits.

**Theorem 3.4.6.** [20, 18] Let $U$ be a set of $n$ participants and $U'$ the corresponding boolean variables. That is, for any participant $i \in U$ we assign a boolean variable $x_i \in U'$, and for any boolean variable $x_i \in U'$ there exists a participant $i \in U$.

1. For any access structure $\Gamma$ over $U$, there exists a monoton boolean formula $\varphi$ over $U'$ that is true exactly in any assignation $\gamma$ that marks authorized sets from $\Gamma$.

\[
(\forall A \in \Gamma) \left( (\forall i \in A) \left( \gamma(x_i) = 1 \right) \Rightarrow (\gamma(\varphi) = 1) \right)
\]

2. For any monoton boolean formula $\varphi$ over $U'$, there exists an access structure $\Gamma$ over $U$ that contains only those assignations that make $\varphi$ true.

\[
(\forall A' \in U') \left( (\exists A \in U) \left( (\forall x_i \in A') (i \in A) \right) \left( (\gamma|_{A'}(\varphi) = 1) \Rightarrow (A \in \Gamma) \right) \right)
\]

(Let $\gamma|_{A'}(\varphi)$ denote the restriction of the boolean formula $\varphi$ to the boolean variables in $A'$. Meaning, $\gamma(i) = 1$ for any $i \in A'$.)

**Proof.** The theorems are self-explanatory, if one examines the mathematical formulas above.

The above results can be naturally extended to include boolean circuits instead of boolean formulas.
Corollary 3.4.7. [20, 18] Let $U$ be a set of $n$ participants. Any participant $i \in U$ has assigned a boolean variable, also called $i$ for simplicity.

1. For any access structure $\Gamma$ over $U$, there exists a monoton boolean circuit $C$ over $U$ that is true exactly in any assignation $\gamma$ that marks authorized sets from $\Gamma$:

\[
(\forall A \in \Gamma_0) \left( (\forall i \in A) \left( \gamma(i) = 1 \right) \Rightarrow (\gamma(C) = 1) \right)
\]

(Recall that $\Gamma_0$ is the minimal access structure.)

2. For any monoton boolean circuit $C$ over $U$, there exists an access structure $\Gamma$ over $U$ that contains only those assignations that make $C$ true.

\[
(\forall A \in U) \left( (\gamma|_A(C) = 1) \Rightarrow (A \in \Gamma) \right)
\]

(Let $\gamma|_A(C)$ denote the restriction of the boolean circuit $C$ to the input nodes in $A$. Meaning, $\gamma(i) = 1$ for any $i \in A$.)

Proof. For any boolean formula $\varphi$ a boolean circuit $C$ can be constructed, and that for any boolean circuit $C$ a boolean formula $\varphi$ can be extracted. Therefore, the result of the corollary is obtained.

Next we present the algorithm proposed by Benaloh and Leichter [8] that constructs a perfect secret sharing scheme based on monoton boolean circuits.

Any perfect secret sharing schemes is described by an access structure, denoted $\Gamma$ (see Definition 3.3.11). Therefore, the monotone boolean circuit, denoted $C_{\Gamma_0}$, used in Algorithm 6 must satisfy the condition of Corollary 3.4.7 for $\Gamma_0$ (the basis of $\Gamma$).

Any node from $C_{\Gamma_0}$ is described by type (input, output or intermediary), by value ($\wedge$ or $\lor$) and by label (or labelSet). For any intermediary node there exists only one label, whereas for any input node there may exist multiple labels (contained in labelSet). Regarding the output nod, it will always be label with the shared secret.

Algorithm 6 shares a secret $s \in \mathbb{Z}_m$, by modifying the corresponding labels. Moreover, any participant $i \in U$ has the corresponding shares in labelSet.

For simplicity, we use the feature sons to enumerate all the nodes that have direct output arcs in the current nod.
3.4. Perfect realizations of access structures

input : \( Z_m, s \in Z_m \) and \( C_{\Gamma_0} \) over \( U \);
output: A secret sharing scheme \( (Z_m, (S_i, i \in U), F) \);

begin
  find Nod with type = output;
  update Nod.label as s;
  update Set as \{ Nod \};
  while Set not empty do
    take Nod from Set;
    update Set as Set - \{ Nod \};
    if Nod.value is \( \lor \) then
      for each Nod_i from Nod.sons do
        if Nod_i.type is input then
          update Nod_i.SetList as Nod_i.SetList \( \cap \) Nod.label;
        end
        update Nod_i.label with Nod.label;
      end
    end
    if Nod.value is \( \land \) then
      let \( n \) denote Nod.sons.length;
      generate \( a_1, \ldots, a_{n-1} \) values from \( Z_m \);
      compute \( a_n \) as Nod.label - \( \sum_{i=1}^{n-1} a_i \);
      for each Nod_i from Nod.sons do
        if Nod_i.type is input then
          update Nod_i.SetList as Nod_i.SetList \( \cup \) a_i;
        end
        update Nod_i.label with a_i;
      end
    end
  end
end

Algorithm 6: Benaloh and Leichter algorithm.
Example 3.4.8. [20] Let $U = \{x_1, x_2, x_3, x_4\}$ and $\Gamma_0 = \{\{x_1, x_2, x_3\}, \{x_1, x_2, x_4\}, \{x_1, x_3, x_4\}, \{x_2, x_3, x_4\}\}$. First, we obtain the boolean formula $\varphi$ as

$$\varphi = (x_1 \wedge x_2 \wedge x_3) \lor (x_1 \wedge x_2 \wedge x_4) \lor (x_1 \wedge x_3 \wedge x_4) \lor (x_2 \wedge x_3 \wedge x_4).$$

Secondly, we apply Algorithm 6 (see Figure 3.1).

Step 1. Output node is labeled with $s$.

Step 2. For output node as current node, we label sons (any $\wedge_i$ with $1 \leq i \leq 4$) with $s$.

Step 3. For each node $\wedge_i$ with $1 \leq i \leq 4$, generate $a_i^{(1)} \in \mathbb{Z}_m$ and $a_i^{(2)} \in \mathbb{Z}_m$, and compute $a_i^{(3)} = s - (a_i^{(1)} + a_i^{(2)}) \mod m$.

Step 4. List shares for each input node.

- $x_1.labelSet = \{a_1^{(1)}, a_2^{(1)}, a_3^{(1)}\}$
- $x_2.labelSet = \{a_1^{(2)}, a_2^{(2)}, a_4^{(1)}\}$
- $x_3.labelSet = \{a_1^{(3)}, a_3^{(2)}, a_4^{(2)}\}$
- $x_4.labelSet = \{a_2^{(3)}, a_3^{(3)}, a_4^{(3)}\}$

In Algorithm 6, any node that is labeled with $\wedge$ leads to a new distribution of shares, whereas for any node labeled with $\lor$ the same number of shares is used. Thus, the number of shares a participant $i$ receives is directly proportional to the number of nodes with the label $\wedge$, that are on paths leading to $i$ from the output node.

Theorem 3.4.9. [8] Let $U$ be a set of participants. There exists a perfect secret sharing scheme that realizes any access structure $\Gamma$ over $U$.

Proof. [20, 18] To simplify the proof, let $U$ also be the set of boolean variables used to generate the monoton boolean circuit $C_{\Gamma_0}$ from the minimal access structure $\Gamma_0$, according to Theorem 3.4.6 and Corollary 3.4.7.
3.5. Information rates

Let $|U| = n$ and $S = \mathbb{Z}_m$, for some $m > n$. Using Algorithm 6, we obtain the associated secret sharing scheme $(S, (S_i, i \in U), F)$ that shared $s \in \mathbb{Z}_m$.

The scheme $(S, (S_i, i \in U), F)$ is perfect (Theorem 3.3.14) if and only if for any $B \not\in \Gamma$, any $y \in S_B$ and any $s, s' \in S$ the following property holds

$$|\{f \in F_s \mid f|_B = y\}| = |\{f' \in F_{s'} \mid f|_B = y\}|.$$

Let $A \in \Gamma$ such that $A \cap B \neq \emptyset$, and $\alpha$ the shares that belong both to $s$ and $s'$ thru $A \cap B$:

$$\alpha = \sum_{i \in A \cap B} s_i = \sum_{i \in A \cap B} s'_i.$$

Assume that $A - B = \{i_1, \ldots, i_q\}$, then any shares of $s$ and $s'$ have to satisfy

$$\alpha + s_{i_1} + \cdots + s_{i_q} = s \mod m$$

$$\alpha + s'_{i_1} + \cdots + s'_{i_q} = s' \mod m$$

We define the rules $f \in F_s$ and $f' \in F_{s'}$ as $f(i) = f'(i)$ for any $i \in A \cap B$, and $f(i) = s_i$ and $f'(i) = s'_i$ for any $i \in A - B$.

According to the above construction, there exists an bijection $\phi$ from $|\{f \in F_s \mid f|_B = y\}|$ to $|\{f' \in F_{s'} \mid f|_B = y\}|$ such that $\phi(f(i)) = f'(i)$ for any $i \in A$.

Therefore, the result easily follows.

\[\square\]

3.5 Information rates

In the previous section we proved that any monotone access structure can be realized by a perfect secret sharing scheme. In this section we consider the efficiency of the resulting scheme. We measure the efficiency by the number of shares a participant must have to recover the secret.

**Definition 3.5.1.** Let $(S, (S_i, i \in U), F)$ be a secret sharing scheme. The information rate $\rho_i$ of the participant $i \in U$, denoted $\rho_i$, is

$$\rho_i = \frac{\log |S_i|}{\log |S|}.$$

The number of bits necessary to represent, in base 2, the set $X$ is given by $\log |X|$.

The information rate of a secret sharing scheme [13] is defined as the maximal information rate of any participant $i \in U$:

$$\rho = \max \{\rho_i \mid i \in U\}.$$

---

7 In [51] the information rate is defined without using log. Also, this will be the notation we adhere in our thesis.

8 In [13] the information rate of the participant $i \in U$ was defined as the fraction of $\log |S|$ over $\log |S_i|$. Therefore, we have adapted the definition of information rate to correspond to the notations used in this thesis.
Theorem 3.5.2. [58] For any perfect secret sharing scheme the information rate is greater than or equal to 1.

Proof. Let \((S, (S_i, i \in U), F)\) be a instance of a perfect secret sharing scheme that realizes an access structure \(\Gamma\) over \(U\).

We prove that \(\rho \geq 1\) by showing that there exists \(i \in U\) such that \(|S| \leq |S_i|\).

Let \(A \in \Gamma_0\) and \(i \in A\) for which there exists \(B \notin \Gamma\) such that \(A = B \cup \{i\}\). Moreover, let \(y \in S_A\) and \(y'\) the restriction of \(y\) to \(B\) (meaning, the share of \(i\) is not taken into consideration).

As the scheme is perfect, we have, based on Theorem 3.3.10, that \(P(s \mid y') = P(s)\), for any \(s \in S\).

Considering that \(P(s) > 0\) for any \(s \in S\), then there exists a rule \(f \in F_s\) such that \(f \mid_B = y'\). Meaning, that \(f \mid_B = y'\) can be obtain from any secret \(s \in S\).

According to Definition 3.3.4 and Proposition 3.3.9 there exists a single \(s\) for which \(f \mid_A = y\) can be obtain:

\[
\begin{align*}
&((\forall s, s' \in S)(s \neq s'))(\forall f \in F_s)(\forall f' \in F_{s'})(\forall A \in \Gamma) \Rightarrow f \mid_A \neq f' \mid_A \\
&\text{As } f \mid_B = y' \text{ can be obtain from any secret } s \in S, \text{ but } f \mid_A = y \text{ can be obtain from a single } s \in S, \text{ we have that} \\
&((\forall s, s' \in S)(s \neq s'))(\forall f \in F_s)(\forall f' \in F_{s'})(\forall A \in \Gamma) \Rightarrow f(i) \neq f'(i) .
\end{align*}
\]

Participant \(i\) receives shares from any secret \(s \in S\). Therefore, \(|S_i| \geq |S|\).

\[\square\]

Definition 3.5.3. [11] A secret sharing scheme is called \textit{ideal} if it is perfect and the information rate is equal to 1.

Theorem 3.5.4. [58] The KGH scheme is ideal.

Proof. From Theorem 3.3.15, we have that the KGH scheme is perfect. As the secret and share spaces are equal, the information rate is 1.

Therefore, the scheme is ideal.

\[\square\]

Theorem 3.5.5. [58] The Shamir scheme is ideal.

Proof. From Theorem 3.3.16, we have that the Shamir scheme is perfect. As the secret and share spaces are equal, the information rate is 1.

Therefore, the scheme is ideal.

\[\square\]
3.6 Classification of secret sharing schemes

In this section we classify secret sharing schemes based on the type of access structure used. For each subsection we define the corresponding access structure and describe at least one secret sharing scheme that realizes such structures.

To give a uniform aspect to our thesis, we present all the schemes in this section using a finite cyclic group.

3.6.1 Threshold secret sharing schemes

Threshold secret sharing schemes were independently introduced by Blakley [9] and Shamir [54]. The main characteristic of such schemes is the existence of a threshold \( t \) that denotes the number of participants needed for the recovery of the secret. Furthermore, the scheme should satisfy some security properties with respect to the secret reconstruction from less than \( t \) shares.

Definition 3.6.1. [54] Let \( U \) be a non-empty set of \( n \) participants, and \( t \) a positive integers with \( 1 \leq t \leq n \). A \((t,n)\)-threshold access structure, denoted \( \Gamma(t,n) \), over a set \( U \) is the access structure:

\[
\Gamma(t,n) = \{ A \in \mathcal{P}(U) \mid |A| \geq t \}.
\]

Indeed, \( \Gamma(t,n) \) satisfies the following monotonicity property:

\[
(\forall A \in \Gamma(t,n)) (\forall B \in \mathcal{P}(U)) (A \subseteq B \Rightarrow B \in \Gamma(t,n)).
\]

A \((t,n)\)-threshold secret sharing scheme is a scheme that realizes a \((t,n)\)-threshold access structure.

Lemma 3.6.2. [8] There exists monotone access structures for which there is no threshold secret sharing scheme.

Proof. Let \( U = \{1, 2, 3, 4\} \) and \( \Gamma \). Consider the access structure \( \Gamma \) over the set \( U = \{1, 2, 3, 4\} \) given by

\[
\Gamma_0 = \{\{1,2\}, \{3,4\}\}.
\]

Let \( a, b, c \) and \( d \) be the number of shares held by participants 1, 2, 3, and 4, respectively.

Assume that there exists a \((t,n)\)-threshold secret sharing scheme that realizes \( \Gamma \). Then, according to Definition 3.6.1, any set \( A \in \mathcal{P}(U) \) that satisfies \( |A| \geq t \) is authorized. Meaning, \( a + b \geq t \) and \( c + d \geq t \). Without loss of generality we may assume that \( a \leq b \) and \( c \leq d \).

As \( 2b \geq a + b \geq t \) and \( 2d \geq c + d \geq t \), we have \( b + d \geq t \). Therefore, the set \( A = \{2,4\} \) is authorized and belongs to \( \Gamma \). However, \( A \notin \Gamma \).

In conclusion, our assumption is false, and the result of the lemma follows. \( \square \)
Chapter 3. Secret Sharing Schemes

The Shamir threshold secret sharing scheme has been described in Section 3.3. Recall that the scheme is ideal (see Theorem 3.5.5). Therefore, we only give an example here.

**Example 3.6.3.** Consider the following example for the Shamir scheme, with \( n = 7 \), \( t = 3 \) and \( m = 13 \). We share the secret \( s = 4 \) using the polynomial \( q(x) = 5x^2 + 7x + 4 \), such that the corresponding shares are \( s_1 = 12 \), \( s_2 = 4 \), \( s_3 = 6 \), \( s_4 = 5 \), \( s_5 = 1 \), \( s_6 = 7 \), \( s_7 = 10 \).

Given the set \( A = \{1, 2, 3\} \), the secret can be computed as

\[
s = 12 \cdot \frac{2}{2-1} \cdot \frac{3}{3-1} + 4 \cdot \frac{1}{1-2} \cdot \frac{3}{3-2} + 6 \cdot \frac{1}{1-3} \cdot \frac{2}{2-3} \mod 13.
\]

Blakley has proposed in [9] the following threshold secret sharing scheme:

**Blakley scheme**

- **parameter**
  - consider \( U \) a set of \( n \) participants, and \( t \leq n \) the security parameter for which any set \( A \) that satisfies \( |A| \geq t \) can recover the secret;

- **secret and share spaces**
  - define the secret space as \( \mathbb{Z}_m^t \) and share spaces as \( \mathbb{Z}_m^{t+1} \);

- **secret sharing**
  - given a secret \( s = (x_1, \ldots, x_t) \) in \( \mathbb{Z}_m^t \), each participant \( i \) randomly generate \( t \) distinct elements \( a_{i,1}, \ldots, a_{i,t} \in \mathbb{Z}_m \) and computes \( b_i \in \mathbb{Z}_m \) as
    \[
    b_i = a_{i,1}x_1 + \cdots + a_{i,t}x_t.
    \]
  - The share of participant \( i \) is \( s_i = (a_{i,1}, \ldots, a_{i,t}, b_i) \).

- **secret reconstruction**
  - any set \( A \subseteq U \) of participants, with \( |A| \geq t \) can recover the secret, as \( s \) can be uniquely obtain by solving the system form by the shares \( s_i, \forall i \in A \).
    \[
    a_{i,1}x_1 + \cdots + a_{i,t}x_t = b_i \mod m, \forall i \in A.
    \]

**Theorem 3.6.4.** [11] The Blakley secret sharing scheme is perfect.

*Proof.* The proof is similar to that of Theorem 3.3.16, given for the Shamir scheme. Thus, is omitted.

**Remark 3.6.5.** The Blakley \((t, n)\)-threshold secret sharing scheme is not ideal, as the share space is larger than the secret space. However, with a trivial modification (dropping the value \( b_i \) for each participant \( i \)) the scheme becomes ideal. Meaning, the share of participant \( i \) is

\[
 a_{i,1}x_1 + \cdots + a_{i,t}x_t = 0.
\]

Proof. The secret and share spaces are equal, so the information rate is 1. Moreover, the scheme is perfect (according to Theorem 3.6.4).

Example 3.6.7. Consider the following example for the Blakley scheme, with \( n = 4, t = 2 \) and \( m = 9 \). Given the secret \( s = (4, 7) \in \mathbb{Z}_9 \), the corresponding shares are \( s_1 = (3, 2, 8), s_2 = (1, 8, 6), s_3 = (7, 3, 4) \) and \( s_4 = (4, 4, 8) \).

Let \( A = \{1, 2\} \). The secret \( s = (x_1, x_2) \) can be computed by solving the system

\[
3x_1 + 2x_2 = 8 \mod 9 \\
1x_1 + 8x_2 = 6 \mod 9
\]

Example 3.6.8. Consider the following example for the Blakley scheme modified according to Remark 3.6.5, with \( n = 4, t = 2 \) and \( m = 9 \). Given the secret \( s = (4, 7) \in \mathbb{Z}_9 \), the shares are \( s_1 = (3, 6), s_2 = (1, 2), s_3 = (7, 5) \) and \( s_4 = (4, 8) \).

Let \( A = \{1, 2\} \). The secret \( s = (x_1, x_2) \) can be computed by solving the system

\[
3x_1 + 6x_2 = 0 \mod 9 \\
1x_1 + 2x_2 = 0 \mod 9
\]

Consider the line \( 3x_1 + 2x_2 = 8 \). Eliminating \( b_1 = 8 \), we obtain a different line \( 3x_1 + 6x_2 = 0 \), that contains the point \( (4, 7) \).

3.6.2 Unanimous consent schemes

In unanimous consent schemes the presence of all the participants is required during the recovery of the secret. One may notice, unanimous consent schemes are particular cases of threshold secret sharing schemes were the threshold is equal to the total number of participants.

Definition 3.6.9. [56] Let \( U \) be a non-empty set of \( n \) participants. A unanimous consent access structure over \( U \) is the access structure:

\[ \Gamma = \{ U \} \]

According to the above definition, \( \Gamma \) satisfies the monotonicity property.

A unanimous consent secret sharing schemes is a scheme that realizes a unanimous consent access structure.

The scheme proposed by Karnin, Green and Hellman in [38], has been described in Section 3.3. Recall that the scheme is ideal (see Theorem 3.5.4).
Example 3.6.10. Consider the following example for the KGH scheme, with $n = 4$ and $m = 9$. Given the secret $s = 5$ in $\mathbb{Z}_9$, let a possible share distribution be $s_1 = 3$, $s_2 = 6$, $s_3 = 2$, $s_4 = 5$.

The secret $s$ is obtained by computing

$$s = 3 + 6 + 2 + 5 \mod 9.$$

Example 3.6.11. Consider the following example for the Shamir scheme, with $n = t = 3$ and $m = 13$. We share the secret $s = 2$ from $\mathbb{Z}_{13}$ using the polynomial $q(x) = 5x^2 + 3x + 2$, such that the corresponding shares are $s_1 = 10$, $s_2 = 2$, $s_3 = 4$.

The secret is obtained, from the all the shares, as

$$s = 10 \cdot \frac{2}{2-1} \cdot \frac{3}{3-1} + 2 \cdot \frac{1}{1-2} \cdot \frac{3}{3-2} + 4 \cdot \frac{1}{1-3} \cdot \frac{2}{2-3} \mod 13.$$

3.6.3 Weighted threshold secret sharing schemes

In weighted threshold secret sharing schemes, participants are assigned a positive weight according on their importance (or role). The secret can be reconstructed if and only if the sum of the weights assigned to a set of participants is greater than or equal to a fixed threshold.

This idea was proposed by Shamir [54] who also suggested a realization using tuples of polynomial values associated to each participant. In 1999, Morilo et al. [46] proposed a complete characterization of the weighted threshold access structures of rank two by using graph theory (the rank of a weighted threshold access structure is the maximum cardinality of the minimal authorized sets).

Later, Beimel et al. [4, 5] have proposed a characterization of ideal weighted threshold access structures by showing that weighted threshold access structures are ideal if and only if they are either hierarchical threshold access structures of at most three levels, or tripartite access structures, or compositions of two ideal weighted threshold access structures.

Definition 3.6.12. [46] A weighted threshold access structure (WTAS) over $U$ is a triple $(w, t, \Gamma)$, where:

1. $w : U \rightarrow \mathbb{R}_+^*$ is a function called the weight function;
2. $t > 0$ is a positive real number called threshold;
3. $\Gamma = \{ A \in \mathcal{P}(U) | w(A) \geq t \}$, where $w(A) = \sum_{x \in A} w(x)$, for any $A \in U$.

Indeed, $\Gamma$ satisfies the following monotonicity property:

$$\forall A \in \Gamma \left( \forall B \in \mathcal{P}(U) \right) (A \subseteq B) \Rightarrow B \in \Gamma.$$ 

A weighted threshold secret sharing schemes is a scheme that realizes a weighted threshold access structure.
3.6. Classification of secret sharing schemes

**Corollary 3.6.13.** [8] There exists monotone access structures for which there is no weighted threshold secret sharing scheme.

**Proof.** The proof is similar to the one given to Lemma 3.6.2, only let \( a, b, c, d \) be the weight of the participants, instead of the number of shares. \( \square \)

**Example 3.6.14.** Consider the following example for the Shamir scheme, with \( n = 4, t = 3 \) and \( m = 13 \). The secret \( s = 4 \) is shared by the polynomial \( q(x) = 5x^2 + 7x + 4 \), such that the weight function is \( w(1) = 2, w(2) = 1, w(3) = 2, w(4) = 2 \).

The corresponding shares are \( s_1 = (12, 4) \) from \( q(1) \) and \( q(2) \), \( s_2 = 6 \) from \( q(3) \), \( s_3 = (5, 1) \) from \( q(4) \) and \( q(5) \) and \( s_4 = (7, 10) \) from \( q(6) \) and \( q(7) \).

Let \( A = \{1, 2\} \), the secret is computed using Lagrange interpolation over \( q(1), q(2) \) and \( q(3) \):

\[
s = 12 \cdot \frac{2}{2} \cdot \frac{3}{3} - 1 + 4 \cdot \frac{1}{1} \cdot \frac{3}{3} - 2 + 6 \cdot \frac{1}{1} \cdot \frac{2}{2} - 3 \mod 13 .
\]

Wang, Liu and Zhang proposed in [64] the following weighted threshold secret sharing scheme based on polynomial reduction:

**Wang-Liu-Zhang (WLZ) scheme**

**parameter**
given a set \( U \) of \( n \) participants, consider \( w \) the weight function over the set \( U \), and \( t \) the security parameter for which any set \( A \) that satisfies \( \sum_{i \in A} w(i) \geq t \) can recover the secret. For simplicity, we note \( \sum_{i \in A} w(i) \) as \( w(A) \) for any \( A \subseteq U \);

**secret and share spaces**
define the secret space as \( \mathbb{Z}_m \) and share spaces as \( \mathbb{Z}_m^k \), where \( k = 1 + \max \{w_i \mid i \in U\} \). The share space of participant \( i \) depends on the identity \( x_i \) and the weight function assigned to \( i \);

**secret sharing**
given a secret \( s \in \mathbb{Z}_m \), randomly generate a polynomial \( f \) of degree \( t - 1 \) with the free coefficient \( s \).

\[
f(x) = \sum_{i=1}^{t-1} a_i x^i + s .
\]

The \( i \)th participant, receives the share

\[
s_i = (x_i, \text{REM}(f(x_i), (x - x_i)^{w_i})) ,
\]

where \( \text{REM}(f,g) \) is the remainder of polynomial \( f \) divided by polynomial \( (x - x_i)^{w_i} \) over \( \mathbb{Z}_m[x] \);

**secret reconstruction**
any set \( A \subseteq U \) with \( w(A) \geq t \) can recover the secret.
Example 3.6.15. Consider the following example for the WLZ scheme, with $U = \{1, 2, 3, 4, 5\}$, $t = 5$ and $m = 13$. The secret $s = 3$ is shared by the polynomial $f(x) = 4x^4 + 7x^3 + 2x^2 + 11x + 3$, such that the weight function is $w(1) = 2$, $w(2) = 3$, $w(3) = 2$, $w(4) = 1$, $w(5) = 1$.

For simplicity, let $x_i = i$ for all $1 \leq i \leq n$. The remainder of polynomial $f(x)$ divided by $(x - 1)^2$ is

$$g_1(x) = 0x + 1 \mod 13.$$ 

One may check that $f(x) = (4x^2 + 2x + 2) \cdot (x^2 - 2x + 1) + 1$. Meaning,

$$4x^4 + 7x^3 + 2x^2 + 11x + 3 = 4x^4 - 6x^3 + 2x^2 - 2x + 3.$$

(Recall that $7 = -6$ and $11 = -2$ in $\mathbb{Z}_{13}$.)

Then, the share of participant 1 is $s_1 = (1, (0, 1)) = (x_1, g_1(x))$.

The other shares are $s_2 = (2, (10, 9, 4))$, $s_3 = (3, (7, 0))$, $s_4 = (4, (4))$ and $s_5 = (5, (12))$.

Let $A = \{1, 2\}$ with $w(A) = 5 = t$. For participants 1 and 2, compute polynomials $k(x)$ and $h(x)$ such that

$$(x - 1)^2 \cdot h(x) + k(x) \cdot (x - 2)^3 = 1.$$ 

According to the polynomial form of the Chinese remainder theorem (see Section 2.2.6), we have

$$h(x) = 3x^2 - x + 4$$
$$k(x) = 10x + 2.$$ 

Therefore, the solution can be computed as

$$f(x) = g_1(x)k(x)(x - 2)^3 + g_2(x)h(x)(x - 1)^2 \mod (x - 1)^2(x - 2)^3$$
$$= 4x^6 - 4x^5 - 3x^4 - 4x^3 - x^2 + 9x \mod (x - 1)^2(x - 2)^3$$
$$= 4x^4 - 6x^3 - 11x^2 - 2x + 3 \mod (x - 1)^2(x - 2)^3$$
$$= 4x^4 + 7x^3 + 2x^2 + 11x + 3.$$ 

3.6.4 Multilevel secret sharing schemes

In multilevel secret sharing schemes [55, 60, 5, 6], the participants are divided in disjoint levels according to their importance. The participants on lower levels are more important than participants on higher levels.

Two types of access structures for multilevel secret sharing schemes have been proposed so far, namely disjunctive multilevel access structures [55] and conjunctive multilevel access structures [60] (the terms disjunctive and conjunctive were proposed in [6]).

The difference between these two types of access structures is given by the number of participants needed for the recovery. Let $U_1, \ldots, U_q$ be $q$ levels, where $U_1$ is the lowest one. Each level $U_i$ has associated a threshold $t_i$, such that $t_1 < \cdots < t_q$. In disjunctive multilevel access structures the group of participants reconstruct the secret at some level $1 \leq i \leq q$ if at least $t_i$ participants are taken from $\bigcup_{j=1}^{i} U_j$. Whereas, in conjunctive multilevel
access structures the participants recover the secret for all levels $1 \leq i \leq q$ if at least $t_i$ participants are taken from $\bigcup_{j=1}^{q} U_j$.

**Definition 3.6.16.** [55] 
A *disjunctive multilevel access structure* (DMAS) over a set $U$ of participants is a tuple $(\mathcal{U}, \mathcal{T}, \Gamma)$, where

1. $\mathcal{U} = (U_1, \ldots, U_q)$ is a partition of $U$ called *levels* (that is, all $U_i$ are non-empty and their union is $U$);

2. $\mathcal{T} = (t_1, \ldots, t_q)$ is a vector of positive integers called *thresholds* that satisfies $0 < t_1 < \cdots < t_q$;

3. $\Gamma = \{A \subseteq U | \exists 1 \leq i \leq q (|A \cap (\bigcup_{j=1}^{i} U_j)| \geq t_i)\}$.

Ghodosi, Pieprzyk and Safavi-Naini have proposed in [28] an ideal secret sharing scheme. Their method is to extend the polynomial used by the previous level. Meaning, the extended polynomial gives the same values as the previous polynomial for any participant from the previous level.

**Definition 3.6.17.** [28] Let $f_1(x)$ be a random polynomial of degree $T_1$ over the set $U_1$, with $|U_1| \geq T_1$. The *extension* of $f_1$ is the polynomial $f_2$ of degree $T_2 (> T_1)$, that satisfies the following properties:

1. $f_2(i) = f_1(i)$ for all $i \in U_1$;

2. $f_2(0) = f_1(0)$ (they share the same secret).

Ghodosi et al. [28] have proposed the following disjunctive multilevel secret sharing scheme:

**Ghodosi-Pieprzyk-Safavi-Naini (DMAS-GPS) 10** scheme

<table>
<thead>
<tr>
<th>parameter</th>
<th>setup</th>
<th>secret and share spaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>given a set $U$ of participants, consider $\mathcal{U} = (U_1, \ldots, U_q)$ a partition of $U$, with $</td>
<td>U_i</td>
<td>= n_i$ for any $1 \leq i \leq q$. Let $0 &lt; t_1 &lt; \cdots &lt; t_q$ be a sequence of positive thresholds; define the secret space and share spaces as $\mathbb{Z}_m$;</td>
</tr>
</tbody>
</table>

---

*Simmons [55] called them multilevel access structures. Later, Tassa [60] and Beimel et al. [5] called them hierarchical threshold access structures, and Belenkiy [6] called them disjunctive multilevel access structures and used conjunctive multilevel access structures for the access structures introduced by Tassa.*

*In [28], two schemes are proposed. One that considers multilevel access structures, denoted DMAS-GPS, and another scheme that considers compartmented access structures, denoted C-GPS.*
secret sharing} given a secret \( s \in \mathbb{Z}_m \), randomly generate a polynomial \( f_1 \) of degree \( T_1 \). Then, compute the polynomial \( f_i \) as the extension of \( f_{i-1} \) for any \( 2 \leq i \leq q \). The share of \( j \)th participant from level \( i \), denoted \((i,j)\) is \( s_{i,j} = f_i(j) \mod m \).

**secret reconstruction** any set \( A \subseteq U \), for which there exists \( 1 \leq i \leq q \) such that \( |A \cap \cup_{j=1}^i U_j| \geq t_i \), can recover the secret.

We prove that for any polynomial \( f_1 \) of degree \( T_1 \), there exists an extended polynomial \( f_2 \) of degree \( T_2 \). The result of the following lemma can be extended to include the general case.

**Lemma 3.6.18.** [28] Given a polynomial \( f_1 \) of degree \( T_1 \), over the set \( U_1 \), there exists an extended polynomial \( f_2 \) of degree \( T_2 > t_2 - 1 \) over the set \( U_2 \).

**Proof.** Let \( f_1(x) = s + a_{1,1}x + \cdots + a_{1,T_1}x^{T_1} \) be the polynomial that shares the secret \( s \) to the participants in level \( U_1 \). Extend \( f_1 \) to the polynomial \( f_2(x) = s + a_{2,1}x + \cdots + a_{2,T_2}x^{T_2} \). Recall that \( |U_1| = n_1 \) and \( |U_2| = n_2 \).

As \( f_2(i) = f_1(i) \) for all \( i \in U_1 \), we have the following \( 2 \cdot N_1 \) equations:

\[
\begin{align*}
    s + a_{1,1,i} + \cdots + a_{1,T_1,i}^{T_1} &= s_{1,i}, \quad \forall i \in U_1 \\
    s + a_{2,1,i} + \cdots + a_{2,T_2,i}^{T_2} &= s_{1,i}, \quad \forall i \in U_1
\end{align*}
\]

The first set is from \( f_1 \), the second due to \( f_2 \), but both consider the participants in \( U_1 \).

The number of unknowns for the above system is \( 1 + T_1 + T_2 + n_1 \).

At least \( t_2 \) participants from \( U_2 \) must recover the secret \( s \). Therefore, we have the additional equations

\[
    s + a_{2,1,i} + \cdots + a_{2,T_2,i}^{T_2} = s_{2,i}, \quad \forall i \in A,
\]

where \( A \subseteq U_2 \) with \( |A| \geq t_2 \).

The above system of equations admits a unique solution, if \( 2n_1 + t_2 = 1 + T_1 + T_2 + n_1 \). Thus, \( T_2 \) can be greater or equal to \( n_1 + (t_2 - t_1) \).

Now, given \( A \subseteq (U_1 \cup U_2) \) with \( |A| = t_2 \) and \( |A \cap U_1| = j \). Regardless of the number \( j \), there are still \( n_1 \) unknown shares in the newly obtained system. Therefore, \( T_2 = n_1 + (t_2 - t_1) \). \( \square \)

**Theorem 3.6.19.** [28] The DMAS-GPS scheme is ideal.

**Proof.** The secret and share spaces are equal. Meaning, the information rate assigned to this scheme is 1.

For any \( B \notin \Gamma \), let \( B_i = B \cap (\cup_{j=1}^i U_i) \) be the participants taken from the levels leading to \( i \), and \( \beta_i = |B_i| \). As \( \beta_i < t_i \) the system of equation for the \( i \)th level does not give a unique solution.

The perfectness is obtained similar to the Shamir scheme (see Theorem 3.3.16) \( \square \)
Example 3.6.20. Consider the following example for the DMAS-GPS scheme with $q = 2, m = 13, t_1 = 2$ and $t_2 = 4$. The set of participants is partitioned into $U_1 = \{1, 2, 3, 4\}$ and $U_2 = \{5, 6, 7, 8\}$.

We share the secret $s = 3$, using $f_1(x) = 4x + 3$ to the participants of the first level, so $s_{1,1} = 7$ from $f_1(1)$, $s_{1,2} = 11$ from $f_1(2)$, $s_{1,3} = 2$ from $f_1(3)$ and $s_{1,4} = 6$ from $f_1(4)$. (Note that $T_1 = 1$.)

Compute the extended polynomial
\[ f_2(x) = a_6 x^6 + \cdots + a_1 x + 3 \]
with $T_2 = 6$ such that $f_2(i) = f_1(i)$ for any $i \in U_1$. (Note that $T_2 = |U_1| + (t_2 - t_1)$.)

As the following system of equations has 6 unknown coefficients $(a_6, \ldots, a_1)$ and 4 equations
\[ f_2(i) = s_{1,i}, \forall i \in U_1 \]
one may obtain the solution $(3, 2, 6, 8, 6, 5)$ in $\mathbb{Z}_{13}$. The solution is not unique, as the purpose of the extension is to generate a polynomial that satisfies $f_2(i) = f_1(i)$ for any $i \in U_1$.

We check $f_2(1) = 7$, $f_2(2) = 11$, $f_2(3) = 2$ and $f_2(4) = 6$. The participants on the second level receive $s_{2,1} = 8$ from $f_2(5)$, $s_{2,2} = 4$ from $f_2(6)$, $s_{2,3} = 3$ from $f_2(7)$ and $s_{2,4} = 5$ from $f_2(8)$.

Let $A = \{5, 6, 7, 8\}$ with $|A| = 4 \geq t_2$. For the recovery of the secret $s$, one has to solve the following system of equations
\[ f_1(i) = s_{1,i}, \forall i \in U_1 \]
\[ f_2(i) = s_{1,i}, \forall i \in U_1 \]
\[ f_2(i) = s_{2,i}, \forall i \in A . \]

As the above system has $2n_1 + t_2 = 12$ equations and $1 + T_1 + T_2 + n_1 = 12$ unknown coefficients and shares, there exists a unique solution. Therefore, $s$ can be obtained. (The identity of the participants is public.)

Tassa proposed in [60] the following disjunctive multilevel secret sharing scheme, based on Birkhoff interpolation:

**Disjunctive Tassa (DMAS-Tassa) \(^{11}\) scheme**

**parameter**
given a set $U$ of participants, consider $\overline{U} = (U_1, \ldots, U_q)$

**setup**
a partition of $U$, with $|U_i| = n_i$ for any $1 \leq i \leq q$. Let $0 < t_1 < \cdots < t_q$ be a sequence of positive thresholds;

**secret and share spaces**
define the secret space and share spaces as $\mathbb{Z}_m$;

---

\(^{11}\) In [60], two schemes are proposed. One that considers disjunctive multilevel access structures, denoted DMAS-Tassa, and another scheme that considers conjunctive multilevel access structures, denoted CMAS-Tassa.
secret sharing \[s \in \mathbb{Z}_m,\] randomly generate a polynomial \(f\) of degree \(t_q - 1\) with the dominant coefficient \(s\).
\[f(x) = sx^{t_q - 1} + a_{t_q - 2}x^{t_q - 2} + \cdots + a_0x^0.\]

The \(j\)th participant from level \(i\), denoted \((i,j)\), receives the share \(s_{i,j} = f^{(t_q - t_i - 1)}(j) \mod m\), where \(f^{(t_q - t_i - 1)}\) is the \((t_q - t_i - 1)\) derivative of \(f(x)\) and \(t_{i-1} = 0\).

secret reconstruction any set \(A \subseteq U\) with \(|A \cap \bigcup_{j=1}^{i} U_j| \geq t_i\) for some \(1 \leq i \leq q\), can recover the secret.

Example 3.6.21. Consider the following example for the DMAS-Tassa scheme, with \(q = 2\), \(m = 13\), \(t_1 = 3\) and \(t_2 = 5\). The set of participants is partitioned into \(U_1 = \{1, 2, 3, 4, 5\}\) and \(U_2 = \{6, 7, 8, 9, 10\}\). To share the secret \(s = 2\) we generate the polynomial
\[f(x) = 2x^4 + 5x^3 + 7x + 3\]
and compute the derivate polynomial
\[f^{(2)}(x) = 11x^2 + 4x.\]

The polynomial \(f^{(2)}(x)\) is associated to the first level, so the shares are: \(s_{1,1} = 2, s_{1,2} = 0, s_{1,3} = 7, s_{1,4} = 10\) and \(s_{1,5} = 9\). The shares from the second level are \(s_{2,6} = 12, s_{2,7} = 4, s_{2,8} = 8, s_{2,9} = 11\) and \(s_{2,10} = 9\), due to \(f(x)\).

Let \(A = \{1, 2, 3\}\) with \(|A \cap C_1| = 3 = t_1\). For the recovery of the secret \(s\), one has to solve the following system of equations
\[f^{(2)}(i) = s_{1,i}, \forall i \in \{1, 2, 3\}\]
The system has 3 equations and 3 unknown coefficients. Therefore, \(s\) can be uniquely obtained.

Let \(A = \{1, 2, 3, 6, 7\}\) with \(|A \cap (C_1 \cup C_2)| = 5 = t_2\). For the recovery of the secret \(s\), one has to solve the following system of equations
\[f^{(2)}(i) = s_{1,i}, \forall i \in \{1, 2, 3\}\]
\[f(i) = s_{2,i}, \forall i \in \{6, 7\}\]
The coefficients of \(f\) are \(a_0, \ldots, a_4\), and the coefficients of \(f^{(2)}\) are \(4 \cdot 3 \cdot a_4, 3 \cdot 2 \cdot a_3\) and \(2 \cdot a_2\). Thus, the system has 5 equations and 5 unknown coefficients.

Therefore, \(s\) can be uniquely obtained.

Kasper, Nikov and Nikova have proposed in [39] the following disjunctive multilevel scheme.
3.6. Classification of secret sharing schemes

Disjunctive Kasper-Nikov-Nikova (DMAS-KNN) scheme

Parameter

Consider $U = (U_1, \ldots, U_q)$ a partition of participants, with $|U_i| = n_i$ for any $1 \leq i \leq q$. Let $0 < t_1 < \cdots < t_q$ be a sequence of positive thresholds.

Setup

Define the secret space and share spaces as $\mathbb{Z}_m$.

Secret and share spaces

Given a secret $s \in \mathbb{Z}_m$, randomly generate a polynomial $f_1$ of degree $t_1 - 1$

$$f_1(x) = a_{t_1-1}x_{t_1-1} + \cdots + a_1x + s$$

Then, compute the polynomial $f_i$ as the particular extension of $f_{i-1}$ for any $2 \leq i \leq q$, such that

$$f_i(x) = a_{t_i-1}x_{t_i-1} + \cdots a_{t_{i-1}}x_{t_{i-1}}^{t_{i-1}} + f_{i-1}(x) \mod m.$$  

The share of the $j$th participant from level $i$, denoted $(i,j)$ is $s_{i,j} = f_i(j) \mod m$.

Secret reconstruction

Any set $A \subseteq U$, for which there exists $1 \leq i \leq q$ such that $|A \cap \bigcup_{j=1}^i U_j| \geq t_i$, can recover the secret through polynomial interpolation.

Example 3.6.22. Consider the following example for the DMAS-KNN scheme, with $q = 2$, $m = 13$, $t_1 = 3$ and $t_2 = 4$. The set of participants is partitioned into $U_1 = \{1, 2, 3, 4, 5\}$ and $U_2 = \{6, 7, 8, 9, 10\}$. To share the secret $s = 3$, we generate the following polynomials:

$$f_1(x) = 2x^2 + 4x + 3$$

$$f_2(x) = 7x^3 + 2x^2 + 4x + 3$$

Polynomial $f_2(x)$ must contain the polynomial $f_1$.

The share are $s_{1,1} = 9, s_{1,2} = 6, s_{1,3} = 7, s_{1,4} = 12, s_{1,5} = 8, s_{2,1} = 12, s_{2,2} = 8, s_{2,3} = 3, s_{2,4} = 0$ and $s_{2,5} = 2$.

Let $A = \{1, 5, 7, 8\}$ with $|A \cap (C_1 \cup C_2)| = 4 \geq t_2$. For the recovery of the secret $s$, one has to solve the following system of equations

$$f_1(1) = s_{1,1}$$

$$f_2(i) = s_{2,i}, \forall i \in \{5, 7, 8\}.$$  

The system has 4 equations and 4 unknown coefficients. Therefore, $s$ can be uniquely obtained.

\[\text{In [39], two schemes are proposed. One that considers disjunctive multilevel access structures, denoted DMAS-KNN, and another scheme that considers conjuctive multilevel access structures, denoted CMAS-KNN. Furthermore, the DMAS-KNN scheme is a more simpler variant of the DMAS-Tassa scheme.}\]
Chapter 3. Secret Sharing Schemes

Definition 3.6.23. [60] A conjunctive multilevel access structure (CMAS) over a set $U$ of participants is a tuple $(\overline{U}, \overline{t}, \Gamma)$, where

1. $\overline{U} = (U_1, \ldots, U_q)$ is a partition of $U$ called levels (that is, all $U_i$ are non-empty and their union is $U$);
2. $\overline{t} = (t_1, \ldots, t_q)$ is a vector of positive integers called thresholds that satisfies $0 < t_1 < \cdots < t_q$;
3. $\Gamma = \{ A \subseteq U | (\forall 1 \leq i \leq q)(|A \cap (\bigcup_{j=1}^{i} U_j)| \geq t_i) \}$.

Tassa proposed in [60] the following conjunctive multilevel secret sharing scheme, based on Birkhoff interpolation:

Conjunctive Tassa (CMAS-Tassa)\(^{13}\) scheme

- **Parameter**
  - Given a set $U$ of participants, consider $\overline{U} = (U_1, \ldots, U_q)$ a partition of $U$, with $|U_i| = n_i$ for any $1 \leq i \leq q$. Let $0 < t_1 < \cdots < t_q$ be a sequence of positive thresholds;

- **Secret and Share Spaces**
  - Define the secret space and share spaces as $\mathbb{Z}_m$;

- **Secret Sharing**
  - Given a secret $s \in \mathbb{Z}_m$, randomly generate a polynomial $f$ of degree $t_q - 1$ with the free coefficient $s$.
  - $f(x) = \sum_{i=1}^{t_q-1} a_i x^i + s$.
  - The $j$th participant from level $i$, denoted $(i,j)$, receives the share $s_{i,j} = f^{(t_{i-1})}(j) \mod m$, where $f^{(t_{i-1})}$ is the $t_{i-1}$ derivative of $f(x)$ and $t_{i-1} = 0$.

- **Secret Reconstruction**
  - Any set $A \subseteq U$ with $|A \cap (\bigcup_{j=1}^{i} U_j)| \geq t_i$ for all $1 \leq i \leq t_q$, can recover the secret.

Example 3.6.24. Consider the following example for the CMAS-Tassa scheme, with $q = 2$, $m = 13$, $t_1 = 3$ and $t_2 = 5$. The set of participants is partitioned into $U_1 = \{1, 2, 3, 4, 5\}$ and $U_2 = \{6, 7, 8, 9, 10\}$. To share the secret $s = 3$, we generate the polynomial

\[ f(x) = 2x^4 + 5x^3 + 7x + 3 \]

and compute the derivate polynomial

\[ f^{(3)}(x) = 9x + 4 \]

\(^{13}\) See footnote 11.
3.6. Classification of secret sharing schemes

The share are \( s_{1,1} = 4, s_{1,2} = 11, s_{1,3} = 9, s_{1,4} = 5, s_{1,5} = 2 \) obtained from \( f(x) \), and \( s_{2,6} = 6, s_{2,7} = 2, s_{2,8} = 11, s_{2,9} = 7 \) and \( s_{2,10} = 3 \) obtained from \( f^{(3)}(x) \).

Let \( A = (1, 2, 3, 4, 5) \) with \( |A| = 5 \geq t_2 \) and \( |A \cap C_1| = 5 > t_1 \) and \( |A \cap (C_1 \cup C_2)| = 5 = t_2 \). For the recovery of the secret \( s \), one has to solve the following system of equations

\[
\begin{align*}
\forall i \in \{1, 2, 3, 4, 5\} : f(i) &= s_{1,i} \\
\forall i \in \{6, 7\} : f^{(3)}(i) &= s_{2,i}
\end{align*}
\]

The system has 5 equations and 5 unknown coefficients. Therefore, \( s \) can be uniquely obtained.

Let \( A = \{1, 2, 3, 6, 7\} \) with \( |A| = 5 \geq t_2 \) and \( |A \cap C_1| = 3 = t_1 \) and \( |A \cap (C_1 \cup C_2)| = 5 = t_2 \). For the recovery of the secret \( s \), one has to solve the following system of equations

\[
\begin{align*}
\forall i \in \{1, 2, 3\} : f(i) &= s_{1,i} \\
\forall i \in \{6, 7\} : f^{(3)}(i) &= s_{2,i}
\end{align*}
\]

Notice that if the coefficients of \( f \) are \( a_0, \ldots, a_4 \), then the coefficients of \( f^{(3)} \) are \( 4 \cdot 3 \cdot 2 \cdot a_4 \) and \( 3 \cdot 2 \cdot a_3 \). Thus, the system has 5 equations and 5 unknown coefficients.

Therefore, \( s \) can be uniquely obtained.

Kasper, Nikov and Nikova have proposed in [39] the following conjunctive multilevel scheme

**Conjunctive Kasper-Nikov-Nikova (CMAS-KNN) \(^{14}\)** scheme

- **Parameter**: consider \( \mathcal{U} = (U_1, \ldots, U_q) \) a partition of participants, with \( |U_i| = n_i \) for any \( 1 \leq i \leq q \). Let \( 0 < t_1 < \cdots < t_q \) be a sequence of positive thresholds;

- **Secret and share spaces**: define the secret space and share spaces as \( \mathbb{Z}_m \);

- **Secret sharing**: given a secret \( s \in \mathbb{Z}_m \), randomly generate a polynomial \( f_1 \) of degree \( t_q - 1 \)

\[
f_1(x) = a_{t_q-1}x^{t_q-1} + \cdots + a_1x + s
\]

Then, compute the polynomial \( f_i \) as the particular extension of \( f_{i-1} \) for any \( 2 \leq i \leq q \), such that

\[
f_i(x) = a_{t_q-t_{i-1}}x^{t_q-t_{i-1}} + \cdots + a_1x^1 + s \mod m.
\]

The share of the \( j \)th participant from level \( i \), denoted \((i,j)\), is \( s_{i,j} = f_i(j) \mod m \).

\(^{14}\) See footnote 12. The CMAS-KNN scheme is a more simpler variant of the CMAS-Tassa scheme.
secret reconstruction any set \( A \subseteq U \), for which there exists \( 1 \leq i \leq q \) such that \(|A \cap \bigcup_{j=1}^{i} U_j| \geq t_i\), can recover the secret through polynomial interpolation.

Example 3.6.25. Consider the following example for the CMAS-KNN scheme, with \( q = 2 \), \( m = 13 \), \( t_1 = 1 \) and \( t_2 = 4 \). The set of participants is partitioned into \( U_1 = \{1, 2, 3, 4, 5\} \) and \( U_2 = \{6, 7, 8, 9, 10\} \). To share the secret \( s = 6 \), we generate the following polynomials

\[
\begin{align*}
f_1(x) &= 3x^3 + 4x^2 + 7x + 6 \\
f_2(x) &= 4x^2 + 7x + 6
\end{align*}
\]

The polynomial \( f_2(x) \) is obtained from polynomial \( f_1 \).

The share are \( s_{1,1} = 7 \), \( s_{1,2} = 8 \), \( s_{1,3} = 1 \), \( s_{1,4} = 4 \), \( s_{1,5} = 9 \), \( s_{2,6} = 10 \), \( s_{2,7} = 4 \), \( s_{2,8} = 6 \), \( s_{2,9} = 3 \) and \( s_{2,10} = 8 \).

Let \( A = \{1, 5, 7, 8\} \) with \( |A \cap C_1| = 1 \geq t_2 \) and \( |A \cap (C_1 \cup C_2)| = 4 \geq t_2 \).

For the recovery of the secret \( s \), one has to solve the following system of equations

\[
\begin{align*}
f_1(1) &= s_{1,1} \\
f_2(i) &= s_{2,i}, \forall i \in \{5, 7, 8\}
\end{align*}
\]

The system has 4 equations and 4 unknown coefficients. Therefore, \( s \) can be uniquely obtained.

3.6.5 Compartmented secret sharing schemes

In compartment secret sharing schemes \([55, 11, 28, 62]\) the participants are assigned into disjoint sets. Similar to multilevel schemes, each compartment is characterized by a threshold. That is, authorized sets must take participants from each compartment. Moreover, there exists a global threshold that establishes the number of participants needed to recover the secret. Depending on the restriction imposed to the number of participants that take part in the recovery of the secret there are two types of compartment schemes: with lower bounds \([55, 11, 28]\), or with upper bounds \([62]\).

**Definition 3.6.26.** \([55]\) A compartmented access structure with lower bounds\(^{15}\) over a set \( U \) of participants is a tuple \((\mathcal{C}, t, \Gamma)\), where

1. \( \mathcal{C} = (C_1, \ldots, C_q) \) is a partition of \( U \) called compartments (that is, all \( C_i \) are non-empty and their union is \( U \));
2. \( t = (t_1, \ldots, t_q, t) \) is a vector of positive integers called thresholds that satisfy \( 0 < t_1 < \cdots < t_q \) and \( t_1 + \cdots + t_q \leq t \);
3. \( \Gamma = \{ A \subseteq U | (\forall 1 \leq i \leq q) (|A| = t_i) \land (|A \cap \bigcup_{j=1}^{i} C_j| \geq t_i) \} \).

\(^{15}\) Simmons called them compartmented access structure, and Tassa et al. \([62]\) called them compartmented access structure with lower bounds.
Ghodosi, Pieprzyk and Safavi-Naini have proposed in [28] an ideal secret sharing scheme. The scheme has two cases depending on the difference between $t$ and $t_1 + \cdots + t_q$. Let $T = t - (t_1 + \cdots + t_q)$. If $T = 0$ it means the global threshold is equal to the sum of all the compartment thresholds, otherwise $T > 0$ means the global threshold is greater to the sum of all the compartment thresholds.

**Compartment Ghodosi-Pieprzyk-Safavi-Naini (C-GPS)** scheme

- **Parameter** consider $C = (C_1, \ldots, C_q)$ a partition of participants, with $|C_i| = n_i$ for any $1 \leq i \leq q$. Let $0 < t_1 < \cdots < t_q$ be a sequence of positive thresholds, $t$ the global threshold, and $T = t - (t_1 + \cdots + t_q)$.

- **Secret and share spaces** define the secret space as and share spaces as $\mathbb{Z}_m$.

- **Secret sharing** given a secret $s \in \mathbb{Z}_m$, randomly generate $(q - 1)$ coefficients $a_{q-1}, \ldots, a_1$ from $\mathbb{Z}_m$ such that the polynomial $f$ is obtained:

  $$f(x) = a_{q-1}x^{q-1} + \cdots + a_1x + s \mod m.$$  

  For each compartment $i$ a partial secret $f(i)$ is computed, for all $1 \leq i \leq q$. Then, $f(i)$ is shared to all the participant in $C_i$, using a polynomial $g_i$ of degree $(t_i + T - 1)$

  $$g_i(x) = f(i) + \sum_{j=1}^{t_i-1} a_{i,j}x^j + \sum_{j=1}^{T} b_jx^{t_i-1+i} \mod m.$$  

  The values $b_T, \ldots, b_1$ are generated only once, while the coefficients $a_{i,t_i-1}, \ldots, a_{i,1}$ are randomly generated for each compartment $i$.

  The share of the $j$th participant from level $i$, denoted $(i, j)$ is $s_{i,j} = g_i(j) \mod m$.

- **Secret reconstruction** any $t_i$ participants from each compartment $i$ recovers, using Lagrange interpolation, the polynomial $g_i(x)$ (or more precisely the partial secret $f(i)$) for any $1 \leq i \leq q$. Another interpolation is needed, over the points $(i, f(i))$ for all $1 \leq i \leq q$, to extract the secret $s$.

**Theorem 3.6.27.** [28] The C-GPS scheme is ideal.

*Proof.* We prove that the C-GPS scheme realizes the access structure $\Gamma$. Let $A \in \Gamma$ with $|A| = \alpha$ and $|A \cap C_i| = \alpha_i$. As there must be at least $t_i$
participants from the each compartment $C_i$, we have $\alpha_i \geq t_i$. Moreover, $t \leq \alpha$.

For any $j \in A \cap C_i$ and any $1 \leq i \leq q$, we have the following system

$$g_i(j) = b_{T}j^{t_{i}+T-1} + \cdots + b_{1}j^{t_{i} + a_{i_{1}t_{i}}-1} + \cdots + a_{i_{1}j_{i}} + f(i) \mod m.$$ 

There are $t$ unknown coefficients and $\alpha$ equations. There exits a unique solution, so one can obtain $f(1), \ldots, f(q)$. (Recall that $T + t_1 + \cdots + t_q = t$, and $\alpha_1 + \cdots + \alpha_q = \alpha$.)

Now, the polynomial $f(x)$ can be uniquely deduced, and the secret $s$ recovered.

We prove the scheme is perfect. Let $B \notin \Gamma$ and $|B \cap C_i| = \alpha_i$. So, there exists a compartment $i$ such that $\alpha_i < t_i$, or $\alpha < t$. Both situations lead to the fact that there is no unique solution for the equation system (see Theorem 3.3.16 for the Shamir scheme).

**Example 3.6.28.** Consider the following example for the C-GPS scheme, with $q = 2$, $m = 13$, $t_1 = 3$, $t_2 = 4$ and $t = 7$. ($T = 0$). The set of participants is partitioned into $U_1 = \{1, 2, 3, 4, 5\}$ and $U_2 = \{6, 7, 8, 9, 10\}$.

To share the secret $s = 3$, we first generate

$$f(x) = 4x + 3$$ 

and compute the partial secrets $f(1) = 7$ and $f(2) = 11$ in $\mathbb{Z}_{13}$.

For the two compartments, we randomly generate the following polynomials

$$g_1(x) = 5x^2 + 3x + 7,$$

$$g_2(x) = 4x^3 + 4x^2 + 3x + 11.$$ 

The share are $s_{1,1} = 2, s_{1,2} = 7, s_{1,3} = 9, s_{1,4} = 8, s_{1,5} = 4$ for the first compartment, and $s_{2,6} = 10, s_{2,7} = 1, s_{2,8} = 12, s_{2,9} = 2, s_{2,10} = 8$ for the second compartment.

Let $A = \{1, 2, 3, 6, 7, 8, 9\}$ with $|A| = 7 \geq t$, $|A \cap C_1| = 3 = t_1$ and $|A \cap C_2| = 4 = t_2$. For the recovery of the secret $s$, one has to solve the following system of equations

$$a_{1,2}i^2 + a_{1,1}i + a_{1,0} = s_{1,i}, \forall i \in \{1, 2, 3\}$$

$$a_{2,3}i^3 + a_{2,2}i^2 + a_{2,1}i + a_{2,0} = s_{1,i}, \forall i \in \{6, 7, 8, 9\}$$

The above system has 7 equations and 7 unknown coefficients. Therefore, $s$ can be uniquely obtained.

Let $A = \{1, 2, 5, 7, 8, 9, 10\}$ with $|A| = 7 \geq t$, $|A \cap C_1| = 3 = t_1$ and $|A \cap C_2| = 4 = t_2$. Similarly, one has 7 equations and 7 unknown coefficients. Thus, the secret $s$ is obtained.
Definition 3.6.29. [62] A compartmented access structure with upper bounds over a set $U$ of participants is a tuple $(\mathcal{C}, \bar{t}, \Gamma)$, where

1. $\mathcal{C} = (C_1, \ldots, C_q)$ is a partition of $U$ called compartments (that is, all $C_i$ are non-empty and their union is $U$);

2. $\bar{t} = (t_1, \ldots, t_q, t)$ is a vector of positive integers called thresholds that satisfy $0 < t_1 < \cdots < t_q$ and $(t_1 + \cdots + t_q) \geq t$;

3. $\Gamma = \{ A \subseteq U | (\forall 1 \leq i \leq q)((|A| = t) \land (|A \cap (\cup_{j=1}^{i} C_j)| \leq t_i)\}.$

Tassa and Dyn have proposed in [62] a secret sharing scheme, that deals with the situations where one may limit the number of participants taken each compartment:

**Tassa-Dyn (TD) scheme**

- **Parameter**
  consider $\mathcal{C} = (C_1, \ldots, C_q)$ a partition of $U$, with $|C_i| = n_i$ for any $1 \leq i \leq q$. Let $0 < t_1 < \cdots < t_q$ be a sequence of positive thresholds, and $t$ the global threshold;

- **Secret and share spaces**
  define the secret space as and share spaces as $\mathbb{Z}_m$;

- **Secret sharing**
  given a secret $s \in \mathbb{Z}_m$, randomly generate $q$ values $x_1, \ldots, x_q$ and compute the Lagrange polynomials of degree $(q - 1)$

$$L_i(x) = \prod_{1 \leq j \leq q, j \neq i} \frac{x - x_j}{x_i - x_j}.$$  

The value $x_i$ is used to identify the participants from compartment $i$, as $L_i(x_i) = 1$ and $L_i(x_j) = 0$ for any $1 \leq j \leq q$ with $j \neq i$.

Generate $q \cdot t_i$ values $a_{i,j}$ with $1 \leq i \leq q$ and $0 \leq j < t_i$, such that $s = \sum_{i=1}^{q} \sum_{j=0}^{t_i-1} a_{i,j}$, and

$$f_i(y) = \sum_{j=0}^{t_i-1} a_{i,j} y^j.$$  

Define the bivariate polynomial $f(x, y)$ as

$$f(x, y) = \sum_{i=1}^{q} f_i(y) L_i(x) = \sum_{i=1}^{q} \sum_{j=0}^{t_i-1} a_{i,j} y^j L_i(x).$$

The share of the $j$th participant from compartment $i$, denoted $(x_i, y_{i,j})$ is $s_{i,j} = f(x_i, y_{i,j}) \mod m$. Also, we publish the values of $f(x, y)$ in $k = (\sum_{i=1}^{q} t_i - t)$ additional points $(x'_i, z_i)$ with $x'_i \notin \{x_1, \ldots, x_q\}$ for all $1 \leq i \leq k$. 

82
Chapter 3. Secret Sharing Schemes

any $t$ participants can recover the secret $s$. Recall that there are $k$ additional points, meaning there are $t + k$ points, and their corresponding value. Then, for each compartment $i$ one computes the polynomial $f_i$, as $L_i(x_i) = 1$ and $f_i(x_i, y) = f_i(y)$.

Example 3.6.30. Consider the following example for the TD scheme, with $q = 2$, $m = 13$, $t_1 = 2$, $t_2 = 3$ and $t = 4$. ($k = 1$). The set of participants is partitioned into $U_1 = \{1, 2, 3, 4\}$ and $U_2 = \{5, 6, 7\}$. Given $x_1 = 3$ and $x_2 = 7$, compute $L_1(x)$ and $L_2(x)$ as

$$L_1(x) = 3x - 8 \mod 13$$
$$L_2(x) = 10x - 4 \mod 13.$$  

To share the secret $s = 3$, we generate $a_{1,1}, a_{1,0}, a_{2,2}, a_{2,1}, a_{2,0}$ such that  

$$a_{1,1} + a_{1,0} + a_{2,2} + a_{2,1} + a_{2,0} = s \mod 13$$

Let $(a_{1,1}, a_{1,0}, a_{2,2}, a_{2,1}, a_{2,0}) = (4, 2, 8, 5, -3)$ be a possible share of $s$. Then, we have

$$f_1(y) = 4y + 2$$
$$f_2(y) = 8y^2 + 5y - 3$$

and the bivariate polynomial

$$f(x, y) = 2xy^2 - 3xy - 6y^2 + 2x - 4 \mod 13.$$  

The shares are $s_{1,1} = 6, s_{1,2} = 10, s_{1,3} = 1, s_{1,4} = 5$ for the first compartment, and $s_{2,5} = 1, s_{2,6} = 3, s_{2,5} = 8$ for the second compartment. And, the additional point is $(5, 4)$ with the value $f(5, 4) = 10$. Recall that participant $j$ from compartment $i$ has the point $(x_i, y_{i,j})$ and the value $f(x_i, y_{i,j})$. For example, for participant 2 of compartment 1, we have $(3, 2)$ and $f(3, 2) = 10$ or for participant 1 of compartment 2, we have $(7, 5)$ and $f(7, 5) = 1$.

Let $A = \{1, 2, 6, 7\}$ with $|A| = 4 = t$, $|A \cap C_1| = 2 = t_1$ and $|A \cap C_2| = 2 < t_2$. For the recovery of the secret $s$, one has to solve the following system of equations

$$f(x_1, y_{1,j}) = s_{1,i}, \forall i \in \{1, 2\}$$
$$f(x_1, y_{2,j}) = s_{1,i}, \forall i \in \{6, 7\}$$
$$f(5, 4) = 10$$

The above system has 5 equations, and 5 unknown coefficients $a_{1,1}, a_{1,0}, a_{2,2}, a_{2,1}, a_{2,0}$. Therefore, $s$ can be uniquely obtained.
Chapter 4

CRT-based threshold schemes and their security

4.1 Threshold secret sharing schemes . . . . . . . . . 86
4.2 Security properties . . . . . . . . . . . . . . . . . 92
4.3 Compact sequences of co-primes . . . . . . . . . 95
4.4 Bounding the loss of entropy . . . . . . . . . . . 101
4.5 Security of the GRS scheme . . . . . . . . . . . 103
4.6 Security of the Asmuth-Bloom scheme . . . . . 110
4.7 Security of the Mignotte scheme . . . . . . . . . 120

In this chapter we introduce the CRT-based threshold secret sharing schemes from [1, 29, 45], and present the security concepts introduced by Quisquater et al. [51] and their results concerning the security of the threshold scheme in [29] based on sequences of consecutive primes.

Our contribution consists of proposing a generic construction for CRT-based threshold secret sharing schemes (for uniformity presented at the end of Section 4.1) and the introduction of compact sequences of co-primes [3] (that were further extended to $k$-compact sequences in [21, 27]) as the formal approach to “integers of the same magnitude” [29]. Moreover, we adapt the security concepts from Section 4.2 to include the sequences discussed, and study some of their basic properties.

Another direction, concerning our contribution, is to the security of the schemes in [1, 29, 45], for which we provide a more suitable bound [27] for the loss of entropy, and study the security of the schemes in [1, 29, 45] based on $k$-compact sequences of co-primes. Furthermore, for the schemes in [1] and [29] a necessary and sufficient condition is provided with respect to asymptotic idealness.
4.1 Threshold secret sharing schemes

Secret sharing schemes based on the Chinese Remainder Theorem (CRT) have independently been introduced by Asmuth and Bloom [1] and Mignotte [45], and later by Goldreich, Ron and Sudan [29]. The schemes in this category are based on sequences of positive co-primes with special properties. The shares are obtained by dividing the secret or secret-dependent quantity by the numbers in the sequence and collecting the remainders. The secret can be recovered from some sufficient number of shares by using CRT.

4.1.1 Asmuth-Bloom scheme

Let \( t \) and \( n \) be two positive integers with \( 0 < t + 1 \leq n \). We call a sequence of co-primes \( m_0, m_1, \ldots, m_n \) an Asmuth-Bloom \((t+1, n)\)-threshold sequence of co-primes if the following properties are satisfied:

- \( m_0 < m_1 < \cdots < m_n \);
- \( \prod_{i=1}^{t+1} m_i > m_0 \prod_{i=0}^{t-1} m_{n-i} \) (called the Asmuth-Bloom constraint).

Let \( t \) and \( n \) be integers with \( 0 < t + 1 \leq n \). The Asmuth-Bloom \((t+1, n)\)-threshold scheme [1] is defined as follows:

Asmuth-Bloom scheme

**parameter**
- Consider \( m_0, m_1, \ldots, m_n \) an Asmuth-Bloom \((t+1, n)\)-threshold sequence of co-primes. The integers \( t, n, m_0, m_1, \ldots, m_n \) are public parameters;

**setup**
- Define the secret space as \( \mathbb{Z}_{m_0} \) and the share space of the \( i \)th participant as \( \mathbb{Z}_{m_i} \), for all \( 1 \leq i \leq n \);

**secret and share spaces**
- Given a secret \( s \), generate a random \( r \) such that \( s' = s + rm_0 < \prod_{i=1}^{t+1} m_i \). Share \( s \), by \( s_i = s' \mod m_i \) for all \( 1 \leq i \leq n \);

**secret sharing**
- Any set \( A \) of participants with \(|A| \geq t + 1\) can uniquely reconstruct the secret \( s \) by computing first the unique solution modulo \( \prod_{i \in A} m_i \) of the system:
  \[ x \equiv s_i \mod m_i, \quad \forall i \in A. \]
- And then reducing it modulo \( m_0 \).

The security of the Asmuth-Bloom scheme was argued by counting the number of possible solutions an unauthorised set (in this case any set with less than \( t + 1 \) participants) has to try to get the secret.
Let $M = \prod_{i=1}^{t+1} m_i$. "If only $t$ shadows were known, essentially no information about the key can be recovered. If $s_{i_1}, \ldots, s_{i_t}$ are known, then all we have is $s' \pmod{N_2}$ where $N_2 = \prod_{j=1}^{t} m_i$. Since $M/N_2 > m_0$ and $(N_2, m_0) = 1$, the collection of numbers $n_i$ with $n_i \equiv s' \pmod{N_2}$ and $n_i \leq M$ covers all congruence classes mod $m_0$, with each class containing at most one more or less $n_i$ than any other class. Thus no useful information (even probabilistic) is available without $t+1$ shadows."

(Asmuth and Bloom [1])

From the quote a few small changes were made, to correspond to the description of the Asmuth-Bloom scheme considered in this thesis. The changes include only:

- the secret space from $p$ to $m_0$;
- the share of participant $i_j$ from $y_{i_j}$ to $s_{i_j}$, and the combined share from $y$ to $s'$;
- and the threshold from $r$ to $t+1$.

**Example 4.1.1.** Consider the Asmuth-Bloom scheme with $n = 5$, $t = 3$ and $m_0 = 7$. Given the set $U = \{1, 2, 3, 4, 5\}$, let $m_1 = 17$, $m_2 = 19$, $m_3 = 23$, $m_4 = 29$ and $m_5 = 31$ such that

$$7 \cdot 29 \cdot 31 < 17 \cdot 19 \cdot 23 \quad (6293 < 7429) .$$

To share $s = 4$, generate $r = 999$ and compute $s' = 4 + 7 \cdot 999 = 6997$. The shares are $s_1 = 10 \pmod{17}$, $s_2 = 5 \pmod{19}$, $s_3 = 5 \pmod{23}$, $s_4 = 8 \pmod{29}$ and $s_5 = 22 \pmod{31}$.

Let $A = \{1, 2, 4\}$. The secret can be obtained, using CRT, from the following system

$$x = s_i \mod m_i \; \forall i \in A .$$

The solution to the system is

$$x = \sum_{i \in A} s_i \cdot (M/m_1) \cdot ((M/m_i)^{-1} \mod m_i) \mod M ,$$

where $M = 17 \cdot 19 \cdot 29 = 9367$ and

$$(M/m_1)^{-1} = 551^{-1} = 7^{-1} = 5 \mod 17 ,$$

$$(M/m_2)^{-1} = 493^{-1} = 18^{-1} = 18 \mod 19 ,$$

$$(M/m_4)^{-1} = 323^{-1} = 4^{-1} = 22 \mod 29 .$$

Therefore, $x$ can be computed

$$x = 10 \cdot 551 \cdot 5 + 5 \cdot 493 \cdot 18 + 8 \cdot 323 \cdot 22 \mod 9367 ,$$

$$x = 6997 \mod 9367 .$$

The secret $s$ can be extracted from $x$ by modular reduction with $m_0 = 7$, so $s = 4$. 87
4.1. Threshold secret sharing schemes

4.1.2 Mignotte scheme

In the Mignotte [45] scheme the secret space is much larger than the one consider in the Asmuth-Bloom scheme. Moreover, \( m_0 \) is not used.

For symmetry, we introduce the Mignotte \((t + 1, n)\)-threshold sequence of co-primes as a sequence of co-primes \( m_1, \ldots, m_n \) which satisfies:

1. \( m_1 < \cdots < m_n \);
2. \( \alpha \leq \beta \), where \( \alpha = 1 + \prod_{i=0}^{t-1} m_{n-i} \) and \( \beta = \prod_{i=1}^{t+1} m_i \).

One may notice that the Mignotte \((t + 1, n)\)-threshold sequence is a particular case of the Asmuth-Bloom \((t + 1, n)\)-threshold sequence of co-primes, where \( m_0 \) is 1.

Let \( t \) and \( n \) be integers with \( 0 < t + 1 \leq n \). The Mignotte \((t + 1, n)\)-threshold scheme [45] is defined as follows:

Mignotte scheme

- **parameter**
  - Consider \( m_1, \ldots, m_n \) an Mignotte \((t + 1, n)\)-threshold sequence of co-primes. The integers \( t, n, m_1, \ldots, m_n \) are public parameters;

- **secret and share spaces**
  - Define the secret space as \([\alpha, \beta]\) and the share space of the \( i \)th participant as \( \mathbb{Z}_{m_i} \), for all \( 1 \leq i \leq n \);

- **secret sharing**
  - Given a secret \( s \), the shares are computed as \( s_i = s \mod m_i \) for all \( 1 \leq i \leq n \);

- **secret reconstruction**
  - Any set \( A \) of participants with \(|A| \geq t + 1\) can uniquely reconstruct the secret \( s \) as the unique solution modulo \( \prod_{i \in A} m_i \) of the system:

\[
x \equiv s_i \mod m_i, \quad \forall i \in A.
\]

The security of the Mignotte scheme is based on the number of possible solutions an maximal unauthorised set has to try to get the secret.

Let \( M = \prod_{i=1}^t m_i \), and \( z_i = ((M/m_i)^{-1} \mod m_i) \cdot (M/m_i) \). According to the (extended) Euclidean Algorithm (see Section 2.2.4), there exists \( r_i \) such that \( z_i + r_i m_i = 1 \), for any \( 1 \leq i \leq t \).

When only \( t \) of the \( s_j \) are known, say \( s_1, \ldots, s_t \) then

\[
 s \equiv s_1 z_1 + \cdots s_t z_t \mod m_1 \cdots m_t
\]

so that the interval \([\alpha, \beta - 1]\) contains at least

\[
c = \left\lfloor \frac{\beta - 1 - \alpha}{m_1 \cdots m_t} \right\rfloor
\]
values which satisfy this condition and are equally possible values of $s$. If $c$ is large enough (for example $c = 10^6$) then it is practically impossible to find $s$.

A possible choice is

- $m_j \simeq 10^l$, $1 \leq j \leq n$
- $\alpha = 5.10^{(t+1)l-1}$, $\beta = 10^{(t+1)l}$,

where $l$ is some positive integer (for example $l = 6$).

Then when only $t$ or few of the $s_j$’s are known there are at least about $5.10^{l-1}$ candidates for $s$.” (Mignotte [45])

In the quote a few small changes were made, to correspond to the description of the Mignotte scheme considered in this thesis. The changes are reflected only by:

- the secret from $S$ to $s$ and secret space from $[a, b]$ to $[\alpha, \beta]$ where $\alpha = a$ and $\beta = b + 1$;
- the share of participant $i$ from $x_i$ to $s_i$, and the moduli from $d_i$ to $m_i$;
- and the threshold from $k$ to $t + 1$.

\textbf{Example 4.1.2.} \footnote{\textsuperscript{1} We adapt Example 4.1.1, by eliminating $m_0$.} Consider the Mignotte scheme with $U = \{1, 2, 3, 4, 5\}$, $t = 3$ and the sequence of co-primes $m_1 = 17$, $m_2 = 19$, $m_3 = 23$, $m_4 = 29$ and $m_5 = 31$, such that

\[ \alpha \leq \beta , \]

where $\alpha = 1 + 29 \cdot 31 = 900$ and $\beta = 17 \cdot 19 \cdot 23 = 7429$.

The secret $s = 6997$ is shared by $s_1 = 10 \mod 17$, $s_2 = 5 \mod 19$, $s_3 = 8 \mod 23$, $s_4 = 5 \mod 29$, $s_5 = 22 \mod 31$.

Let $A = \{1, 2, 4\}$. The secret can be obtained, using CRT, from the following system

\[
\begin{align*}
x &= 10 \mod 17 \\
x &= 5 \mod 19 \\
x &= 8 \mod 29 .
\end{align*}
\]

Similar to Example 4.1.1, the secret is

\[ x = 6997 \mod 9367 . \]

\subsection*{4.1.3 Goldreich, Ron and Sudan scheme}

The Goldreich, Ron and Sudan scheme [29], called GRS for short, is similar to the construction proposed by Asmuth and Bloom [1]. Instead of constraining the sequence of co-primes, the GRS scheme uses the Chinese Remainder Theorem for both the construction and reconstruction of the secret.
Let \( t \) and \( n \) be integers with \( 0 < t + 1 \leq n \). The \( GRS(t+1,n) \)-threshold scheme [29] is defined as follows:

**Goldreich, Ron and Sudan (GRS) scheme**

- **parameter setup**
  - Consider a sequence \( m_0 < \cdots < m_n \) of co-primes. The integers \( t, n, m_0, \ldots, m_n \) are public parameters;
- **secret and share spaces**
  - Define the secret space as being \( \mathbb{Z}_{m_0} \) and the share space of the \( i \)th participant as being \( \mathbb{Z}_{m_i} \), for all \( 1 \leq i \leq n \);
- **secret sharing**
  - Given a secret \( s \), randomly generate \( r_i \) from \( \mathbb{Z}_{m_i} \) for all \( 1 \leq i \leq t \), and compute \( s' \) as the unique solution modulo \( m_0 \prod_{i=1}^{t} m_i \) of the system
    \[
    x \equiv r_i \mod m_i, \quad 0 \leq i \leq t
    \]
  - Where \( r_0 = s \). The shares are obtained from \( s' \), by \( s_i = s' \mod m_i \), for all \( 1 \leq i \leq n \). (Note that \( r_i = s_i \) for all \( 1 \leq i \leq t \).)
- **secret reconstruction**
  - Any set \( A \) of participants with \( |A| \geq t + 1 \) can uniquely reconstruct the secret \( s \) by computing first the unique solution modulo \( \prod_{i \in A} m_i \) of the system
    \[
    x \equiv s_i \mod m_i, \quad \forall i \in A
    \]
  - And then reducing it modulo \( m_0 \).

The security of the GRS scheme was explained in a rather different way, by showing that the secrets are “indistinguishable” if at most \( t - 1 \) shares are known and the sequence of co-prime integers consists of prime numbers of the “same magnitude”.

Let \( I \) be a set of participants, and \( X \) the random variable associated to the secret space \( \mathbb{Z}_{m_0} \). Then, for any \( I \) and any \( s, s' \in \mathbb{Z}_{m_0} \), the statistical difference between \( X = s \) and \( X = s' \) is at most

\[
2 \cdot \frac{\prod_{i \in I} m_i}{\prod_{i=1}^{t} m_i}.
\]

“Thus, in general, security is provided only for \( |I| \leq t - 1 \) (rather than for \( |I| \leq t \) as in case of Shamir’s scheme). An advised choice of parameters is to have \( m_i \)’s be the same magnitude and large enough so that \( 1/m_i \) is negligible in the security parameter.” (Goldreich et al. [29])

In the quote only one change was made, to correspond to the description of the GRS scheme considered in this thesis:

- The moduli from \( p_i \) to \( m_i \).
Chapter 4. CRT-based threshold schemes and their security

Example 4.1.3. ²

Consider the GRS scheme with \( U = \{1, 2, 3, 4, 5\} \), \( t = 3 \) and the sequence \( m_0 = 7, m_1 = 17, m_2 = 19, m_3 = 23, m_4 = 29, m_5 = 31 \).

Let \( s = 4 \mod 7 \). Randomly generate \( r_1 = 10 \) from \( \mathbb{Z}_{17} \) and \( r_2 = 5 \) from \( \mathbb{Z}_{19} \), and compute \( s' = 214 \mod 2261 \) from the system

\[
\begin{align*}
    s' &= 4 \mod 7 \\
    s' &= 10 \mod 17 \\
    s' &= 5 \mod 19 .
\end{align*}
\]

The shares are \( s_1 = 10 \mod 17, s_2 = 5 \mod 19, s_3 = 7 \mod 23, s_4 = 11 \mod 29, s_5 = 28 \mod 31 \).

Let \( A = \{1, 2, 4\} \); the secret is obtained using CRT. Therefore, the system

\[
x = s_i \mod m_i, \forall i \in A .
\]

has the following solution

\[
\begin{align*}
    x &= 10 \cdot 551 \cdot 5 + 5 \cdot 493 \cdot 18 + 11 \cdot 323 \cdot 22 \mod 9367 \\
    x &= 214 \mod 9367 .
\end{align*}
\]

The secret \( s \) can be extracted from \( x \) by modular reduction with \( m_0 = 7 \), so \( s = 4 \).

4.1.4 A Generic CRT-based scheme

As one may notice, there are a few similarities between the secret sharing schemes based on CRT \([1, 29, 45]\) described in the previous sections. Therefore, in this sub-section we present a general method for constructing threshold schemes based on CRT \([3]\).

Given \( t \) and \( n \) such that \( 0 < t + 1 \leq n \), the main idea of constructing a \( CRT \) \((t + 1, n)\)-threshold scheme is the following:

**CRT scheme**

- **parameter** consider a sequence \( m_0 < \cdots < m_n \) of co-primes. The sequence may be subject to various constraints. The integers \( t, n, m_0, \ldots, m_n \) are public parameters;
- **setup** define the secret space as being an interval \([\alpha, \beta]\), where \( \alpha \) and \( \beta \) depend on the sequence of co-primes (and on \( t \)), and the share space of the \( i \)th participant as being \( \mathbb{Z}_{m_i} \), for all \( 1 \leq i \leq n \);

² The same values as in Example 4.1.1 were used, such that one may compare the secret share phase of the two schemes. The recovery is done identically as in the Asmuth-Bloom scheme.
secret sharing  given a secret $s$ in the secret space, let $s'$ denote the secret-dependent quantity obtained from $s$ (that may depend on $t$ and on the scheme). The shares are computed as $s_i = s' \mod m_i$, for all $1 \leq i \leq n$.

secret reconstruction any authorized set $A$ of participants (which has cardinality greater or equal to $t + 1$) should allow an easy reconstruction of the secret. Moreover, the scheme is expected to satisfy some security properties with respect to the secret reconstruction from less than $t + 1$ shares. From an information and complexity theoretic point of view, less than $t + 1$ shares should give no information on the secret.

Remark 4.1.4. The Asmuth-Bloom scheme, the Mignotte scheme and GRS scheme are particular cases of the CRT $(t + 1, n)$-threshold scheme.

4.2 Security properties

From the way the CRT-based threshold secret sharing schemes were introduced, their security is unclear from an information theoretic point of view, or from an complexity point of view. A important step in this direction was first made by Quisquater, Preneel and Vandewalle [51].

Starting from the security arguments in [1, 45], Quisquater et al. [51] have introduced the modern concepts of asymptotic perfectness and asymptotic idealness, in order to provide a more detailed study of the security of threshold schemes based on CRT. Then, they proved that the GRS threshold scheme [29] is asymptotically ideal (and, therefore, asymptotically perfect) and perfect zero-knowledge provided that it uses sequences of consecutive primes.

For simplicity, let $U = \{1, 2, \ldots, n\}$ be the set of participants. Given a CRT $(t + 1, n)$-threshold scheme and a non-empty set $I \subseteq U$, consider the random variables $X$ and $Y_I$ that take values into the secret space $\mathbb{Z}_{m_0}$ and into the share space $\prod_{i \in I} \mathbb{Z}_{m_i}$, respectively.

We define the loss of entropy $[51]$ assigned to $y_I$, denoted $\Delta(y_I)$, as

$$\Delta(y_I) = H(X) - H(X \mid Y_I = y_I),$$

for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$.

Remark 4.2.1. [51] The loss of entropy $\Delta(y_I)$ may be negative. Let $X$ take values into $\{-1, 0, 1\}$ such that $P(X = -1) = 7/8$, $P(X = 0) = 1/16$ and $P(X = 1) = 1/16$. Consider that $Y_I$ takes the value 1 if $X \geq 0$, and 0 otherwise. We have $P(X = -1 \mid Y_I = 1) = 0$, $P(X = 0 \mid Y_I = 1) = 1/2$ and $P(X = 1 \mid Y_I = 1) = 1/2$. Therefore,

$$\Delta(1) = H(X) - H(X \mid Y_I = 1) \approx -0.33.$$
Definition 4.2.2. [51] Let $0 < t + 1 \leq n$ be two positive integers. The CRT $(t + 1, n)$-threshold scheme is called asymptotically perfect if, for any non-empty subset $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$ and any $\epsilon > 0$, there exists $m \geq 0$ such that for any sequence of co-primes $m_0 < m_1 < \cdots < m_n$ with $m_0 \geq m$, the following hold:

1. $H(X) \neq 0$;
2. $|\Delta(y_I)| < \epsilon$ for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$.

Definition 4.2.3. [51] Let $0 < t + 1 \leq n$ be two positive integers. The CRT $(t + 1, n)$-threshold scheme is called asymptotically ideal if it is asymptotically perfect and for any $\epsilon > 0$ there exists $m \geq 0$ such that for any sequence $m_0 < m_1 < \cdots < m_n$ of co-primes with $m_0 \geq m$ and any $1 \leq i \leq n$ the following holds:

$$\frac{|Z_{m_i}|}{|Z_{m_0}|} < 1 + \epsilon.$$ 

Note that $|Z_{m_i}|/|Z_{m_0}|$ is the information rate $^3$ associated to the $i$th participant.

In [51] it was shown that the loss of entropy for the GRS threshold scheme can be upper bounded. Furthermore, the GRS threshold scheme based on sequences of consecutive primes, under the uniform distribution over the secret space, is asymptotically perfect, and asymptotically ideal (the proofs are omitted).

Lemma 4.2.4. [51] Let $0 < t + 1 \leq n$ be two positive integers. The loss of entropy of the GRS $(t + 1, n)$-threshold scheme with respect to the uniform distribution on the secret space satisfies the following relations:

1. $\Delta(y_I) \leq \log \left( \frac{C(I) + 1}{m_0} + 1 \right)$, if $C(I) \neq 0$, 
2. $\Delta(y_I) = \log m_0$, if $C(I) = 0$,

for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, for any sequence $m_0 < m_1, \ldots, m_n$ of co-primes and for any $I \subseteq \{1, \ldots, n\}$, where

$$C(I) = \left\lfloor \frac{m_0 \prod_{i=1}^t m_i}{\prod_{i \in I} m_i} \right\rfloor.$$ 

$^3$ See Definition 3.5.1.
4.2. Security properties

The following result is a straightforward adaptation of the previous lemma.

**Corollary 4.2.5.** Let $0 < t + 1 \leq n$ be two positive integers. The loss of entropy of the Asmuth-Bloom ($t+1,n$)-threshold scheme, satisfies the same relations as those in Lemma 4.2.4 for $C(I) = \left\lfloor \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i \in I} m_i} \right\rfloor$.

**Theorem 4.2.6.** [51] Let $0 < t + 1 \leq n$ be two positive integers. The GRS ($t+1,n$)-threshold scheme based on sequences of consecutive primes is asymptotically perfect, under the uniform distribution on the secret space.

**Theorem 4.2.7.** [51] Let $0 < t + 1 \leq n$ be two positive integers. The GRS ($t+1,n$)-threshold scheme based on sequences of consecutive primes is asymptotically ideal, under the uniform distribution on the secret space.

If we consider the secret as the private key associated to a public key, the entropy of the secret is 0. Therefore, the concept of (asymptotic) perfectness can not be used in public key cryptography. Desmedt et al. [23] proposed a perfect zero-knowledge approach. Meaning, given a set of shares is indistinguishable from which secret those shares are derived.

Given the CRT ($t+1,n$)-threshold scheme based on the sequence $m_0, m_1, m_2, \ldots, m_n$ of co-primes, a secret $s \in Z_{m_0}$, and a non-empty set $I \subseteq \{1, \ldots, n\}$, we define $Y_{s,I}$ as the random variable that takes the value $y_I = \prod_{i \in I} Z_{m_i}$ as the combined shares of all $i \in I$ in the same process of sharing $s$.

**Definition 4.2.8.** [51] Let $0 < t + 1 \leq n$ be two positive integers. The CRT ($t+1,n$)-threshold scheme is called perfect zero-knowledge if, for any polynomial $poly$ there exists $m \geq 0$ such that for any sequence $m_0 < m_1 < \cdots < m_n$ of co-primes with $m_0 \geq m$, any $s, s' \in Z_{m_0}$, and any non-empty set $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$, the following holds:

$$\sum_{y_I \in \prod_{i \in I} Z_{m_i}} |P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I)| \leq \frac{1}{poly(m_0)}$$

(4.1)

In [51] it was shown that under a uniform distribution over the secret space the GRS threshold scheme based on sequences of consecutive primes is perfect zero-knowledge.

**Theorem 4.2.9.** [51] Let $0 < t + 1 \leq n$ be two positive integers. The GRS ($t+1,n$)-threshold scheme based on consecutive primes is perfect zero-knowledge with respect to the uniform distribution on the secret space.
Chapter 4. CRT-based threshold schemes and their security

4.3 Compact sequences of co-primes

The authors of the GRS \((t + 1, n)\)-threshold scheme have argued that no information is given from a complexity theoretic point of view, if at most \(t - 1\) shares are taken and the scheme is based on sequences of large primes of the same magnitude. This result was extended to \(t\) shares in [51] if consecutive primes are considered. As such, it was proven that the GRS \((t + 1, n)\)-threshold scheme based on sequences of consecutive primes is asymptotically ideal and perfect zero-knowledge.

Although the term integers of the “same magnitude” is not defined in [29], one can easily see that consecutive primes are particular cases. Therefore, in [3] we introduce the concept of compact sequence of co-primes as a suitable definition for co-primes of the “same magnitude”. Furthermore, in [21, 27] we noticed that the secret space \(m_0\) does not always has to be placed before the rest of the sequence. As such, we extend compact sequences to \(k\)-compact sequences of co-primes.

**Definition 4.3.1.** [3] A sequence \(m_0 < \ldots < m_n\) of co-primes, where \(n \geq 1\), is called a compact sequence of co-primes if \(m_n < m_0 + m_0^\theta\), for some real number \(\theta \in (0, 1)\).

**Remark 4.3.2.** [3] A sequence \(m_0 < \ldots < m_n\) of positive integers covers another sequence \(q_0 < \ldots < q_s\) of positive integers if \(m_0 \leq q_0\) and \(q_s \leq m_n\).

If a sequence of co-primes is covered by a compact sequence of co-primes, then it is a compact sequence of co-primes too.

Compact sequences of co-primes play an important role in designing secure CRT-based threshold secret sharing schemes. Therefore, a few particular cases were considered in [3] for the GRS scheme and Asmuth-Bloom scheme:

- \((t, \Theta)\)-compact sequence of co-primes. A sequence is \((t, \Theta)\)-compact, where \(0 \leq t < n\) and \(\Theta \in (0, 1)\), if \(m_{t+1} \geq m_t + 2\) and \(m_n < m_0 + m_0^\theta\) for some \(\theta \in (0, \Theta]\).

- quasi-compact sequence of co-primes \(^4\). A sequence is quasi-compact, if \(m_0 - m_0^\theta < m_i < m_0\) for any \(1 \leq i \leq n\), and some \(\theta \in (0, \Theta]\).

- almost \(\Theta\)-compact sequence of co-primes. A sequence is almost \(\Theta\)-compact if \(m_i \in (x, x^\theta)\) for all \(1 \leq i \leq n\), where \([x^\theta] = 2m_0 - 2\) and \(\theta \in (0, \Theta]\). One can replace “\(x = 2m_0 - 2\)” by “\(x = km_0 - 2\)”, for any fixed integer \(k \geq 2\).

The constraints used in this particular cases of compact sequences of co-primes are technical and were necessary in proofs in [3]. As large consecutive

\(^4\) See Remark 4.3.4.
4.3. Compact sequences of co-primes

primes satisfy the constraint \( m_{t+1} \geq m_t + 2 \), that is not always true about by sequences of co-primes. However, one can easily extract a \((t, \Theta)\)-compact sequence of length \( n + 1 \) \((m_0 < m_1 < \cdots < m_n \) or \( m_1 < \cdots < m_n < m_{n+1} \)) from a compact sequences \( m_0 < m_1 < \cdots < m_n < m_{n+1} \) of co-primes of length \( n + 2 \). (If \( m_{t+1} = m_t + 1 \), then \( m_t \geq m_{t-1} + 2 \) or \( m_{t+2} \geq m_{t+1} + 2 \).)

With regard of the “asymptotic” nature of the security properties, one must require \( \theta \leq \Theta \) to ensure that \( m_0^\theta/m_0 \) converges to 0 as \( m_0 \) goes to infinity. Therefore, the information rate \( m_i/m_0 \) of the \( i \)th participant converges to 1 as \( m_0 \) goes to infinity.

Note that the GRS \((t + 1, n)\)-threshold scheme [29] and the Asmuth-Bloom \((t + 1, n)\)-threshold scheme [1], as defined and used in all subsequent papers, are based on a increasing sequences \( m_0 < m_1 < \cdots < m_n \) of co-primes. The integer \( m_0 \), which defines the secret space, is the first element in this sequence. Therefore, the share spaces of the participants are always larger than the secret space. In this context, a more optimal choice for \( m_0 \) would be in the “middle” of the sequence \( m_1 < \cdots < m_n \). This would result in a balanced distribution of the participants information rates around 1.

According to this discussion we introduce the following concept.

Definition 4.3.3. [21, 27] 5

1. A sequence \( m_0, m_1, \ldots, m_n \) of pair-wise co-primes is called \((k, \theta)\)-compact, where \( k \geq 1 \) and \( \theta \in (0, 1) \) are two real numbers, if \( m_1 < \cdots < m_n \) and \( km_0 - m_0^\theta < m_i < km_0 + m_0^\theta \) for all \( 1 \leq i \leq n \).

2. A sequence \( m_0, m_1, \ldots, m_n \) of pair-wise co-primes is called \( k \)-compact if it is \((k, \theta)\)-compact for some \( \theta \in (0, 1) \).

In a \( k \)-compact sequence \( m_0, m_1, \ldots, m_n \) of co-primes, the integer \( m_0 \) may be smaller than \( m_1 \), greater than \( m_n \), or in between \( m_1 \) and \( m_n \), while \( m_1, \ldots, m_n \) are in increasing order.

Let such a sequence be denoted by \( m_0, m_1 < \cdots < m_n \). Furthermore, 1-compact sequences of co-primes will also be called compact sequences of co-primes.

Remark 4.3.4. Regarding quasi-compact sequences, in [3] we have called such sequences a compact sequences \( m_0 < m_1 < \cdots < m_n \) of co-primes with \( m_n \) the secret space, and \( m_i \) the share space, for all \( 0 \leq i < n \). In [27] we have called such sequences \((n - 1, \Theta)\)-compact, and kept the same secret space \( m_n \), and \( m_i \) the share space, for all \( 0 \leq i < n \).

With the introduction of \( k \)-compact sequences, where the secret is mobile, one may consider this type of sequence as a particular case of \( k \)-compact

5 In [21] \( k \) was considered a real number greater than 1, while in [27] \( k \) is a positive integer greater than or equal to 1. More details about this difference is given in Section 4.6 (Proposition 4.6.7).
sequences with $k = 1$ and the elements $m_i$ to be taken from $(m_0 - m_0^\theta, m_0)$, for all $1 \leq i \leq n$.

To prove the correctness of our re-naming, we must show that for any compact interval $(x, x + x^\theta)$ with $x \geq 0$ and some $\theta \in (0, 1)$ there exists $y \geq 0$ such that the interval $(y - y^\theta, y)$ covers the interval $(x, x + x^\theta)$. Meaning

$$y - y^\theta \leq x < x + x^\theta \leq y + y^\theta.$$  

For simplicity, let $y = x + x^\theta$, and we prove $y - y^\theta < x$.

As $y > x$, we have that $x^\theta - y^\theta < 0$. Therefore, $y - y^\theta = x + (y^\theta - y^\theta) < x$.

### 4.3.1 More on security properties

The concepts of asymptotic perfectness, asymptotic idealness, and perfect zero-knowledge were introduced for an increasing sequence of co-primes, where the secret space was the smallest number in the sequence. Therefore, one has to take into account that the changes in the sequences of co-primes lead to changes in the definitions of asymptotic perfectness and idealness. As $k$-compactness is the largest class of co-primes considered in this chapter, we modify the definitions accordingly.

**Remark 4.3.5.** [3] One can easily see that the constraint “for any $\epsilon > 0$” in the concepts of asymptotic perfectness and idealness (Definitions 4.2.2 and 4.2.3) can be equivalently replaced by “for any $0 < \epsilon < 1$”.

**Definition 4.3.6.** [21, 27] Let $0 < t + 1 \leq n$ be two positive integers. The CRT $(t + 1, n)$-threshold scheme based on $k$-compact sequences of co-primes is called asymptotically perfect if, for any non-empty subset $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$, for any $\theta \in (0, 1)$ and any $\epsilon \in (0, 1)$, there exists $m \geq 0$ such that for any $(k, \theta)$-compact sequence of co-primes $m_0, m_1, \ldots, m_n$ with $m_0 \geq m$, the following hold:

- $H(X) \neq 0$;
- $|\Delta(y_I)| < \epsilon$ for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$.

As asymptotic idealness depends on the information rate, we re-define the information rate to take into account the freedom given to the secret space $m_0$.

**Definition 4.3.7.** [21, 27] Let $0 < t + 1 \leq n$ be two positive integers. The information rate of the CRT $(t + 1, n)$-threshold scheme based on $k$-compact sequences of co-primes goes asymptotically to $r$ if for any $\theta \in (0, 1)$ and any $\epsilon \in (0, 1)$, there exists $m \geq 0$ such that for any $(k, \theta)$-compact sequence of co-primes $m_0, m_1, \ldots, m_n$ with $m_0 \geq m$ and any $1 \leq i \leq n$ the following holds:

$$\left| \frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} - r \right| < \epsilon.$$
4.3. Compact sequences of co-primes

Definition 4.3.8. [21, 27] Let \(0 < t + 1 \leq n\) be two positive integers. The CRT \((t + 1, n)\)-threshold scheme based on \(k\)-compact sequences of co-primes is asymptotically ideal if it is asymptotically perfect and its information rate goes asymptotically to \(1\).

Definition 4.3.9. [51] Let \(0 < t + 1 \leq n\) be two positive integers. The CRT \((t + 1, n)\)-threshold scheme based on \(k\)-compact sequences of co-primes is called perfect zero-knowledge if, for any polynomial \(\text{poly}\) and for any \(\theta \in (0, 1)\) there exists \(m \geq 0\) such that for any \(\theta\)-compact sequence of co-primes \(m_0, m_1, \ldots, m_n\) with \(m_0 \geq m\), any \(s, s' \in \mathbb{Z}_{m_0}\), and any non-empty set \(I \subseteq \{1, \ldots, n\}\) with \(|I| \leq t\), the following holds:

\[
\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} \left| P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I) \right| \leq \frac{1}{\text{poly}(m_0)} \tag{4.2}
\]

The Asmuth-Bloom scheme, GRS scheme, and Mignotte scheme are particular cases of the CRT \((t + 1, n)\)-threshold scheme. Therefore, the above definitions can be used to analyze the security properties of the Asmuth-Bloom \((t + 1, n)\)-threshold scheme, GRS \((t + 1, n)\)-threshold scheme and Mignotte \((t + 1, n)\)-threshold scheme.

4.3.2 Properties of compact sequences

As one may notice, \(k\)-compact sequences are natural generalizations of compact sequences of co-primes. Therefore, all the results we have established for compact sequences of co-primes [3], also hold for \(k\)-compact.

Lemma 4.3.10. [3] For any \(n \geq 1\) there exists \(m \geq 0\) such that any sequence \(m_0 < \cdots < m_n\) of consecutive primes (or co-primes) with \(m_0 \geq m\) is a compact sequence of co-primes.

Proof. Let \(n \geq 1\). As

\[
\lim_{i \to \infty} \frac{p_{i+1} - p_i}{p_i} = 0,
\]

there exists \(i_0\) such that \(p_{i+1} < (1 + \epsilon)p_i\), for any \(\epsilon > 0\) and any \(i \geq i_0\). Therefore, \(p_{i+j} < (1 + \epsilon)^j p_i\), for any \(i \geq i_0\) and \(j \geq 1\).

Given \(\epsilon \in (\sqrt{3/2} - 1, \sqrt{2} - 1)\) and \(i_0\) such that \(p_{i+1} < (1 + \epsilon)p_i\) for any \(i \geq i_0\), we show that \(p_i < p_{i+1} < \cdots < p_{i+n}\) is a compact sequence of co-primes. Consider \(m = p_{i_0}\). Because \(\epsilon \in (\sqrt{3/2} - 1, \sqrt{2} - 1)\) it follows that

\[0 < 1 + \log_{p_i} ((1 + \epsilon)^n - 1) < 1.\]

Therefore, for any \(\theta\) in between \(1 + \log_{p_i} ((1 + \epsilon)^n - 1)\) and \(1\) we obtain

\[p_{i+n} < (1 + \epsilon)^n p_i < p_i + \theta^p_i,\]
for any \( p_i \geq p_0 \). As a conclusion, \( p_i < p_{i+1} < \cdots < p_{i+n} \) is a compact sequence of co-primes with \( p_i \geq m \).

For a \( m_0 < \cdots < m_n \) consecutive co-prime sequence, we show that the above sequence \( p_i < p_{i+1} < \cdots < p_{i+n} \) of consecutive primes covers the current sequence of co-primes. Let \( m = p_{i0} \), as obtained above, and \( p_i \geq m_0 \). As \( m_1 \) is the smallest integer greater than \( m_0 \) and co-prime to \( m_0 \) and \( p_i+1 \) is prime, we have \( p_{i+1} \geq m_1 \). Inductively, one obtains \( m_j \leq p_{i+j} \), for any \( 1 \leq j \leq n \).

The result follows, as \( p_i < p_{i+1} < \cdots < p_{i+n} \) covers \( m_0 < \cdots < m_n \). (see Remark 4.3.2)

**Corollary 4.3.11.** [3] For any \( n \geq 1 \) and \( m \geq 0 \) there are compact sequences of co-primes of length \( n+1 \) whose first element is greater than or equal to \( m \).

**Proof.** Directly from Lemma 4.3.10.

According to Definition 4.3.1, given \( x > 0 \) and \( \theta \in (0, 1) \), any sequence of co-primes in between \( x \) and \( x + x^{\theta} \) is a compact sequence of co-primes. We prove that the interval \((x, x + x^{\theta})\) has sequences of co-primes “significantly denser” [3] than sequences of consecutive primes in the same interval.

Let \( \ell(x, \theta) = \pi(x + x^{\theta}) - \pi(x) \) \(^6\) denote the longest sequence of consecutive primes in between \( x \) and \( x + x^\theta \).

Baker et al. [2] have shown that, if \( x \) is sufficiently large, then

\[
\ell(x, \theta) = \pi(x + x^{\theta}) - \pi(x) > \frac{2x^\theta}{5 \log (x + x^{\theta})} \quad (4.3)
\]

**Lemma 4.3.12.** [3] For any \( k \geq 2 \) there exists \( \theta, \theta_2, \ldots, \theta_k \in (0, 1) \) and \( x_0 > 0 \) such that, for any \( x \geq x_0 \), the interval \((x, x + x^{\theta})\) contains compact sequences of co-primes whose length \( \ell \) satisfies

\[
\ell > \ell(x, \theta) + \sum_{i=2}^{k} \frac{2ix^{\theta_i/i}}{5 \log (x + x^{\theta})}
\]

**Proof.** To prove the lemma we count the number of prime powers that are in the interval \((x, x + x^{\theta})\) for some \( x \) and some \( \theta \in (0, 1) \).

**Claim 1:** The interval \((x, x + x^{\theta})\) contains at most one power of a prime number

**Proof of Claim 1:** We prove that for any prime \( p \), there exists only one \( e \geq 1 \) such that \( x < p^e < x + x^\theta \). If \( x < p^e < x + x^\theta \) for some \( e \geq 1 \), then \( p^{e+1} > x + x^\theta \) because

\[
p^{e+1} = p \cdot p^e > 2x > x + x^\theta.
\]

\(^6\) \( \pi(x) \) is defined as the number of primes less than or equal to \( x \).
4.3. Compact sequences of co-primes

(Note that the smallest prime number is 2.)

As \((x, x + x^\theta)\) may contain at most one power of a prime number, the sequence of all prime powers in the interval \((x, x + x^\theta)\) forms a sequence of co-primes.

We estimate the length of this sequence, using the function \(\pi^*\) from [49], which is given by

\[
\pi^*(x) = |\{p \mid p \text{ is a prime and } p^e \leq x \text{ for some } e \geq 1\}|
\]

for any \(x > 0\).

Given \(s = \max\{1, [\log x/\log 2]\}\), \(\pi^*(x)\) can also be computed by

\[
\pi^*(x) = \pi(x) + \pi(x^{1/2}) + \cdots + \pi(x^{1/s}).
\]

Therefore, \(\pi^*(x + x^\theta) - \pi^*(x)\) gives the number of prime powers in between \(x\) and \(x + x^\theta\):

\[
\pi^*(x + x^\theta) - \pi^*(x) \geq \sum_{i=1}^s (\pi((x + x^\theta)^{1/i}) - \pi(x^{1/i}))
\]

Claim 2: There exists a sequence of positive real numbers

\[0.54 \leq \theta_k \leq \theta_{k-1} \leq \cdots \leq \theta_2 < \theta\]

such that \((x + x^\theta)^{1/i} > x^{1/i} + x^{\theta/i}, \) for all \(2 \leq i \leq k\).

Proof of Claim 2: Remark that the following inequalities hold for any positive integer \(k \geq 2\):

\[k(\theta - 1) + 1 < (k - 1)(\theta - 1) + 1 < \cdots < 2(\theta - 1) + 1 < \theta\]

Given the binomial formula

\[(x^{1/i} + x^{\theta/i})^i = x + O(x^{(i-1+\theta)/i})\]

if we choose \(\theta_i < i(\theta - 1) + 1,\) then \((x + x^\theta)^{1/i} > x^{1/i} + x^{\theta/i}, \) for all \(2 \leq i \leq k\) and for \(x\) large enough.

For \(\theta > 1 - 0.46/k,\) then \(k(\theta - 1) + 1 > 0.54.\) Therefore, there exists \(\theta_2, \ldots, \theta_k\) satisfying the claim.

Combining the values considered in Claim 2 with (4.3) we obtain

\[
\pi^*(x + x^\theta) - \pi^*(x) > \ell(x, \theta) + \sum_{i=2}^k (\pi((x + x^\theta)^{1/i}) - \pi(x^{1/i}))
\]

\[
> \ell(x, \theta) + \sum_{i=2}^k (\pi(x^{1/i} + x^{\theta/i}) - \pi(x^{1/i}))
\]

\[
> \ell(x, \theta) + \sum_{i=2}^k \frac{\pi(x^{1/i} + x^{\theta/i})}{2x^{\theta/i}}
\]

\[
> \ell(x, \theta) + \sum_{i=2}^k \frac{5\log (x^{1/i} + x^{\theta/i})}{2x^{\theta/i}}
\]

\[
= \ell(x, \theta) + \sum_{i=2}^k \frac{5\log (x + x^\theta)}{2ix^{\theta/i}}
\]
for large enough $x$. This proves the lemma.

### 4.4 Bounding the loss of entropy

Lemma 4.3.10 and Corollary 4.3.11 are important tools in studying the loss of entropy for the threshold secret sharing schemes based on CRT. The following result sharpens it by providing a more precise approximation of the loss of entropy in the Asmuth-Bloom threshold scheme. Furthermore, the same results can be extended to the GRS threshold scheme.

**Remark 4.4.1.** Under a uniform distribution over the secret space $\mathbb{Z}_{m_0}$, it follows $P(X = s) = 1/m_0$ and, therefore,

$$H(X) = \sum_{s \in \mathbb{Z}_{m_0}} P(X = s) \log \frac{1}{P(X = s)} = \log m_0$$

**Lemma 4.4.2.** [27] Let $0 < t + 1 \leq n$ be two positive integers and $I \subseteq \{1, \ldots, n\}$ a non-empty subset. The loss of entropy of the Asmuth-Bloom $(t+1, n)$-threshold scheme under a uniform distribution over the secret space satisfies the following relations:

- $\Delta(y_I) = \log m_0 + \delta_1 \left\lfloor \frac{C_I}{m_0} \right\rfloor \log \frac{C_I}{m_0} + \delta_2 \left\lfloor \frac{C_I}{m_0} \right\rfloor + \log \left\lfloor \frac{C_I}{m_0} \right\rfloor + 1$, if $C_I \neq 0$,
- $\Delta(y_I) = \log m_0$, if $C_I = 0$,

for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ and any sequence $m_0, m_1, \ldots, m_n$ of co-primes, where $\delta_1 + \delta_2 = m_0$, $\delta_2 = C_I \mod m_0$, and $C_I$ is either $C(I)$ or $C(I)+1$ depending on $I$ ($C(I)$ is the one defined in Corollary 4.2.5).

**Proof.** Let $m_0, m_1, \ldots, m_n$ be an Asmuth-Bloom sequence of co-primes.

**Case 1:** $|I| > t$. According to the secret recovery phase of the Asmuth-Bloom $(t+1, n)$-threshold scheme, the participants of $I$ can recover uniquely the shared secret $s$ from $\mathbb{Z}_{m_0}$. Therefore,

$$P(X = s \mid Y_I = y_I) = 1$$

and

$$P(X = s' \mid Y_I = y_I) = 0$$

for any $s' \in \mathbb{Z}_{m_0}$ with $s' \neq s$. Moreover, $C_I = C(I) = 0$.

As there is no uncertainty over the obtained secret, we have the conditional entropy $H(X \mid Y_I = y_I) = 0$. Based on Remark 4.4.1, the loss of entropy is $\Delta(y_I) = \log m_0$.

**Case 2:** $|I| \leq t$. Given the the shares of the participants in $I$, let $x_0$ be the unique solution modulo $\prod_{i \in I} m_i$ obtained by using CRT. Consider the set

$$B = \left\{ x \in \mathbb{Z}_{\prod_{i \in I} m_i} \mid x = x_0 + r \cdot \prod_{i \in I} m_i, \ r \in \mathbb{Z} \right\}.$$
According to [24], the congruential equation
\[ r \prod_{i \in I} m_i \equiv (s - x_0) \mod m_0 \]
admits a unique solution modulo \( m_0 \) in \( r \). Thus, for any \( x \in B \) there exists a unique \( s \in \mathbb{Z}_{m_0} \) such that \( s \equiv x \mod m_0 \).

As the cardinality of \( B \) could be larger or smaller than \( m_0 \), it is possible for a given \( s \in \mathbb{Z}_{m_0} \) to correspond to none or more \( x \) values from \( B \) such that \( s \equiv x \mod m_0 \).

For the sake of simplicity, let \( C_I \) be the cardinality of \( B \). Then,
\[ B = \{x_0, \ldots, x_{C_I-1}\} \, . \]

If \( x_0 < \left( \prod_{i=1}^{I+1} m_i - C(I) \cdot \prod_{i \in I} m_i \right) \) then \( C_I = C(I) + 1 \); otherwise, \( C_I = C(I) \).

Note, that the residues modulo \( m_0 \) of any consecutive \( m_0 \) values from the set \( B \) cover the entire secret space \( \mathbb{Z}_{m_0} \). Let \( C_I = m_0 \cdot q + \delta_2 \) and \( \delta_1 = m_0 - \delta_2 \), where \( 0 \leq \delta_2 < m_0 \). For exactly \( \delta_1 \) elements in \( \mathbb{Z}_{m_0} \), each element contains the residues modulo \( m_0 \) of exactly \( q \) elements from \( B \). And, for the other \( \delta_2 \) elements in \( \mathbb{Z}_{m_0} \), each element contains the residues modulo \( m_0 \) of exactly \( q + 1 \) elements from \( B \).

Thereby, the conditional probabilities are
\[ P(X = s \mid Y_I = y_I) = \frac{q}{C_I} \]
for exactly \( \delta_1 \) values \( s \in \mathbb{Z}_{m_0} \), and
\[ P(X = s \mid Y_I = y_I) = \frac{q + 1}{C_I} \]
for exactly \( \delta_2 \) values \( s \in \mathbb{Z}_{m_0} \).

Combining the above probabilities, one obtains the result of the lemma
\[
\Delta(y_I) = H(X) - H(X \mid Y_I = y_I)
= \log m_0 - \sum_{s \in \mathbb{Z}_{m_0}} P(X = s \mid Y_I = y_I) \log \frac{1}{P(X = s \mid Y_I = y_I)}
= \log m_0 + \sum_{s \in \mathbb{Z}_{m_0}} P(X = s \mid Y_I = y_I) \log P(X = s \mid Y_I = y_I)
= \log m_0 + \delta_1 \left\lfloor \frac{C_I}{m_0} \right\rfloor \log \left( \frac{C_I}{m_0} \right) + \delta_2 \left\lfloor \frac{C_I}{m_0} \right\rfloor + 1 \log \left( \frac{C_I}{m_0} + 1 \right)
\]
where \( q = \left\lfloor \frac{C_I}{m_0} \right\rfloor \).

**Proposition 4.4.3.** [27] Corollary 4.2.5 is a direct consequence of Lemma 4.4.2.

**Proof.** If \( C(I) = 0 \), the results follows. We prove now for \( C(I) \neq 0 \).

For simplicity, replace \( \left\lfloor \frac{C_I}{m_0} \right\rfloor \) by \( q \), where \( C_I = m_0 \cdot q + \delta_2 \) and \( \delta_1 + \delta_2 = m_0 \).
Thus,

\[ \Delta(y_I) = \log m_0 + \delta_1 \frac{q}{C_I} \log \frac{q}{C_I} + \delta_2 \frac{q+1}{C_I} \log \frac{q+1}{C_I} \]

\[ \leq \log m_0 + \left( \delta_1 \frac{q}{C_I} + \delta_2 \frac{q+1}{C_I} \right) \log \frac{q+1}{C_I} \]

\[ = \log m_0 + \frac{\delta_1 q + \delta_2 (q + 1)}{C_I} \log \frac{q+1}{C_I} . \]

As \( \delta_1 q + \delta_2 (q + 1) = C_I \), we replace \( q \) back with \( \lfloor C_I/m_0 \rfloor \). Thus,

\[ \Delta(y_I) \leq \log m_0 + \log \frac{q + 1}{C_I} = \log m_0 + \log \left( \frac{C_I}{m_0} \right) + 1 . \]

As \( C(I) \leq C_I \leq C(I) + 1 \), the result is straightforward

\[ \Delta(y_I) \leq \log \frac{m_0 \left( \frac{C(I)+1}{m_0} \right) + 1}{C(I)} . \]

\[ \square \]

**Corollary 4.4.4.** Let \( C(I) \) be defined as in Lemma 4.2.4. The result in Lemma 4.4.2, equally holds for the GRS \((t,n,m_0,m_1,\ldots,m_n)\)-threshold scheme.

**Proof.** This is similar to the proof of Lemma 4.4.2, with the following difference:

- \( \prod_{i=1}^{t+1} m_i \) should be replaced by \( m_0 \prod_{i=1}^{t} m_i \).

\[ \square \]

### 4.5 Security of the GRS scheme

In [51] it was shown that the GRS \((t+1,n)\)-threshold scheme is asymptotically ideal (and, therefore, asymptotically perfect), and perfect zero-knowledge if consecutive primes are considered.

Regarding our contribution to the security of the GRS \((t+1,n)\)-threshold scheme, we have introduced compact sequences of co-primes [3] and extended the results in [51] to include \((t,\Theta)\)-compact sequences. Theorems 4.5.1 and 4.5.2 are proven using the definitions of [51] (see Definitions 4.2.2 and 4.2.3).

Then, in [21] with the introduction of \(k\)-compact sequence we proved there exists a necessary and sufficient condition regarding the security of the GRS scheme. Meaning, the GRS \((t+1,n)\)-threshold scheme is asymptotically ideal if and only if \((1)\)-compact sequences are considered. The result is given in Theorem 4.5.3 and Corollary 4.5.4.

We proved in [3] that the GRS \((t+1,n)\)-threshold scheme based on \((t,\Theta)\)-compact sequences is perfect zero-knowledge. The results is shown in Theorem 4.5.5, and extended to \(k\)-compact sequences in Theorem 4.5.6.
4.5. Security of the GRS scheme

With respect to the changes brought to the co-prime sequences used by the GRS scheme, we consider the following variations, obtained by simply changing the parameter setup phase

**parameter** consider \( m_0, m_1, \ldots, m_n \) a \( X \) sequence of co-primes. The integers \( t, n, m_0, m_1, \ldots, m_n \) are public parameters.

Where \( X \) is one of the following types of sequences:

- consecutive primes [51];
- \((t, \Theta)\)-compact sequences [3];
- and \( k \)-compact sequences [21].

In the case of the GRS \((t + 1, n)\)-threshold scheme based on \( k \)-compact sequences, the constraint \( s' < \prod_{i=1}^{t+1} m_i \) is added to the secret sharing phase.

### 4.5.1 Asymptotic idealness

For simplicity, consider the set of participants used to share the secret \( s \) in the GRS \((t + 1, n)\)-threshold scheme the set \( U = \{1, \ldots, n\} \) with \( n \geq 1 \).

**Theorem 4.5.1.** [3] Let \( 0 < t + 1 \leq n \) and \( \Theta \in (0, 1) \). The GRS \((t + 1, n)\)-threshold scheme based on \((t, \Theta)\)-compact sequences of co-primes is asymptotically perfect with respect to the uniform distribution over the secret space.

**Proof.** Let \( 0 < t + 1 \leq n \) be positive integers, \( m_0 < \cdots < m_n \) be a \((t, \Theta)\)-compact sequence of co-primes, and \( I \subseteq \{1, \ldots, n\} \) with \( |I| \leq t \). Therefore, there exists \( \theta \in (0, \Theta] \) such that \( m_n < m_0 + m_0^\theta \). Three cases are to be considered.

**Case 1:** \(|I| < t \). From Lemma 4.2.4 and by using the inequalities \( x - 1 < \lfloor x \rfloor \leq x \), one obtains

\[
\Delta(y_I) \leq \log \frac{m_0 m_1 \cdots m_t (m_0 + 1) \prod_{i \in I} m_i}{m_0 m_1 \cdots m_t - \prod_{i \in I} m_i}
\]

As \( m_0 < m_i < m_0 + m_0^\theta \) for any \( 1 \leq i \leq n \), and \(|I| < t \), the fraction in the right hand side of the above inequality goes to 1 as \( m_0 \) goes to infinity.

**Case 2:** \( I = \{1, \ldots, t\} \). Note that \( C(I) = m_0 \). As

\[
m_0 \cdot \prod_{i=1}^{t} m_i - C(I) \cdot \prod_{i \in I} m_i = 0,
\]

we have, from the proof of Corollary 4.2.4, \( C_I = C(I) = m_0 \).

From \( \delta_2 = C_I \mod m_0 \) and \( \delta_1 + \delta_2 = m_0 \), one obtains \( \delta_2 = 0 \) and \( \delta_1 = m_0 \).
Chapter 4. CRT-based threshold schemes and their security

Therefore, the conditional entropy is

\[
H(X \mid Y_I = y_I) = -\delta_1 \left\lfloor \frac{C_I}{m_0} \right\rfloor \log \frac{C_I}{m_0} - \delta_2 \left\lfloor \frac{C_I}{m_0} \right\rfloor + 1 \log \frac{C_I}{m_0} + 1
\]

As \( H(x) = \log m_0 \) (see Remark 4.4.1), the loss of entropy is

\[
\Delta(y_I) = H(X) - H(X \mid Y_I = y_I) = 0.
\]

Case 3: \(|I| = t\) and \(I \neq \{1, \ldots, t\}\). Then,

\[
m_0 \frac{m_1 \cdots m_t}{\prod_{i \in I} m_i} \leq m_0 \frac{m_t}{m_{t+1}} \leq m_0 \frac{m_t}{m_t + 2}
\]

As \( m_t \leq m_n - 2 < m_0 + m_0^\theta - 2 < 2m_0 - 2 \), it follows that

\[
m_0 \frac{m_t}{m_t + 2} < m_0 - 1
\]

which leads to \( C(I) < m_0 - 1 \). Then, from Lemma 4.4.2 and by using the inequality \( x - 1 < \lfloor x \rfloor \) it follows

\[
\Delta(y_I) \leq \log \frac{m_0}{C(I)} \leq \log \frac{m_0 \prod_{i \in I} m_i}{m_0 m_1 \cdots m_t - \prod_{i \in I} m_i}
\]

Similar to Case 1, the fraction in the right hand side of the above inequalities goes to 1 as \( m_0 \) goes to infinity.

From the above cases, we have that for any \( \epsilon > 0 \) there exists \( m \) such that \( \Delta(y_I) < \epsilon \) if \( m_0 \geq m \). \( \square \)

**Theorem 4.5.2.** [3] Let \( 0 < t + 1 \leq n \) and \( \Theta \in (0, 1) \). The GRS \((t + 1, n)\)-threshold scheme based on \((t, \Theta)\)-compact sequences of co-primes is asymptotically ideal with respect to the uniform distribution over the secret space.

**Proof.** Recall from Theorem 4.5.1 that the scheme is asymptotically perfect. Consider \( m_0 < \cdots < m_n \) a compact sequence of co-primes such that \( m_n < m_0 + m_0^\theta \) for some \( \theta \in (0, \Theta) \).

According to Definition 4.2.3,

\[
\frac{|Z_{m_i}|}{|Z_{m_0}|} = \frac{m_i}{m_0} < \frac{m_0 + m_0^\theta}{m_0}
\]

for any \( 1 \leq i \leq n \).

As \( \Theta \) is fixed, the right hand side of the last inequality goes to 1 as \( m_0 \) goes to infinity

Therefore, for any \( \epsilon > 0 \) there exists \( m \) such that \( |Z_{m_i}|/|Z_{m_0}| < 1 + \epsilon \) if \( m_0 \geq m \). \( \square \)
4.5. Security of the GRS scheme

**Theorem 4.5.3.** [21] Let \(0 < t + 1 \leq n\) be two positive integers and \(k \geq 1\) a real number. The GRS \((t + 1, n)\)-threshold scheme under the uniform distribution over the secret space is asymptotically perfect and its information rate goes asymptotically to \(k\) if and only if it is based on \(k\)-compact sequences of co-primes.

**Proof.** For simplicity, we prove our results using GRS \((t, n, m_0, m_1, \ldots, m_n)\) as a instance of the GRS \((t + 1, n)\)-threshold scheme.

Assume that GRS \((t, n, m_0, m_1, \ldots, m_n)\) is asymptotically perfect and its information rate goes asymptotically to \(k\).

Regarding the asymptotic nature of the information rate, we have that for any \(\epsilon \in (0, 1)\) there exists \(m \geq 0\) such that

\[
km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0 ,
\]

holds for any \(1 \leq i \leq n\).

**Claim:** For any \(\epsilon \in (0, 1)\) there exists \(\theta \in (0, 1)\) such that \(\epsilon m_0 \leq m_\theta\), where \(m_\theta\) is as above.

**Proof of Claim:** If \(\epsilon\) is taken from \((m_0^1, 1)\), then one can compute the value \(\theta = 1 + \log m_\theta \epsilon\); otherwise if \(\epsilon\) is from \((0, m_0^1)\), then any \(\theta \in (0, 1)\) should suffice.

Therefore, for any sequence \(m_0, m_1 < \cdots < m_n\) of co-primes with \(km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0\) for all \(1 \leq i \leq n\) and some \(\epsilon \in (0, 1)\) there exists \(\theta \in (0, 1)\) (defined as in the Claim) such that

\[
km_0 - m_\theta \leq km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0 \leq km_0 + m_\theta .
\]

According to Definition 4.3.3, the sequence \(m_0, m_1 < \cdots < m_n\) is \(k\)-compact.

We prove now the converse of the theorem, that given a \((k, \theta)\)-compact sequence \(m_0, m_1 < \cdots < m_n\) of co-primes, the GRS \((t, n, m_0, m_1, \ldots, m_n)\)-threshold scheme is asymptotically perfect and its information rate goes asymptotically to \(k\).

**Asymptotic perfectness.** Let \(I \subseteq \{1, \ldots, n\}\) a non-empty set with \(|I| \leq t\). The following cases are considered.

**Case 1:** \(|I| < t\). Using \(x - 1 < \lfloor x \rfloor \leq x\) over the result in Lemma 4.2.4, we obtain

\[
\Delta(g_I) \leq \log \frac{\min\{m_0, m_{t+1}\} \cdot m_1 \cdots m_t + (m_0 + 1) \prod_{i \in I} m_i}{\min\{m_0, m_{t+1}\} \cdot m_1 \cdots m_t - \prod_{i \in I} m_i} .
\]

As \(|I| < t\) and \(km_0 - m_\theta^0 < m_i < km_0 + m_\theta^0\) for all \(1 \leq i \leq n\), the right hand side of the above inequality goes to 0 as \(m_0\) goes to infinity. This shows that for any \(\epsilon \in (0, 1)\) there exists \(m\) such that \(\Delta(g_I) < \epsilon\) if \(m_0 \geq m\).
Chapter 4. CRT-based threshold schemes and their security

Case 2: $I = \{1, \ldots, t\}$. Note that $C(I) = m_0$, and

$$m_0 \cdot \prod_{i=1}^{t} m_i - C(I) \cdot \prod_{i \in I} m_i = 0.$$ 

Therefore, from the proof of Corollary 4.4.4, we have $C_I = C(I) = m_0$.

As $\delta_2$ is defined as $C_I \mod m_0$ and $\delta_1 + \delta_2 = m_0$, we have $\delta_2 = 0$ and $\delta_1 = m_0$.

According to Corollary 4.4.4, the loss of entropy is

$$\Delta(y_I) = \log m_0 + \delta_1 \frac{|C_I|}{m_0} \log \frac{|C_I|}{C_I} + \delta_2 \frac{|C_I| - 1}{|C_I|} \log \frac{|C_I|}{C_I} + 1$$

$$= \log m_0 + \frac{m_0}{|C_I|} \log \frac{1}{C_I}$$

$$= \log 1 = 0.$$ 

Case 3: $m_0 < m_{t+1}$ and $|I| = t$ and $I \neq \{1, \ldots, t\}$. From

$$C(I) < m_0 \frac{m_1 \cdots m_t}{\prod_{i \in I} m_i} \leq m_0 \frac{m_t}{m_{t+1}} \leq m_0 \frac{m_t}{m_t + 1} = m_0 \left( 1 - \frac{1}{m_t + 1} \right)$$

and $m_t + 1 < km_0 + m_0^\theta$, clearly $C(I) < m_0$. Furthermore, $C(I)$ is a positive integer, and as such we have

$$C(I) \leq m_0 - 1.$$ 

Consider the two sub-cases $C(I) = m_0 - 1$ and $C(I) < m_0 - 1$.

Case 3.1: $C(I) = m_0 - 1$. Let $x_0$ denote the unique solution modulo $\mathbb{Z}_{\prod_{i \in I} m_i}$ over the shares of the participants in $I$, and let

$$B = \left\{ x \in \mathbb{Z}_{\prod_{i \in I} m_i} \mid x \equiv x_0 \mod \prod_{i \in I} m_i \right\}.$$ 

Let $x_0 + r \cdot \prod_{i \in I} m_i$ be an element in $B$. If $x_0 \leq m_1 \cdots m_{t-1}(m_t + 1 - m_0)$ then $r \leq m_0 - 1$, otherwise $r \leq m_0 - 2$. Therefore, $m_0 - 1 \leq |B| \leq m_0$.

If $|B| = m_0$ then it follows $P(X = s | Y_I = y_I) = 1/m_0$ in a similar way to Case 2. If $|B| = m_0 - 1$, then there exists at most one $x \in B$ such that $s \equiv x \mod m_0$, for each secret $s$. As a conclusion, $P(X = s | Y_I = y_I)$ is either $1/(m_0 - 1)$ or 0.

These facts lead to

$$\log(m_0 - 1) \leq H(X | Y_I = y_I) \leq \log m_0$$

and, therefore,

$$0 \leq \Delta(y_I) \leq \log \frac{m_0}{m_0 - 1}.$$ 

This shows that for any $\epsilon \in (0, 1)$ there exists $m$ such that $|\Delta(y_I)| < \epsilon$ if $m_0 \geq m$. 

107
Case 3.2: $C(I) < m_0 - 1$. Based on Lemma 4.2.4 and on the inequality $x - 1 < \lfloor x \rfloor$ we obtain

$$\Delta(y_I) \leq \log \frac{m_0}{C(I)} \leq \log \frac{m_0 \prod_{i \in I} m_i}{m_0 m_1 \cdots m_t - \prod_{i \in I} m_i}$$

As in the first case, the fraction in the right hand side of the above inequalities goes to 1 as $m_0$ goes to infinity and, therefore, we obtain the same conclusion as in the first case.

Case 4: $m_0 > m_{t+1}$ and $|I| = t$. Then,

$$C(I) = \left\lfloor \frac{m_{t+1} \cdot \prod_{i=1}^t m_i}{\prod_{i \in I} m_i} \right\rfloor \leq m_{t+1} \leq m_0 - 1.$$

As one can easily see, the same analysis as in the cases 3.1 and 3.2 can be carried here (with the same conclusions).

Information rate. The following inequalities hold for all $1 \leq i \leq n$ and any $(k, \Theta)$-compact sequence $m_0, m_1 < \cdots < m_n$ of co-primes

$$\frac{km_0 - m_i^\Theta}{m_0} < \frac{|Z_{m_i}|}{m_0} = \frac{m_i}{m_0} < \frac{km_0 + m_i^\Theta}{m_0},$$

which show that the information rate goes to $k$ as $m_0$ goes to infinity. □

Corollary 4.5.4. [21] Let $0 < t + 1 \leq n$ be two positive integers. The GRS $(t + 1, n)$-threshold scheme under the uniform distribution over the secret space is asymptotically ideal if and only if it is based on $1$-compact sequences of co-primes.

Proof. This is the case $k = 1$ in Theorem 4.5.3. □

4.5.2 Perfect zero-knowledge

Theorem 4.5.5. [3] Let $0 < t + 1 \leq n$ and $\Theta \in (0, 1)$. The GRS $(t + 1, n)$-threshold scheme based on $(t, \Theta)$-compact sequences of co-primes is perfect zero-knowledge with respect to the uniform distribution over the secret space.

Proof. Let $0 < t + 1 \leq n$ be positive integers, and $m_0, m_1 < \cdots < m_n$ be a $(t, \Theta)$-compact sequence of co-primes, for some $\Theta \in (0, 1)$. Given two secret $s, s' \in \mathbb{Z}_{m_0}$, and $I \subseteq \{1, \ldots, n\}$ a non-empty set with $|I| \leq t$, we introduce the uniform random variable $U_I$ which takes values in $\prod_{i \in I} \mathbb{Z}_{m_i}$.

As

$$|P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I)| \leq |P(Y_{s,I} = y_I) - P(U_I = y_I)| + |P(Y_{s',I} = y_I) - P(U_I = y_I)|$$

it is sufficient to prove a suitable upper bound exists for the term

$$\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{s,I} = y_I) - P(U_I = y_I)|$$
To simplify the notations, let $M_t = \prod_{i=1}^{t} m_i$ and $M_I = \prod_{i \in I} m_i$.

As there exists an isomorphism $\varphi$ from $\prod_{i \in I} \mathbb{Z}_{m_i}$ to $\mathbb{Z}_{M_I}$, we can define a new random variable $Z_I$ such that $U_I$ takes the value $y_I$ with probability $p$ if and only if $Z_I$ takes the value $\varphi(y_I)$ with probability $p$.

*Claim:* Given the shares $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, obtained from the secret $s \in \mathbb{Z}_{m_0}$, there exits only one $r \in M_I$ such that $y_I = (s + rm_0) \mod m_i$ for all $i \in I$. Furthermore, for each $r$ there exist $\lfloor M_I/M_t \rfloor$ values of $r' \in M_I$ such that $r' = r \mod M_I$.

*Proof of Claim:* Recall that for any secret $s$ in $\mathbb{Z}_{m_0}$, there exists a quantity $s'$ in $m_0 \cdot M_I$ such that $s' = s \mod m_0$. (Note that $s'$ is the value from the description of the GRS scheme, and not the one from the definition of perfect zero-knowledge.) In other words, there exists a unique value $r'$ in $M_I$ such that $s' = s + r' \cdot m_0$.

Let $y_I$ be the shares in $\prod_{i \in I} \mathbb{Z}_{m_i}$, obtained from the secret $s$. Using the Chinese remainder theorem, over the shares $y_I$, leads to the secret $s^0$ in $\mathbb{Z}_{M_I}$. If $|I| \geq t + 1$, then $s^0 = s'$; otherwise $s^0 = s' \mod M_I$. Therefore, $s^0 = s + r' \cdot m_0$.

Replacing $s^0$ with the value of $s'$, we have $s^0 = s + r' \cdot m_0 \mod M_I$. As $r'$ is defined in $M_I$, let $r \in \mathbb{Z}_{M_I}$ be computed as $r = r' \mod M_I$. So, $s^0 = s + r \cdot m_0$.

Based on the uniqueness of the solution $s^0$, for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ there exists only one $r \in \mathbb{Z}_{M_I}$. For each $r' \in \mathbb{Z}_{M_I}$ there exists only one $r \in \mathbb{Z}_{M_I}$. However, for each $r$ there may exits none or more $r'$, depending on the value of $\lfloor M_I/M_t \rfloor$. Note that $\lfloor M_I/M_t \rfloor = (M_I - (M_t \mod M_I))/M_t$. ■

Therefore, based on the Claim, we can define the random variable $R_S$ with values into $\mathbb{Z}_{M_I}$ such that
\[
\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{s,t} = y_I) - P(U_I = y_I)| = \sum_{r \in \mathbb{Z}_{M_I}} |P(R_S \mod M_I = r) - P(Z_I = r)|
\]

If $0 \leq r < (M_t \mod M_I)$, then
\[
P(R_S \mod M_I = r) = \frac{M_t - (M_t \mod M_I)}{M_I} + 1,
\]
and if $(M_t \mod M_I) \leq r < M_I$, then
\[
P(R_S \mod M_I = r) = \frac{M_t - (M_t \mod M_I)}{M_IM_I}.
\]

As $P(Z_I = r) = 1/M_I$, we obtain
\[
\sum_{r \in \mathbb{Z}_{M_I}} |P(R_S \mod M_I = r) - P(Z_I = r)| = 2 \left( \frac{M_t \mod M_I}{M_I} - \frac{(M_t \mod M_I)^2}{M_tM_I} \right)
\]

If $|I| = t$, then $M_I \geq M_t$. If $|I| < t$, then $M_I < M_t^0 < M_t$ for sufficiently large $m_0$ because $m_0 < \cdots < m_n$ is a $(t, \Theta)$-compact sequence of co-primes.

Page 109
4.6. Security of the Asmuth-Bloom scheme

From these, the result of the theorem easily follows.

**Theorem 4.5.6.** [21] Let $0 < t + 1 \leq n$. The GRS $(t + 1, n)$-threshold scheme based on $k$-compact sequences of co-primes is perfect zero-knowledge with respect to the uniform distribution over the secret space.

**Proof.** We adapt the proof given in Theorem 4.5.5 to work for the case of $k$-compact sequences as well. We only have to replace “$M_I < m_0^t < M_t$ for sufficiently large $m_0$” in the last part of the proof by

“$M_I < (km_0 + m_0^\theta)^{t-1} < (km_0 - m_0^\theta)^t < M_t$ for some $\theta \in (0, 1)$ and sufficiently large $m_0$”.

4.6 Security of the Asmuth-Bloom scheme

Concerning the security of the Asmuth-Bloom scheme, from the proofs given in [51], one does not obtain the properties of asymptotic perfectness and asymptotic idealness for the Asmuth-Bloom scheme based on consecutive primes. However, regarding the perfect zero-knowledge property, one may adapt the proof given for the GRS scheme to work in the case of the Asmuth-Bloom scheme based on consecutive primes.

In [40] Kaya and Selcuk have felt that replacing the Asmuth-Bloom sequence by extended Asmuth-Bloom sequence may increase the security of the Asmuth-Bloom scheme, but no formal proof was given.

Let extended Asmuth-Bloom sequences of co-primes be defined by replacing the Asmuth-Bloom constraint with the following one:

$$\prod_{i=1}^{t+1} m_i > \prod_{i=0}^{t-1} m_{n-i} \quad (4.4)$$

(The extended Asmuth-Bloom sequences of co-primes are Asmuth-Bloom sequences of co-primes.)

Our contribution, consists of the introduction of compact sequences of co-primes [3] and proving that the Asmuth-Bloom scheme based on almost $\Theta$-compact sequences is asymptotically perfect, and the information rate is asymptotically 2. The result is presented in Theorems 4.6.2 and 4.6.3 (according to Definitions 4.2.2 and 4.3.8).

Moreover, we changed the secret space from the first element in the sequences of co-primes to the last element. Thus, obtaining a variant of the Asmuth-Bloom scheme that is asymptotically ideal if quasi-compact sequences are considered. Proofs are given in Theorems 4.6.4 and 4.6.5 (according to Definitions 4.2.2 and 4.3.7).

Additionally, we proved that the loss of entropy for the Asmuth-Bloom scheme based on Asmuth-Bloom sequences is asymptotically upper bounded by $\log 2$ (see Lemma 4.6.1).
Then, in [27] with the introduction of $k$-compact sequence, we proved there exists a necessary and sufficient condition regarding the security of the Asmuth-Bloom scheme. Meaning, the Asmuth-Bloom $(t + 1, n)$-threshold scheme is asymptotically ideal if and only if $(1-)$compact sequences are considered. The result is given in Theorem 4.6.6 and Corollary 4.6.8. Furthermore, the Asmuth-Bloom scheme based on extended Asmuth-Bloom sequences of co-primes is asymptotically perfect (see Theorem 4.6.9).

Concerning the perfect zero-knowledge property, we have based our proofs for the Asmuth-Bloom scheme on the result obtained by the GRS scheme. Thus, the Asmuth-Bloom $(t + 1, n)$-threshold scheme based on almost $\Theta$-compact sequences, or on quasi-compact sequences, or on $k$-compact sequences are perfect zero-knowledge. The results are shown in Theorem 4.6.11, in Theorem 4.6.12, and in Theorem 4.6.13.

With respect to the changes brought to the co-prime sequences used by the Asmuth-Bloom scheme, we consider the following variations obtained by simply changing the parameter setup phase

**parameter** consider $m_0, m_1, \ldots, m_n$ a $X$ sequence of co-primes. The integers $t, n, m_0, m_1, \ldots, m_n$ are public parameters.

Where $X$ is one of the following types of sequences:

- Asmuth-Bloom sequences [1];
- extended Asmuth-Bloom sequences [40];
- consecutive primes [51];
- almost $\Theta$-compact sequences [3];
- quasi-compact sequences [3, 27];
- $k$-compact sequences [21, 27].

Note that the rest of the Asmuth-Bloom scheme does not need to change, to reflect the modifications done to the sequence of co-primes.

For sufficiently large $m_0$, $k$-compact sequences $m_0, m_1 < \cdots < m_n$ of co-primes with $k \geq 2$ also satisfy the Asmuth-Bloom constraint. Indeed, the Asmuth-Bloom constraint is implied by the inequality

$$(km_0 - m_0^\theta)^{t+1} > m_0(km_0 + m_0^\theta)^t$$

As

$$\lim_{m_0 \to \infty} m_0 \frac{(km_0 + m_0^\theta)^t}{(km_0 - m_0^\theta)^{t+1}} = \frac{1}{k}$$

we conclude that the above inequality holds true for sufficiently large $m_0$. 

111
4.6. Security of the Asmuth-Bloom scheme

4.6.1 Asymptotic idealness

For simplicity, consider the set of participants used to share the secret $s$ in the Asmuth-Bloom $(t+1,n)$-threshold scheme the set $U = \{1, \ldots, n\}$ with $n \geq 1$.

Lemma 4.6.1. [3] Let $0 < t + 1 \leq n$ be positive integers. The loss of entropy of the Asmuth-Bloom $(t+1,n)$-threshold scheme based on Asmuth-Bloom sequences of co-primes under the uniform distribution over the secret space satisfies the following relations:

- $\Delta(y_I) \leq \log \left(1 + \frac{1}{m_0 - 1} + \frac{1}{m_0^2 - 1}\right)$, if $|I| < t$;
- $\Delta(y_I) < \log \left(2 + \frac{1}{m_0}\right)$, if $|I| = t$;

for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, for any sequence $m_0, m_1, \ldots, m_n$ of co-primes, and for any subset $I \subseteq \{1, \ldots, n\}$.

Proof. Let

$$C(I) = \left\lfloor \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i \in I} m_i} \right\rfloor.$$

Consider the following cases.

Case 1: $|I| < t$. From Corollary 4.2.5, and using $x - 1 < |x| \leq x$ we obtain

$$\Delta(y_I) \leq \log \frac{m_1 m_2 \cdots m_{t+1} + (m_0 + 1) \prod_{i \in I} m_i}{m_1 m_2 \cdots m_{t+1} - \prod_{i \in I} m_i}.$$

As $\prod_{i=0}^{t-1} m_i > \prod_{i \in I} m_i$, from the Asmuth-Bloom constraint, one can deduce that $\prod_{i=1}^{t+1} m_i > m_0^2 \prod_{i \in I} m_i$. Therefore,

$$\Delta(y_I) < \log \left(\frac{m_0^2 + m_0 + 1}{m_0^2 - 1}\right) = \log \left(1 + \frac{1}{m_0 - 1} + \frac{1}{m_0^2 - 1}\right).$$

Case 2: $|I| = t$. Similarly, from the Asmuth-Bloom constraint, we have $m_0 < C(I) \leq m_{t+1}$.

According to Corollary 4.2.5, the result of the lemma follows

$$\Delta(y_I) \leq \log \frac{m_0 \left(\frac{C(I) + 1}{m_0} + 1\right)}{C(I)} \leq \log \left(\frac{C(I) + m_0 + 1}{C(I)}\right) \leq \log \left(2 + \frac{1}{m_0}\right).$$

As a conclusion, the Asmuth-Bloom threshold scheme is not asymptotically perfect but, its loss of entropy is bounded from above by $\log 2$.

As the Asmuth-Bloom threshold scheme allows arbitrarily large gaps between $m_0$ and $m_i$, the information rate of the $i$th participant can be arbitrarily large, for any $1 \leq i \leq n$. 
Theorem 4.6.2. [3] Let $0 < t + 1 \leq n$ and $\Theta \in (0,1)$. The Asmuth-Bloom $(t+1,n)$-threshold scheme based on almost $\Theta$-compact sequences is asymptotically perfect if the secret is chosen uniformly from the secret space.

Proof. Let $m_0 < m_1 < \cdots < m_n$ be a almost $\Theta$-compact sequence of co-primes, from the interval $(x,x+x^\theta)$ with $[x+x^\theta] = 2m_0 - 2$, for some $\theta \in (0,\Theta]$.

Case 1: $|I| < t$. Using Corollary 4.2.5 (or Lemma 4.6.1), one obtains

$$\Delta(y_I) \leq \log \frac{m_1m_2 \cdots m_{t+1} + (m_0 + 1)\prod_{i \in I} m_i}{m_1m_2 \cdots m_{t+1} - \prod_{i \in I} m_i}$$

That, leads to

$$\Delta(y_I) < \log \left(1 + \frac{1}{m_0 - 1} + \frac{1}{m_0^2 - 1}\right).$$

When $m_0$ goes to infinity, the logarithm in the right hand side of the above inequality goes to 0.

Case 2: $|I| = t$. In this case we have $C(I) \leq m_{t+1} < 2m_0 - 2$ and $[(C(I)+1)/m_0] \leq 1$, for large enough $m_0$. Therefore,

$$\Delta(y_I) \leq \log \frac{m_0 \left[\frac{C(I)+1}{m_0}\right]+1}{C(I)} \leq \log \frac{2m_0}{C(I)}.$$

As $x < m_i < x+x^\theta \leq 2m_0 - 2$, the fraction in the right hand side of the above inequality goes to 1.

Based on Case 1 and 2, the Asmuth-Bloom $(t+1,n)$-threshold scheme based on almost $\Theta$-compact sequences is asymptotically perfect. \qed

Theorem 4.6.3. [3] Let $0 < t + 1 \leq n$ and $\Theta \in (0,1)$. The Asmuth-Bloom $(t+1,n)$-threshold scheme based on almost $\Theta$-compact sequences, under the uniform distribution over the secret space, has the information rate asymptotically 2.

Proof. Consider $m_0 < \cdots < m_n$ a almost $\Theta$-compact sequence of co-primes such that $x < m_i < x+x^\theta$ with $[x+x^\theta] = 2m_0 - 2$, for some $\theta \in (0,\Theta]$.

According to Definition 4.3.7,

$$\frac{x}{m_0} < \frac{|Z_{m_i}|}{|Z_{m_0}|} = \frac{m_i}{m_0} < \frac{x+x^\theta}{m_0} < \frac{2m_0 - 2}{m_0} < 2$$

for any $1 \leq i \leq n$.

When $m_0$ goes to infinity, the right hand side of the last inequality goes to 2, but the same can be said of the left hand side, as $\Theta$ is fixed. Therefore, for any $\epsilon > 0$ there exists $m$ such that $2 - \epsilon < |Z_{m_i}|/|Z_{m_0}| < 2 + \epsilon$ if $m_0 \geq m$. \qed
Theorem 4.6.4. [3] Let $0 < t + 1 \leq n$. The Asmuth-Bloom $(t + 1, n)$-threshold scheme based on quasi-compact sequences is asymptotically perfect with respect to the uniform distribution over the secret space.

Proof. Let $m_1 < \cdots < m_n < m_0$ be a quasi-compact sequence of co-primes, such that $m_0 - m_i^\theta < m_i < m_0$ for all $1 \leq i \leq n$, and for some $\theta \in (0, 1)$ (see Remark 4.3.4).

Case 1: $|I| < t$. Using Corollary 4.2.5, we have

$$\Delta(y_I) \leq \log \frac{m_1 m_2 \cdots m_{t+1} + (m_0 + 1) \prod_{i \in I} m_i}{m_1 m_2 \cdots m_{t+1} - \prod_{i \in I} m_i}$$

As $m_0 - m_i^\theta < m_i < m_0$ and $|I| \leq t - 1$, the logarithm in the right hand side of the above inequality goes to 0 when $m_0$ goes to infinity.

Case 2: $|I| = t$. As $C(I) \leq m_t$, we have

$$\left\lfloor \frac{C(I) + 1}{m_0} \right\rfloor = 0$$

The loss of entropy is bounded by

$$\Delta(y_I) \leq \log \frac{m_0}{C(I)} \leq \log \frac{m_0 \prod_{i \in I} m_i}{m_1 m_2 \cdots m_{t+1} - \prod_{i \in I} m_i}$$

As $|I| = t$ and $m_0 - m_i^\theta < m_i < m_0$ for all $1 \leq i \leq n$, and $|I| = t$, the fraction in the right hand side of the above inequality goes to 1 when $m_0$ goes to infinity.

Based on Case 1 and 2, the result of the theorem follows.

Theorem 4.6.5. [3] Let $0 < t + 1 \leq n$. The Asmuth-Bloom $(t + 1, n)$-threshold scheme based on quasi-compact sequences of co-primes is asymptotically ideal with respect to the uniform distribution over the secret space.

Proof. Recall from Theorem 4.6.4 that the scheme is asymptotically perfect.

Consider $m_1 < \cdots < m_n < m_0$ a quasi-compact sequence of co-primes, such that $m_0 - m_i^\theta < m_i < m_0$ for all $1 \leq i \leq n$, and for some $\theta \in (0, 1)$.

According to Definition 4.3.8,

$$1 \geq \frac{|Z_{m_i}|}{|Z_{m_0}|} = \frac{m_i}{m_0} > \frac{m_0 - m_i^\theta}{m_0}$$

for any $1 \leq i \leq n$. (Recall that quasi-compact are a particular case of $k$-compact sequences for $k = 1$.)

As $\Theta$ is fixed, the right hand side of the last inequality goes to 1 as $m_0$ goes to infinity.

Therefore, for any $\epsilon > 0$ there exists $m$ such that $1 - \epsilon < |Z_{m_i}|/|Z_{m_0}| < 1 + \epsilon$ if $m_0 \geq m$.

One may notice, that part of the proof given for the following theorem is similar with sections of the proof given in Theorem 4.5.3 for the GRS.
scheme. But, for uniformity, we do not omit anything from the following proof.

**Theorem 4.6.6.** [27] Let \(0 < t + 1 \leq n\) and \(k \geq 1\) be positive integers. The Asmuth-Bloom \((t + 1, n)\)-threshold scheme under the uniform distribution over the secret space is asymptotically perfect and its information rate goes asymptotically to \(k\) if and only if it is based on \(k\)-compact sequences of co-primes.

**Proof.** We prove our results using Asmuth-Bloom \((t, n, m_0, m_1, \ldots, m_n)\) as an instance of the Asmuth-Bloom \((t + 1, n)\)-threshold scheme.

Assume that the Asmuth-Bloom \((t, n, m_0, m_1, \ldots, m_n)\) scheme is asymptotically perfect and its information rate goes asymptotically to \(k\).

In regard with the asymptotic nature of the information rate, we have that for any \(\epsilon \in (0, 1)\) there exists \(m \geq 0\) such that

\[
km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0,
\]

holds for any \(1 \leq i \leq n\).

We prove that for any \(\epsilon \in (0, 1)\) there exists \(\theta \in (0, 1)\) such that \(\epsilon m_0 \leq m_0^\theta\), where \(m_0\) is as above.

If \(\epsilon\) is taken from \((m_0^{-1}, 1)\), then one can compute \(\theta = 1 + \log_{m_0} \epsilon\); otherwise if \(\epsilon\) is from \((0, m_0^{-1})\), then any \(\theta \in (0, 1)\) should suffice.

Therefore, given any sequence \(m_0, m_1 < \cdots < m_n\) of co-primes with \(km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0\) for all \(1 \leq i \leq n\) and some \(\epsilon \in (0, 1)\) there exists \(\theta \in (0, 1)\) (defined as above) such that:

\[
km_0 - m_0^\theta \leq km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0 \leq km_0 + m_0^\theta.
\]

According to Definition 4.3.3, the sequence \(m_0, m_1 < \cdots < m_n\) is \(k\)-compact.

We prove now the converse of this theorem. We prove that the Asmuth-Bloom \((t + 1, n)\)-threshold scheme is asymptotically perfect and its information rate goes asymptotically to \(k\) if it is based on \(k\)-compact sequences of co-primes and the secret is uniformly chosen from the secret space.

Asymptotic perfection. Let \(I \subseteq \{1, \ldots, n\}\) be a non-empty set with \(|I| \leq t\), and let \(\theta \in (0, 1)\). The following cases are to be considered.

**Case 1:** \(|I| < t\). Using \(x - 1 < |x| \leq x\) over the result in Corollary 4.2.5, we obtain

\[
\Delta(y_I) \leq \log \frac{m_0 m_1 \cdots m_t + (m_0 + 1) \prod_{i \in I} m_i}{m_0 m_1 \cdots m_t - \prod_{i \in I} m_i}.
\]

As \(|I| < t\) and \(km_0 - m_0^\theta < m_i < km_0 + m_0^\theta\) for all \(1 \leq i \leq n\), the right hand side of the above inequality goes to 0 as \(m_0\) goes to infinity.

**Case 2:** \(|I| = t\). We prove first the following Claim which establishes lower and upper bounds for \(C_I\).
4.6. Security of the Asmuth-Bloom scheme

Claim: For any $\theta \in (0,1)$ there exists $m$ such that any $(k,\theta)$-compact sequence $m_0, m_1, \ldots, m_n$ with $m_0 \geq m$ satisfies:

$$km_0 - (m_0^\theta + 1) < C_I < km_0 + (m_0^\theta + 1)$$

Proof of Claim: Note that

$$C(I) \leq \prod_{i=1}^{t+1} m_i \leq \prod_{i=1}^{t+1} m_i = m_{t+1}.$$

As $C_I \leq C(I) + 1$ (from Lemma 4.4.2), we have $C_I \leq m_{t+1} + 1 < km_0 + (m_0^\theta + 1)$.

One can easily see that

$$\lim_{m_0 \to \infty} \frac{\prod_{i=1}^{t+1} m_i}{m_0 \prod_{i \in I} m_i} = k$$

and thus, for any $\epsilon > 0$ and sufficiently large $m_0$ we have

$$\frac{\prod_{i=1}^{t+1} m_i}{m_0 \prod_{i \in I} m_i} > k - \epsilon.$$

Therefore, for any $\epsilon > 0$ and sufficiently large $m_0$ the following holds:

$$C_I \geq C(I) \geq \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i \in I} m_i} - 1 > km_0 - \epsilon m_0 - 1$$

For $\epsilon < m_0^{\theta-1}$ we obtain the inequality in the Claim.

Let Asmuth-Bloom $(t, n, m_0, m_1, \ldots, m_n)$ be a instance of the Asmuth-Bloom $(t+1, n)$-threshold scheme, where $m_0, m_1 < \ldots < m_n$ is a $(k, \theta)$-compact sequence of co-primes, which satisfies Claim 1. The following two cases are in order:

Case 2.1: Consider $km_0 - (m_0^\theta + 1) < C_I < km_0$. Then, $\left\lfloor \frac{C_I}{m_0} \right\rfloor = k - 1$. As

$$C_I = m_0 \cdot \left\lfloor \frac{C_I}{m_0} \right\rfloor + \delta_2,$$

we obtain

$$m_0 - (m_0^\theta + 1) < \delta_2 < m_0$$

which shows that $\delta_2/m_0$ goes to 0 and $\delta_1$ goes to 0 as $m_0$ goes to infinity (recall that $\theta$ is fixed). Then, from Lemma 4.4.2 it follows:

$$\Delta(y_I) = \log m_0 + \delta_1 \left\lfloor \frac{C_I}{m_0} \right\rfloor \log \frac{C_I}{m_0} + \delta_2 \left\lfloor \frac{C_I}{m_0} \right\rfloor + \log \frac{C_I}{m_0} + 1$$

$$= \log m_0 + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k-1}{(k-1)m_0 + \delta_2}$$

$$+ \delta_2 \frac{k}{(k-1)m_0 + \delta_2} \log \frac{k}{(k-1)m_0 + \delta_2}$$

$$= \log m_0 + (\delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} + \delta_2 \frac{k}{(k-1)m_0 + \delta_2}) \log \frac{k}{(k-1)m_0 + \delta_2}$$

$$+ \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k}{(k-1)m_0 + \delta_2} - \log \frac{k}{(k-1)m_0 + \delta_2}$$

116
Chapter 4. CRT-based threshold schemes and their security

\[ \Delta(y_i) = \log m_0 + \log k \frac{(k-1)m_0 + \delta_2}{(k-1)m_0 + \delta_2} + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k-1}{k} \]

\[ = \log \frac{k m_0}{(k-1)m_0 + \delta_2} + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k-1}{k} \]

\[ = \log \frac{k m_0}{k m_0 - \delta_1} + \delta_1 \frac{k-1}{k m_0 - \delta_1} \log \frac{k-1}{k} \]

if \( k > 1 \), and

\[ \Delta(y_i) = \log m_0 + \delta_1 \frac{C_i}{m_0} \log \frac{C_i}{C_f} + \delta_2 \frac{C_i}{m_0} + 1 \log \frac{C_i}{m_0} + 1 \]

\[ = \log \frac{m_0}{\delta_2} \]

\[ = \log \frac{m_0}{m_0 - \delta_1} \]

if \( k = 1 \) (the convention \( 0 \log 0 = 0 \) was used).

As both \( \delta_1 / (km_0 - \delta_1) \) and \( \delta_1 / m_0 \) go to 0 as \( m_0 \) goes to infinity, we deduce that \( \Delta(y_i) \) goes to 0 as \( m_0 \) goes to infinity.

**Case 2.2:** Consider \( km_0 \leq C_I < km_0 + (m_0^\theta + 1) \). Then, \( \left[ \frac{C_I}{m_0} \right] = k \). As \( C_I = m_0 \cdot \left[ \frac{C_I}{m_0} \right] + \delta_2 \), we obtain

\[ 0 \leq \delta_2 < m_0^\theta + 1 \]

which shows that \( \delta_2 / m_0 \) goes to 0 and \( \delta_1 \) goes to 1 as \( m_0 \) goes to infinity (recall that \( \theta \) is fixed). Then, from Lemma 4.4.2 it follows:

\[ \Delta(y_i) = \log m_0 + \delta_1 \frac{C_I}{m_0} \log \frac{C_I}{C_f} + \delta_2 \frac{C_I}{m_0} + 1 \log \frac{C_I}{m_0} + 1 \]

\[ = \log m_0 + \delta_1 \frac{k}{km_0 + \delta_2} \log \frac{k}{km_0 + \delta_2} + \delta_2 \frac{k+1}{km_0 + \delta_2} \log \frac{k+1}{km_0 + \delta_2} \]

\[ = \log m_0 + \delta_1 \frac{k}{km_0 + \delta_2} + \delta_2 \frac{k+1}{km_0 + \delta_2} \log \frac{k+1}{k} \]

As \( \delta_2 / (km_0 + \delta_2) \) goes to 0 as \( m_0 \) goes to infinity, we deduce that \( \Delta(y_i) \) goes to 0 as \( m_0 \) goes to infinity.

**Information rate.** The following inequalities hold for all \( 1 \leq i \leq n \) and any \((k, \theta)\)-compact sequence \( m_0, m_1 < \cdots < m_n \) of co-primes

\[ \frac{km_0 - m_0^\theta}{m_0} < \left| \frac{Z_{m_i}}{Z_{m_0}} \right| = \frac{m_i}{m_0} < \frac{km_0 + m_0^\theta}{m_0} \]

which show that the information rate goes to \( k \) as \( m_0 \) goes to infinity. \( \square \)

As one may notice, the \( k \)-compact sequences used in the Asmuth-Bloom scheme, considers \( k \geq 1 \) a positive integer. In the following proposition, we prove that if \( k \) is anything other than an integer, the Asmuth-Bloom scheme
4.6. Security of the Asmuth-Bloom scheme

is not asymptotically perfect.

Proposition 4.6.7. The Asmuth-Bloom \((t+1,n)\)-threshold scheme is not asymptotically perfect if it based on \(k\)-compact sequences with \(k\) not an integer.

Proof. Let \(k \geq 1\) be a real number but not a integer, then there exists \(c\) a positive integer and \(d \in (0,1)\) such that \(c = \lfloor k \rfloor\) and \(k = c + d\). Consider the \(m_0, m_1, \ldots, m_n\) a \(k\)-compact sequence. Therefore, \([C_I/m_0] = c\).

From Lemma 4.4.2 we have \(\delta_2 = C_I \mod m_0\). As \(\delta_2/m_0\) goes to \(d\) as \(m_0\) goes to infinity, let \(\delta_2 = dm_0 + \epsilon\) for some \(\epsilon > 0\).

According to Lemma 4.4.2, the loss of entropy is:

\[
\Delta(y_I) = \log m_0 + \delta_1 \frac{C_I}{m_0} \log \frac{C_I}{m_0} + \delta_2 \frac{C_I}{m_0} \log \left(\frac{C_I}{m_0} + \frac{1}{C_I}\right) + \frac{1}{C_I} \log \left(\frac{C_I}{m_0} + 1\right)
\]

For simplicity, let \(q\) be the fraction \(\frac{(c+1)\delta_2}{C_I m_0 + \delta_2}\). As \(m_0\) goes to infinity, \(q\) goes to \(\frac{d(c+1)\delta_2}{c} \frac{m_0}{m_0 + d}\). Therefore,

\[
\Delta(y_I) = \log \frac{c(c+1)^2m_0}{c^2(c+d)m_0 + \epsilon c^2}
\]

which shows that the entropy loss goes to zero as \(m_0\) goes to infinity.

Corollary 4.6.8. [27] The Asmuth-Bloom \((t + 1,n)\)-threshold scheme under the uniform distribution over the secret space is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes.

Proof. This is the case \(k = 1\) in Theorem 4.6.6.

Theorem 4.6.9. [27] Let \(0 < t + 1 \leq n\) be positive integers. The Asmuth-Bloom \((t+1,n)\)-threshold scheme based on extended Asmuth-Bloom sequences of co-primes is asymptotically perfect with respect to the uniform distribution over the secret space.

Proof. Let \(I \subseteq \{1,\ldots,n\}\) be a non-empty set with \(|I| \leq t\). Then, \(C(I) > m_0^3\) for any extended Asmuth-Bloom sequence of co-primes \(m_0, m_1, \ldots, m_n\). Then, Corollary 4.2.5 leads to

\[
\Delta(y_I) \leq \log \frac{C(I) + 2m_0}{C(I)}
\]

which shows that the entropy loss goes to zero as \(m_0\) goes to infinity. 

\[
\text{\(118\)}
\]
Remark 4.6.10. One may define extended Asmuth-Bloom sequences of co-primes in a more liberal way by requiring
\[ \prod_{i=1}^{t+1} m_i > m_0^{1+\theta} \prod_{i=0}^{t-1} m_{n-i} \]
for some real number \( \theta > 0 \).

The result in Theorem 4.6.9 holds in this case too. Moreover, \( m_0^{1+\theta} < m_1 \)
which shows that the information rate of the first participant (and in fact, of all participants) is greater than \( m_0^\theta \).

4.6.2 Perfect zero-knowledge

Theorem 4.6.11. [3] Let \( 0 < t + 1 \leq n \) and \( \Theta \in (0,1) \). The Asmuth-Bloom \( (t + 1, n) \)-threshold scheme based on almost \( \Theta \)-compact sequences of co-primes is perfect zero-knowledge with respect to the uniform distribution over the secret space.

Proof. Let \( 0 < t + 1 \leq n \) be positive integers, and \( m_0, m_1 < \cdots < m_n \) be a almost \( \Theta \)-compact sequence of co-primes, for some \( \theta \in (0,1) \). Given two secret \( s, s' \in \mathbb{Z}_{m_0} \), and \( I \subseteq U \) a non-empty set with \( |I| \leq t \), we introduce the uniform random variable \( U_I \) which takes values in \( \prod_{i \in I} \mathbb{Z}_{m_i} \).

As
\[ |P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I)| \leq |P(Y_{s,I} = y_I) - P(U_I = y_I)| + |P(Y_{s',I} = y_I) - P(U_I = y_I)| \]
it is sufficient to prove a suitable upper bound exists for the term
\[ \sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{s,I} = y_I) - P(U_I = y_I)| \]

To simplify the notations, let \( M_I = \sum_{i=1}^{t+1} m_i / m_0 \) and \( M_I = \prod_{i \in I} m_i \).

There exists an isomorphism \( \varphi \) from \( \prod_{i \in I} \mathbb{Z}_{m_i} \) to \( \mathbb{Z}_{M_I} \). Let \( Z_I \) denote a random variable such that \( Z_I \) takes the value \( \varphi(y_I) \) with probability \( p \) if and only if \( U_I \) takes the value \( y_I \) with probability \( p \).

As the secret \( s \) was used to obtain the shares \( y_I \), there exists an unique \( r' \in M_I \) such that \( y_i = (s + r' \cdot m_0) \mod m_i \) for all \( i \in I \). Let \( r \in M_I \) be obtained from \( r' \) as \( r = r' \mod M_I \). The value \( r \) is also unique with respect to \( s \) and \( y_I \). However, for each \( r \) there may exits none or more \( r' \), depending on the value of \( |M_I/M_I| \). (Note that \( |M_I/M_I| = (M_I - (M_I \mod M_I))/M_I \).

Therefore, we can define the random variable \( R_S \) with values into \( \mathbb{Z}_{M_I} \) such that
\[ \sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{s,I} = y_I) - P(U_I = y_I)| = \sum_{r \in \mathbb{Z}_{M_I}} |P(R_S \mod M_I = r) - P(Z_I = r)| \]
4.7. Security of the Mignotte scheme

If \(0 \leq r < (M_t \mod M_I)\), then

\[
P(R_S \mod M_I = r) = \frac{M_I - (M_t \mod M_I)}{M_I} + 1,
\]

and if \((M_t \mod M_I) \leq r < M_I\), then

\[
P(R_S \mod \prod_{i \in I} m_i = r) = \frac{M_I - (M_t \mod M_I)}{M_I}\prod_{i \in I} m_i.
\]

As \(P(Z_I = r) = 1/M_I\), we obtain

\[
\sum_{r \in Z_I} |P(R_S \mod M_I = r) - P(Z_I = r)| = 2 \left(\frac{M_I \mod M_I}{M_I} - \frac{(M_t \mod M_I)^2}{M_I}\right).
\]

If \(|I| = t\), then \(M_I < M_t\). If \(|I| < t\), then \(M_I < m_1^t < M_t\) for sufficiently large \(m_0\) because \(m_0 < \cdots < m_n\) is a almost \(\Theta\)-compact sequence of co-primes.

From these, the result of the theorem easily follows.

**Theorem 4.6.12.** [3] Let \(0 < t + 1 \leq n\). The Asmuth-Bloom \((t + 1, n)\)-threshold scheme based on quasi-compact sequences of co-primes is perfect zero-knowledge with respect to the uniform distribution over the secret space.

**Proof.** We adapt the proof given in Theorem 4.6.11 to work for the case of quasi-compact sequences as well. We only have to replace “\(M_I < m_1^t < M_t\)” for sufficiently large \(m_0\)” in the last part of the proof by

“\(M_I < m_0^{\theta t - 1} < (m_0 - m_0^\theta)^t < M_t\)” for some \(\theta \in (0, 1)\) and sufficiently large \(m_0\).”

**Theorem 4.6.13.** [27] Let \(0 < t + 1 \leq n\). The Asmuth-Bloom \((t + 1, n)\)-threshold scheme based on \(k\)-compact sequences of co-primes is perfect zero-knowledge with respect to the uniform distribution over the secret space.

**Proof.** We adapt the proof given in Theorem 4.6.11 to work for the case of \(k\)-compact sequences as well. We only have to replace “\(M_I < m_1^t < M_t\)” for sufficiently large \(m_0\)” in the last part of the proof by

“\(M_I < (km_0 + m_0^\theta)^{t-1} < (km_0 - m_0^\theta)^t < M_t\)” for some \(\theta \in (0, 1)\) and sufficiently large \(m_0\).”

### 4.7 Security of the Mignotte scheme

To our knowledge, the security of the Mignotte scheme has never been studied using the modern concepts of asymptotic perfectness, and perfect zero-knowledge. In [3] we have studied the security of the Mignotte scheme using compact sequences. As we will show in this section, there is no reason to adapt the proofs to take into account \(k\)-compcteness.
Chapter 4. CRT-based threshold schemes and their security

**Theorem 4.7.1.** [3] Let \( 0 < t + 1 \leq n \) be positive integers. The loss of entropy of the Mignotte \((t + 1, n)\)-threshold scheme cannot be bounded from above.

**Proof.** Let \( U = \{1, \ldots, n\} \) be the set of all participants, and \( I \subseteq U \) a non-empty subset at most \( t \) participants.

As the system
\[
x \equiv s \mod m_i, \quad \forall i \in I
\]
has a unique solution \( x_0 \) in \( \mathbb{Z}_{\prod_{i \in I} m_i} \) (obtained by CRT), the secret \( s \) should take the form
\[
s = x_0 + j \cdot \prod_{i \in I} m_i,
\]
where \( j \) satisfies
\[
\left| \frac{\alpha - x_0}{\prod_{i \in I} m_i} \right| < j \leq \left| \frac{\beta - x_0}{\prod_{i \in I} m_i} \right|,
\]
This means that \( j \) can take at most \( \lceil (\beta - \alpha + \prod_{i \in I} m_i)/\prod_{i \in I} m_i \rceil \) and at least \( \lfloor (\beta - \alpha - \prod_{i \in I} m_i)/\prod_{i \in I} m_i \rfloor \) values.

Note that the conditional probability of the secret \( s \) given by the shares \( y_I \) is
\[
P(X = s | Y_I = y_I) \geq \frac{1}{\left| \prod_{i \in I} m_i \right|}.
\]

As \( P(X = s | Y_I = y_I) \) defines a probability distribution over \( \prod_{i \in I} \mathbb{Z}_{m_i} \),
we obtain
\[
\Delta(y_I) \geq \log(\beta - \alpha - 1) - \log \left| \frac{\beta - \alpha + \prod_{i \in I} m_i}{\prod_{i \in I} m_i} \right| = \log \frac{\beta - \alpha - 1}{\left| \prod_{i \in I} m_i \right|}.
\]

The right hand side of the above inequality goes to infinity as \( m_1 \) goes to infinity, as the numerator of the fraction is \( O(m_1^{t+1}) \) while the denominator is \( O(m_1^{t+1-|I|}) \). (Note that compact sequences were used.)

Therefore, the loss of entropy cannot be bounded.

Based on Theorem 4.7.1, we must conclude that the scheme is not asymptotically perfect.

**Theorem 4.7.2.** [3] Let \( 0 < t + 1 \leq n \) be positive integers. The information rate of the Mignotte \((t + 1, n)\)-threshold scheme converges to 0.

**Proof.** The secret space is of size \( O(m_1^{t+1}) \). This leads to the fact that the information rate \( m_i/(\beta - \alpha - 1) \) of the \( i \)th participant converges to 0 as \( m_1 \) goes to infinity.

Therefore, based on Theorem 4.7.2, the Mignotte threshold scheme is far from being asymptotically ideal.

**Theorem 4.7.3.** [3] Let \( 0 < t + 1 \leq n \) be positive integers. The Mignotte \((t + 1, n)\)-threshold scheme is not perfect zero-knowledge.
4.7. Security of the Mignotte scheme

Proof. Consider $s$ and $s'$ two distinct secrets and $I \subseteq U$ with $|I| \leq t$, then
\[ \sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} \left| P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I) \right| = 2, \]
which proves our claim. \hfill \Box

Although the Mignotte threshold scheme does not satisfy any of the canonical security properties, some degree of security is provided. The entropy of the secret when $|I| \leq t$ shares are pulled together is roughly
\[ (t + 1 - |I|) \log m_1 \geq \log m_1 \]

Therefore, even considering the massive loss of entropy in the Mignotte threshold scheme based on some sequence of co-primes, the entropy of the secret when revealing at most $t$ shares is comparable (or rather of the same magnitude) with the entropy of the secret in other CRT-based threshold schemes that use the same sequence of co-primes (namely GRS or Asmuth-Bloom).
Chapter 5

CRT-based weighted schemes and their security

5.1 DWTAS ........................................ 124
  5.1.1 The access structure ......................... 124
  5.1.2 DWTAS do not have ideal realizations ....... 126
5.2 DWTSSS ........................................ 128
  5.2.1 Epsilon sequences of co-primes ............... 128
  5.2.2 Distributive weighted threshold scheme ...... 132
5.3 Security issues of DWTSSS ....................... 133
  5.3.1 More on security properties ................. 133
  5.3.2 Asymptotic idealness ......................... 135
  5.3.3 Perfect zero-knowledge ....................... 136

In this chapter we deal with one of the open problems concerning the construction of other CRT-based schemes, that satisfy the security properties of Section 4.2.

In [26] we considered multilevel access structures where each participant has associated a weight and where each participant in an authorized set can be replaced by any number of participants whose weights can compensate the weight of that participant. These new multilevel access structure are introduced via weighted threshold access structures and are called distributive weighted threshold access structures (DWTAS).

Furthermore, we prove there exists sequences of co-primes that satisfy the requirements of DWTAS and proposed a CRT-based secret sharing scheme that realizes such access structures (DWTSSS).

Concerning the security of the DWTSSS, we proved that the scheme is asymptotically perfect and perfect zero-knowledge. As the scheme allows for the share spaces to be arbitrarily large compared to the secret space, the scheme can not be asymptotically ideal.
5.1 DWTAS

In a disjunctive multilevel access structure, DMAS for short (see Section 3.6), the set of participants $U$ is partitioned in $q$ level $U_1, \ldots, U_q$, according to a hierarchy. Meaning, that any participant on level $i$ is less important than any participant from the previous level $i-1$, for all $2 \leq i \leq q$. Furthermore, each level $i$ has assigned a positive threshold $t_i$, such that $0 < t_1 < \cdots < t_q$. Any set $A$ with participants taken from the first $i$ levels, must satisfy $|A| \geq t_i$ for some level $1 \leq i \leq q$.

To understand the motivation of our contribution to weighted threshold access structures, let us consider the following example of DMAS with just two levels $U_1$ and $U_2$ and thresholds $t_1 = 2$ and $t_2 = 4$. Assume that $U_1$ consists of directors, and $U_2$ of senior tellers, of a bank. The choice of these parameters tells that a bank vault can be opened by either any two directors or four senior tellers. According to the definition of a DMAS, the bank vault can also be opened by three senior tellers together with one director, but not by two senior tellers together with one director. This is somewhat contrary to our intuition that, according to the choice of the parameters, one director can be replaced by any two senior tellers.

5.1.1 The access structure

**Definition 5.1.1.** [26] Let $U$ be a non-empty finite set. A *distributive weighted threshold access structure* (DWTAS) over $U$ is a triple $(w, \bar{t}, \Gamma)$, where:

1. $\bar{t} = (t_1, \ldots, t_q) \in \mathbb{Z}^q$ satisfies $0 < t_1 < \cdots < t_q$, where $q \geq 1$;
2. $w : U \rightarrow \mathbb{R}$ is the weight function which enjoys the properties:
   a. $w(x) \in \{1/t_1, \ldots, 1/t_q\}$;
   b. $|\{x \in U | w(x) = 1/t_i\}| \geq t_i$, for any $1 \leq i \leq q$;
3. $\Gamma = \{A \subseteq U | w(A) \geq 1\}$.

The terminology “distributive” is justified by the fact that a DWTAS can be viewed as a multilevel access structure [55], whose authorized sets are “distributed” over levels. Indeed, the set $U$ of participants can be partitioned into levels $U_i = \{x \in U | w(x) = 1/t_i\}$, where $1 \leq i \leq q$. Each level $U_i$ satisfies $1 \leq t_i \leq n_i$, where $n_i$ is the cardinality of $U_i$. Moreover, all participants in $U_i$ have the same weight $1/t_i$.

An authorized set $A \in \Gamma$ of participants may contain participants from any level provided that the sum of the weights of the participants in $A$ exceeds 1. Thus, if $A \subseteq U$ contains at least $t_i$ participants from the level $U_i$, for some $i$, then $A$ is an authorized set (that is, $t_i$ acts as a threshold
for this level. This is the reason we have chosen the global threshold 1 for DWTAS.

**Lemma 5.1.2.** [26] DWTAS are strict extensions\(^1\) of DMAS.

**Proof.** Given a DMAS \((U, t, \Gamma)\), one can construct a DWTAS \((w, t, \Gamma')\) such that \(\Gamma \subseteq \Gamma'\). Indeed, for each participant \(x\) from level \(U_i\) we assign the weight \(w(x) = 1/t_i\). Thus, DWTAS can be viewed as extensions of DMAS.

Moreover, there are DWTAS whose authorized sets cannot be defined by any DMAS. Consider \(U = \{x_1, x_2, y_1, \ldots, y_4\}\) a set of six participants with \(t_1 = 2, t_2 = 4, w(x_1) = w(x_2) = 1/2, \) and \(w(y_1) = \cdots = w(y_4) = 1/4\). These elements define a DWTAS \((w, t, \Gamma)\) for which \(\Gamma\) cannot be defined by any DMAS.

Therefore, DWTAS are strict extensions of DMAS. \(\square\)

**Definition 5.1.3.** [26] Given \(A \subseteq U\), the characteristic vector of \(A\) w.r.t. \((w, t, \Gamma)\) is a vector \(c_A = (c_1, \ldots, c_q)\) which satisfies

\[
 c_i = \left| \{a \in A \mid w(a) = 1/t_i\} \right| ,
\]

for all \(1 \leq i \leq q\).

As \(c_i\) is the number of participants with the same weight \(1/t_i\), let \(w(A) = \sum_{i=1}^{q} c_i/t_i\). Therefore, \(A\) is an authorized set if \(\sum_{i=1}^{q} c_i/t_i \geq 1\), and \(A\) is a minimal authorized set if it is an authorized set and the following relationship holds for all \(j\) with \(c_j > 0\):

\[
 \sum_{i=1, i \neq j}^{q} \frac{c_i}{t_i} + \frac{c_j - 1}{t_j} < 1 .
\]

The following lemma shows that if the participants in a minimal authorized set of a DWTAS are taken from the \(l\)th level up to the \(r\)th level, then the number of participants is at least \(t_l\) and at most \(t_r\).

**Lemma 5.1.4.** [26] Let \((w, t, \Gamma)\) be a DWTAS and \(A\) a minimal authorized set whose characteristic vector is \(c_A = (c_1, \ldots, c_q)\). If there are \(l\) and \(r\) such that

1. \(1 \leq l \leq r \leq q\);
2. \(c_i = 0\) for all \(1 \leq i \leq l - 1\) and \(r + 1 \leq i \leq q\);
3. \(c_l > 0\) and \(c_r > 0\),

then \(t_l \leq \sum_{i=l}^{r} c_i \leq t_r\). Moreover, if \(l < r\) then \(t_l < \sum_{i=l}^{r} c_i \leq t_r\).

**Proof.** Let \(c_A, l,\) and \(r\) be as in the lemma.

**Case 1:** \(l = r\). Then, \(c_l = k_l = k_r\) and the result in the lemma holds true.

---

\(^1\) In the sense that from any DMAS, a DWTAS can be constructed. And, the converse is not necessary true.
5.1. DWTAS

**Case 2:** \( l < r \). Let \( j \) such that \( c_j > 0 \). As \( A \) is minimal, it follows

\[
1 \leq \sum_{i=1}^{q} \frac{c_i}{t_i} \quad \text{and} \quad \sum_{i=1, i \neq j}^{q} \frac{c_i}{t_i} + \frac{c_j - 1}{t_j} < 1.
\]

These lead to the following bounds for \( c_j \):

\[
t_j - \sum_{i=l, i \neq j}^{r} \frac{c_i t_j}{t_i} \leq c_j < t_j + 1 - \sum_{i=l, i \neq j}^{r} \frac{c_i t_j}{t_i}.
\]

As the thresholds are in an increasingly order, we obtain the following lower bound:

\[
\sum_{i=l}^{r} c_i = c_l + \sum_{i=l+1}^{r} c_i \geq t_l + \sum_{i=l+1}^{r} c_i(1 - \frac{t_l}{t_i}) > t_l,
\]

and the following upper bound

\[
\sum_{i=l}^{r} c_i = c_r + \sum_{i=l}^{r-1} c_i < t_r + 1 + \sum_{i=l}^{r-1} c_i(1 - \frac{t_r}{t_i}).
\]

As \( \sum_{i=l}^{r-1} c_i \) is a positive integer, it follows \( t_l < \sum_{i=1}^{r} c_i \leq t_r \).

**5.1.2 DWTAS do not have ideal realizations**

We show in this sections that DWTAS do not have ideal realizations. The main argument is based on a characterization theorem for ideal weighted threshold secret sharing schemes proposed in [4].

**Theorem 5.1.5.** [4] A WTAS \( \Gamma \) over \( U \) is ideal if and only if one of the following three conditions holds:

1. \( \Gamma \) is an DMAS of at most three levels \(^2\);
2. \( \Gamma \) is a TPAS;
3. \( \Gamma \) is a composition of two ideal WTAS defined on sets of participants smaller than \( U \).

Based on this theorem we obtain the following result.

**Theorem 5.1.6.** [26] There are DWTAS that are not ideal.

**Proof.** We show that there are DWTAS that do not satisfy any of the three conditions in Theorem 5.1.5.

**Case 1:** DMAS with at most three levels. Recall from Lemma 5.1.2, that there exists DWTAS for which no DMAS can be constructed. Therefore, given a DWTAS with at least four levels, the authorized sets from each level is described by 4 different thresholds. Whereas, a DMAS with at most three levels is described by less than 4 different thresholds.

\(^2\) See Section 3.6.4 and Lemma 5.1.2).
Chapter 5. CRT-based weighted schemes and their security

Case 2: TPAS. Similarly, the authorized sets of the TPAS are characterized by a global threshold. Whereas, the authorized sets of a DWTAS with at least four levels, take values from smallest threshold up to the largest threshold (note there are 4 thresholds).

Case 3: Composition of two WTAS. We prove that no DWTAS with two or more levels can be decomposed into two WTAS. For the sake of simplicity we consider the case of a DWTAS \((w, t, \Gamma)\) with two levels (that is, \(t = (t_1, t_2)\)) over a set of participants \(U\).

Assume, by contradiction, that \(\Gamma\) can be written as a composition of two WTAS \(\Gamma_1\) and \(\Gamma_2\) via \(u\), where \(\Gamma_1\) is over \(U'\), \(\Gamma_2\) is over \(U''\), \(U' \cap U'' = \emptyset\), \(u \in U'\), and \(|U| = |U'| + |U''| - 1\).

Without loss of generality we may assume that any authorized set \(A \in \Gamma_1\) satisfies \(A - \{u\} \neq \emptyset\) and \(\Gamma_2\) has at least two minimal authorized sets. The assumption on \(\Gamma_2\) leads to the fact that there exist \(B_1, B_2 \in \Gamma_2\) such that \(B_1 - B_2 \neq \emptyset\) and \(B_2 - B_1 \neq \emptyset\).

Claim: All elements of any set \(A \in \Gamma_1\) with \(u \in A\) must be on the same level in \(\Gamma\), and all the elements in \(U''\) must be on the other level in \(\Gamma\).

Proof of Claim: Assume there exists \(A \in \Gamma_1\) with \(u \in A\) such that \((A - \{u\}) \cap U_1 \neq \emptyset\) and \((A - \{u\}) \cap U_2 \neq \emptyset\) (that is, \(A - \{u\}\) overlaps the two levels \(U_1\) and \(U_2\) in \(\Gamma\)). Given \(b \in B_1 - B_2\) for some \(B_1, B_2 \in \Gamma_2\), \(b\) is either on the first level or on the second one in \(\Gamma\) because \((A - \{u\}) \cup B_1 \in \Gamma\). If \(b\) is on the first level, then let \(a \in (A - \{u\}) \cap U_1\). Then, \((A - \{a, u\}) \cup \{b\} \cup B_2\) must be in \(\Gamma\) because \(a\) and \(b\) have the same weight in \(\Gamma\). However, \((A - \{a, u\}) \cup \{b\} \cup B_2\) cannot be obtained by composing \(\Gamma_1\) and \(\Gamma_2\) via \(u\). Similarly, \(b\) cannot be on the second level.

Iterating the above argument for all sets \(A \in \Gamma_1\) with \(u \in A\) we obtain the statement in the Claim.

According to the above claim we assume that all the elements of the sets \(A \in \Gamma_1\) with \(u \in A\) are on the first level and all the elements in \(U''\) are on the second level. Moreover, no element of a set \(a \in A\) with \(A \in \Gamma_1\) and \(u \notin A\) can be on the second level. This follows from the fact that, otherwise, \((A - \{a\}) \cup \{b\}\) is authorized set, for any \(b \in U''\) on the second level. However, this set cannot be obtained by the composition of \(\Gamma_1\) and \(\Gamma_2\) via \(u\) (remark that \(a\) and \(b\) must have the same weight in \(\Gamma\)).

As a conclusion, the second level must contain only elements of \(U''\); this is a contradiction because any level in \(\Gamma\) should contain authorized sets, the second level of \(\Gamma\) contains only elements from \(U''\), and the composition of \(\Gamma_1\) and \(\Gamma_2\) via \(u\) cannot yield authorized sets with elements only from \(U''\). \(\square\)
5.2 DWTSSS

We show in this section that there are CRT-based realizations of distributive weighted threshold access structures. Our approach is based on sequences of pairwise co-prime integers with some special properties. A DWTAS \((w, \tau, \Gamma)\) over a set \(U\) of participants partitions the set \(U\) into levels \(U_i = \{x \in U | w(x) = 1/t_i\}\), \(1 \leq i \leq q\). To each level \(U_i\), we associate a sequence \(L_i\) of pairwise co-prime integers. The secret is shared among the participants on this level by using \(L_i\) in a manner similar to most CRT-based secret sharing schemes [45, 1, 29].

5.2.1 Epsilon sequences of co-primes

**Definition 5.2.1.** [26] Let \(0 < \epsilon \leq 1\) be a real number and \(\tau = (t_1, \ldots, t_q)\) and \(\pi = (n_1, \ldots, n_q)\) be two vectors of positive integers with \(0 < t_1 < \cdots < t_q\) and \(t_i \leq n_i\) for all \(1 \leq i \leq q\). An \((\epsilon, \tau, \pi)\)-sequence is a pair \(\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))\) consisting of a positive integer \(m_0\) and \(q\) sets \(L_1, \ldots, L_q\) of positive integers such that:

1. \(|L_i| = n_i\), for all \(1 \leq i \leq q\);
2. \((m_0, x) = 1\) and \((x, y) = 1\) for any \(x, y \in \bigcup_{i=1}^{q} L_i\) with \(x \neq y\);
3. \(m_0 \cdot \alpha < \beta\), where \(\alpha = \max\{x^{t_i} - \epsilon | 1 \leq i \leq q, x \in L_i\}\) and \(\beta = \min\{x^{t_i} | 1 \leq i \leq q, x \in L_i\}\).

For simplicity, every time we need these sequences, but not the exact value of the co-primes, we call them epsilon sequences of co-primes.

The number \(m_0\) in an \((\epsilon, \tau, \pi)\)-sequence \(\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))\) is called the security parameter of \(\mathcal{L}\) (the terminology is justified by the fact that, as we will see later, \(m_0\) is used to define a secret space).

Let \(m_{i,1} < \cdots < m_{i,n_i}\) denote a total ordering over the elements of \(L_i\). Therefore, the third requirement in Definition 5.2.1 can be rewritten in the form

\[m_0 \cdot \alpha < \beta\], where \(\alpha = \max_{i=1}^{q} \{m_{i,n_i}^{k_{i}-\epsilon}\}\) and \(\beta = \min_{i=1}^{q} \{m_{i,1}^{k_{i}}\}\)+

This notation will be used throughout the thesis from now on.

**Lemma 5.2.2.** [26] For any \((\epsilon, \tau, \pi)\)-sequence \(\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))\), where \(\epsilon, \tau, \pi\) and \(\mathcal{L}\) are as in Definition 5.2.1, the following inequalities hold:

1. \(m_0 < m_{q,1}^{\epsilon} \leq m_{q,1}\);
2. \(m_{q,1} < \cdots < m_{q,n_q} < \cdots < m_{i,1} < \cdots < m_{1,n_1}\).

**Proof.** (1) According to Definition 5.2.1 it follows that \(m_0 m_{q,n_q}^{t_i-\epsilon} < m_{q,1}^{t_i}\) and, therefore, \(m_0 < m_{q,1}^{\epsilon}\). As \(0 < \epsilon \leq 1\), we also have \(m_{q,1}^{\epsilon} \leq m_{q,1}\).

(2) For simplicity we prove that \(m_{i,n_i} < m_{i-1,1}\), for all \(2 \leq i \leq q\). Again, from Definition 5.2.1 it follows \(m_{i,n_i}^{t_i-\epsilon} < m_{i-1,1}^{t_{i-1} - \epsilon}\). As \(t_{i-1} \leq k_i - \epsilon\) for any \(0 < \epsilon \leq 1\), we obtain \(m_{i-1,1}^{t_{i-1} - \epsilon} \leq m_{i-1,1}^{k_i - \epsilon}\) and, therefore, \(m_{i,n_i} < m_{i-1,1}\). \(\square\)
The following theorem deals with the existence of sequences of co-primes that satisfy the requirements of Definition 5.2.1.

**Theorem 5.2.3.** [26] There are \((\epsilon, \ell, \pi)\)-sequences with arbitrarily large security parameters, for any \(\epsilon, \ell\), and \(\pi\) as in Definition 5.2.1.

**Proof.** Let \(\epsilon, \ell, \) and \(\pi\) be as in Definition 5.2.1, and \(m_0\) a security parameter.

Recall first [53] that the infinite sequence of prime numbers \(p_1, p_2, \ldots\) satisfies the following property

\[
\lim_{i \to \infty} \frac{p_{i+1} - p_i}{p_i} = 0
\]

This shows that for any \(\delta > 0\) there exists \(i_0\) such that

\[
p_{i+1} < (1 + \delta)p_i,
\]

for any \(i \geq i_0\). Therefore, \(p_{i+j} < (1 + \delta)^j p_i\), for any \(i \geq i_0\) and \(j \geq 1\).

The proof of the theorem follows 3 steps. The case of a singular level \((q = 1)\) and the case of a two level access structure \(q = 2\), are used as building blocks for the general case.

**Case 1:** For \(q = 1\), we prove that there are large enough primes such that any \(n_1\) consecutive primes can satisfy the following constraint:

\[
m_0 \cdot \alpha < \beta\]

with \(\alpha = p_{i+n_1-1}^{t-\epsilon}\) and \(\beta = p_i^{t}\).

Given a real number \(\delta > 0\), there exists \(i_0\) such that

\[
p_{i+j} < (1 + \delta)^{j} p_i\quad \text{and} \quad p_i > (m_0(1 + \delta)^{(n_1-1)(t-\epsilon)})^{1/\epsilon},
\]

for any \(i \geq i_0\) and \(j \geq 1\). Then, one can easily obtain the third requirement of Definition 5.2.1 for any \(i \geq i_0\):

\[
m_0 p_{i+n_1-1}^{t-\epsilon} < m_0 (1 + \delta)^{(n_1-1)(t-\epsilon)} p_i^{t} p_i^{t-\epsilon} < p_i^{t} p_i^{t-\epsilon} = p_i^{t}.
\]

Therefore, the sequence \(p_i < \ldots < p_{i+n_1-1}\) of consecutive primes together with \(m_0\) form an \((\epsilon, \ell, \pi)\)-sequence.

**Case 2:** Consider now the case \(q = 2\). We show that there are two sequences of consecutive primes

\[
L_2: \quad p_i < \cdots < p_{i+n_2-1} \quad \text{and} \quad L_1: \quad p_{i+j} < \cdots < p_{i+j+n_1-1}
\]

where \(j \geq n_2\), such that \((m_0, (L_1, L_2))\) is an \((\epsilon, \ell, \pi)\)-sequence.

That is, \(L_1\) and \(L_2\) must fulfill the following inequalities:

\[
m_0 p_{i+n_2-1}^{t_2-\epsilon} < p_i^{t_2}\]

\[
m_0 p_{i+n_2-1}^{t_2-\epsilon} < p_{i+j}^{t_1} \quad \text{(5.3)}
\]

\[
m_0 p_{i+j+n_1-1}^{t_1-\epsilon} < p_i^{t_2}\]

\[
m_0 p_{i+j+n_1-1}^{t_1-\epsilon} < p_{i+j}^{t_1}\] (5.5)
5.2. DWTSSS

Using the same reasoning as the one given in the previous case, that there are infinitely many prime numbers, for any real number \( \delta > 0 \) there exists \( i \) such that
\[
p_i > \max\{(m_0(1 + \delta)^{(n_2-1)(t_2-\epsilon)})^{1/\epsilon}, (m_0(1 + \delta)^{n_1(t_1-\epsilon)}t_1/(ct_2))\}
\]
(5.6)

Next, we establish that for any sequence \( L_2 \) (given by \( p_i \)), there exists at least one sequence \( L_1 \) (given by \( p_{i+j} \)) such that the inequalities (5.2)-(5.5) are satisfied.

**Claim 5.2.4.** Given a real number \( \delta > 0 \) and a positive integer \( i \) which satisfies the inequality (5.6), there exists \( j \) such that
\[
p_i^{k_2/k_1} < p_{i+j} < m_0^{-1/(k_1-\epsilon)}(1 + \delta)^{-(n_1-1)p_i^{k_2/(k_1-\epsilon)}}
\]
(5.7)

**Proof.** Let \( s \) be the largest positive integer such that \( p_s < p_i^{k_2/k_1} < p_{s+1} \).

We prove that \( p_{s+1} < m_0^{-1/(k_1-\epsilon)}(1 + \delta)^{-(n_1-1)p_i^{k_2/(k_1-\epsilon)}} \).
We have:
\[
p_{s+1} < (1 + \delta)p_s < (1 + \delta)p_i^{t_2/t_1} < m_0^{-1/(t_1-\epsilon)}(1 + \delta)^{-(n_1-1)p_i^{t_2/(t_1-\epsilon)}}
\]
The first inequality follows from (5.1), the second inequality from the choice of \( s \), and the third one from the fact that \( p_i > (m_0(1 + \delta)^{n_1(t_1-\epsilon)}t_1/(ct_2)) \).

As \( t_2/t_1 > 1 \), \( s + 1 \) must be of the form \( s + 1 = i + j \) for some \( j \geq 1 \).

Given the positive integers \( i \) and \( j \) as in Claim 5.2.4, we prove that the inequalities (5.2)-(5.5) are satisfied for any \( \delta > 0 \).

For the inequality (5.2) we use (5.1) and (5.6) and obtain:
\[
m_0p_{i+n_2-1}^{t_2-\epsilon} < m_0(1 + \delta)^{(n_2-1)(t_2-\epsilon)}p_i^{t_2-\epsilon} < p_i^{t_2-\epsilon} = p_i^{t_2}.
\]
To prove the inequality (5.3) we use (5.2) and (5.7):
\[
m_0p_{i+n_2-1}^{t_2-\epsilon} < p_i^{t_2} < p_{i+j}^{t_1}.
\]
Remark that the inequality (5.3) implies \( j \geq n_2 \) as \( t_1 \leq t_2 - \epsilon \).

The inequality (5.4) can be obtained from (5.1) and (5.7):
\[
m_0p_{i+j+n_1-1}^{k_2-\epsilon} < m_0(1 + \delta)^{(n_1-1)(k_2-\epsilon)}p_{i+j}^{k_2-\epsilon} < p_{i+j}^{k_2}
\]
Finally, (5.4) and (5.7) lead to the inequality (5.5):
\[
m_0p_{i+j+n_1-1}^{k_2-\epsilon} < p_{i+j}^{k_2} < p_{i+j}^{k_1-\epsilon}
\]

**Case 3:** For the general case we show that there are \( q \) sequences of consecutive primes
\[
L_q: \quad p_i < \cdots < p_{i+n_q-1}
\]
\[
L_{q-1}: \quad p_{i+j_1} < \cdots < p_{i+j_1+n_{q-1}-1}
\]
\[
\cdots
\]
\[
L_1: \quad p_{i+j_{q-1}} < \cdots < p_{i+j_{q-1}+n_1-1}
\]

130
where \( j_1 > n_q - 1, j_2 > j_1 + n_q - 1, \ldots, j_{q-1} > j_{q-2} + n_2 - 1 \), such that
\[
m_0 p_{i+ j_l + n_q - l - 1} > p_i < p_{i+j_r}
\] (5.8)
for all \( 0 \leq l \leq q - 1 \) and \( 0 \leq r \leq q - 1 \), where \( j_0 = 0 \).

Remark that (5.8) is a parameterized inequality, comprising \( q^2 \) inequalities, each of them being obtained by assigning values to \( l \) and \( r \).

Following the same line as in the case \( q = 2 \), we can easily show that for any \( \delta > 0 \) there exists \( i \) such that
\[
p_i > \max_{l=1}^{q-1} \left( m_0 (1 + \delta)^{(n_q - l - 1)/(t_q - \epsilon)} (m_0 (1 + \delta)^{n_l/(t_l - \epsilon)} t_l / (t_q - \epsilon)) \right)
\] (5.9)
Now, for each \( i \) which satisfies (5.9) and each \( 1 \leq l \leq q - 1 \), there exists \( j_l \) such that
\[
p_i^{t_q/t_l} < p_{i+j_l} < m_0^{1/(t_l - \epsilon)} (1 + \delta)^{n_l / (t_l - \epsilon)} p_i^{t_q / (t_l - \epsilon)}
\] (5.10)
(this is a generalization of Claim 5.2.4).

In the same way as we did in the case \( q = 2 \), one can easily prove that, given \( \delta > 0 \), any positive integers \( i, j_1, \ldots, j_{q-1} \) which satisfy the inequalities (5.9) and (5.10) will also satisfy the inequalities (5.8). Moreover, \( j_l > j_{l-1} + n_q - l + 1 - 1 \), for all \( 1 \leq l \leq q - 1 \) (recall that \( j_0 = 0 \)).

The proof of Theorem 5.2.3 suggests the following construction for Algorithm 7 to generate \((\epsilon, \bar{t}, \overline{n})\)-sequences. Furthermore, note that the smaller \( \delta \) is, the smaller \( i, j_1, \ldots, j_{q-1} \) are.

<table>
<thead>
<tr>
<th>input</th>
<th>the values ( 0 &lt; \epsilon \leq 1, \bar{t} ) and ( \overline{n} );</th>
</tr>
</thead>
<tbody>
<tr>
<td>output:</td>
<td>an ((\epsilon, \bar{t}, \overline{n}))-sequence;</td>
</tr>
<tr>
<td>begin</td>
<td>choose a security parameter ( m_0 );</td>
</tr>
<tr>
<td>choose</td>
<td>a real number ( \delta &gt; 0 ) (( \delta ) may be less than 1);</td>
</tr>
<tr>
<td>find</td>
<td>( i ) such that the inequalities (5.9) hold w.r.t. ( \delta );</td>
</tr>
<tr>
<td>find</td>
<td>( j_1, \ldots, j_{q-1} ) such that the inequalities (5.10) hold w.r.t. ( \delta ) and ( i );</td>
</tr>
<tr>
<td>output:</td>
<td>( t )</td>
</tr>
<tr>
<td>the ((\epsilon, \bar{t}, \overline{n}))-sequence ((m_0, (L_i \mid 1 \leq i \leq q))), where</td>
<td></td>
</tr>
<tr>
<td>( (\forall 0 \leq l \leq q - 1)(L_{q-l} : p_{i+j_l} &lt; \cdots &lt; p_{i+j_l+n_q-l}) )</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
</tbody>
</table>

**Algorithm 7**: Computing an \((\epsilon, \bar{t}, \overline{n})\)-sequence
5.2.2 Distributive weighted threshold scheme

Given the results established in Theorem 5.2.3, we show now that there are realizations of any DWTAS. A CRT-based distributive weighted threshold secret sharing scheme (DWTSSS) for a DWTAS \((w, \overline{t}, \Gamma)\) over a set \(U\) of participants first choose \(\epsilon > 0\) such that:

\[
\epsilon < (1 - \max\{w(A) - 1/t_i | A \text{ minimal } \wedge (\exists a \in A)(w(a) = 1/t_i)\}) \cdot t_1.
\]

Note that the right hand side of the above inequality is less than or equal to 1 and the equality hold only when \(q = 1\).

In [26], we have proposed the following scheme:

**DWTSSS**

**Parameter setup**
- choose an \((\epsilon, \overline{t}, \overline{\pi})\)-sequence \(L = (m_0, (L_i | 1 \leq i \leq q))\), where \(|L_i| = n_i\) for all \(1 \leq i \leq q\) (\(L\) will be called an \((\epsilon, \overline{t}, \overline{\pi})\)-sequence associated to \((w, \overline{t}, \Gamma)\)).
- The integers \(\overline{t}, \overline{\pi}, m_0, m_1, \ldots, m_q, n_q\) are public parameters;
- define the secret space as \(\mathbb{Z}_{m_0}\) and the share space of the \(j\)th participant on the \(i\)th level as \(\mathbb{Z}_{m_{i,j}}\), for all \(1 \leq i \leq q\) and all \(1 \leq j \leq n_i\).
- For simplicity, let \((i, j)\) denote the \(j\)th participant on the \(i\)th level;
- given a secret \(s\), generate a random \(r\) such that \(s' = s + rm_0 < \beta\) is computed (Recall that \(\beta = \min_{i=1}^{q}\{m_{i,1}^i\}\)).
- Share \(s\), by \(s_{i,j} = s' \mod m_{i,j}\) for all \(1 \leq i \leq q\) and all \(1 \leq j \leq n_i\);

**Secret reconstruction**
- any set \(A\) of participants with \(w(A) \geq 1\) can uniquely reconstruct the secret by computing first the unique solution modulo \(\prod_{(i,j) \in A} m_{i,j}\) of the system

\[
x \equiv s_{i,j} \mod m_{i,j}, \quad \forall (i, j) \in A.
\]

and then reducing it modulo \(m_0\).

Given the secret sharing scheme described above, the following lemma establishes the correctness of the recovery process. Namely, it shows that any authorized access structure can uniquely recover the secret. As with respect to unauthorized access structures, the next section provides full details regarding the security of the scheme.

**Lemma 5.2.5.** [26] Given the DWTSSS described as above, let \(A\) be a minimal authorized set whose characteristic vector is \(c_A = (c_1, \ldots, c_q)\). Then, for any \(1 \leq j \leq q\) with \(c_j > 0\), there exists \(0 < \theta_j < 1\) such that

\[
(\prod_{i \neq j} m_{i,n_i}^{c_i}) \cdot m_{j,n_j}^{c_j - 1} \leq \alpha^{\theta_j} < \alpha < \beta \leq \prod_{i=1}^{q} m_{i,1}^{c_i}.
\]
Chapter 5. CRT-based weighted schemes and their security

Proof. Let $A$ be a minimal authorized set, $c_A = (c_1, \ldots, c_q)$, and let $j$ such that $c_j > 0$. Then, $w(A) \geq 1$ and $w(A) - 1/t_j < 1$.

We prove that $\beta \leq \prod_{i=1}^{q} m_{t_i,1}$. As $\beta = \min_{t_i} m_{t_i,1}$, for simplicity let $\beta = m_{t_r,1}$ for some $1 \leq r \leq q$. From $m_{t_r,1} < m_{t_i,1}$, it follows $m_{t_r,1}^{c_i(t_i/t_r)} \leq m_{t_i,1}^{c_i}$, for all $i \neq r$. Combining all these inequalities we obtain

$$\beta = m_{t_r,1}^{c_r} \leq \prod_{i=1}^{q} m_{t_i,1}^{c_i}.$$  

(Recall that $\sum_{i=1}^{q} (c_i/t_i) \geq 1$.)

In order to prove the other inequalities, let $\alpha = m_{t_s,t_s}^{c_s}$ for some $1 \leq s \leq q$.

Similarly, from $m_{t_s,t_s}^{c_s} > m_{t_i,t_i}^{c_i}$ it follows $m_{t_s,t_s}^{c_s/(t_s-t_i)} \geq m_{t_i,t_i}^{c_i}$, for all $i \neq s$.

Combining all these inequalities we obtain:

$$\left( \prod_{i \neq j} m_{t_i,t_i}^{c_i} \right) \cdot m_{t_j,t_j}^{c_j-1} \leq m_{t_s,t_s}^{c_s/(t_s-t_i)}.$$  

As $\epsilon < (w(A) - 1/t_j)$, we have $\frac{t_i}{t_i-\epsilon} (w(A) - 1/t_j) < 1$. Combining this with $\frac{t_i}{t_i-\epsilon} < \frac{t_i}{t_i-\epsilon}$ for all $i > 1$, we obtain

$$\sum_{i \neq j} c_i \frac{1}{t_i-\epsilon} + (c_j-1) \frac{1}{t_j-\epsilon} = \sum_{i \neq j} c_i \frac{t_i}{t_i-\epsilon} + \frac{c_j-1}{t_j-\epsilon} \leq \frac{t_i}{t_i-\epsilon} (\sum_{i \neq j} c_i \frac{1}{t_i}) = \frac{t_i}{t_i-\epsilon} (w(A) - 1/t_j) < 1.$$  

Let $\theta_j = \sum_{i \neq j} c_i \frac{1}{t_i-\epsilon} + (c_j-1) \frac{1}{t_j-\epsilon}$. Therefore, $\prod_{i \neq j} m_{t_i,t_i}^{c_i} \cdot m_{t_j,t_j}^{c_j-1} \leq \alpha^{\theta_j}$, which concludes the proof of the lemma. \hfill $\square$

5.3 Security issues of DWTSSS

The security of the CRT-based schemes was studied using the concepts of asymptotic perfectness, asymptotic idealness, and perfect zero-knowledge. In this section, we first adapt the definitions involved to account for epsilon sequences of co-primes. Then, we prove the proposed DWTSSS is asymptotically perfect and perfect zero-knowledge.

5.3.1 More on security properties

Consider $L = (m_0, (L_i \mid 1 \leq i \leq q))$ an $(\epsilon, \bar{\bar{\ell}}, \bar{\bar{\pi}})$-sequence associated to the $(w, \bar{\bar{\ell}}, \bar{\bar{\Gamma}})$-DWTSSS and $I \subseteq \{(i,j) \mid 1 \leq i \leq q$ and $1 \leq j \leq n_i\}$ a non-empty set. Let $X$ and $Y_I$ be two random variables. The first one takes values into the secret space $\mathbb{Z}_{m_0}$, while the second one into $\prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}}$.

Definitions 4.2.2, 4.2.3 and 4.2.8 also hold true for $(\epsilon, \bar{\bar{\ell}}, \bar{\bar{\pi}})$-sequences.
5.3. Security issues of DWTSSS

Definition 5.3.1. [26] Let $U$ be a finite set of participants. A distributive weighted threshold secret sharing scheme for a DWTAS $(w, t, \Gamma)$ over a set $U$ of participants is called asymptotically perfect if for any $\lambda \in (0, 1)$ there exists $m \geq 0$ such that any $(\epsilon, t, \pi)$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ associated to $(w, t, \Gamma)$ with $m_0 \geq m$ satisfies the following properties:

- $H(X) \neq 0$;
- $|\Delta(y_I)| < \lambda$, for any unauthorized set $I$ and any $y_I \in \prod_{(i,j) \in I} Z_{m_{i,j}}$.

Definition 5.3.2. [26] Let $U$ be a finite set of participants. The distributive weighted threshold secret sharing scheme for a DWTAS $(w, t, \Gamma)$ over a set $U$ of participants is called asymptotically ideal if it is asymptotic perfect and for any $\lambda \in (0, 1)$ there exists $m \geq 0$ such that any $(\epsilon, t, n)$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ associated to $(w, t, \Gamma)$ with $m_0 \geq m$ satisfies

$$\frac{|Z_{m_{i,j}}|}{|Z_{m_0}|} \leq 1 + \lambda,$$

for any $1 \leq i \leq q$ and $1 \leq j \leq n_i$ ($|Z_{m_{i,j}}|/|Z_{m_0}|$ is the information rate of the $j$th participant on the $i$th level).

Given a secret $s \in Z_{m_0}$ consider the random variable $Y_{s,I}$ which takes values $y_I \in \prod_{(i,j) \in I} Z_{m_{i,j}}$ as possible shares for all $(i,j) \in I$ in the same process of sharing $s$.

Definition 5.3.3. [26] The distributive weighted threshold secret sharing scheme for a DWTAS $(w, t, \Gamma)$ over a set $U$ of participants is called perfect zero-knowledge if for any polynomial $\text{poly}$ there exists $m \geq 0$ such that for any $(\epsilon, t, n)$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ associated to $(w, t, \Gamma)$ with $m_0 \geq m$, any secrets $s, s' \in Z_{m_0}$, and any unauthorized set $I$, the following holds:

$$\sum_{y_I \in \prod_{(i,j) \in I} Z_{m_{i,j}}} |P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I)| \leq \frac{1}{\text{poly}(m_0)}$$

The following result is a straightforward adaptation of Lemma 4.2.4 or Corollary 4.2.5.

Corollary 5.3.4. [26] The loss of entropy of the DWTSSS based on an $(\epsilon, t, \pi)$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$, and under a uniform distribution over the secret space satisfies the same relations as those in Lemma 4.2.4 for

$$C(I) = \min_{1 \leq i \leq q} \left\lfloor \frac{m_{i,j}^k}{\prod_{(i,j) \in I} m_{i,j}} \right\rfloor,$$

for any $I \subseteq \{(i,j) | 1 \leq i \leq q$ and $1 \leq j \leq n_i \}$. 

134
5.3.2 Asymptotic idealness

**Theorem 5.3.5.** [26] Let $U$ be a finite set of participants. The $(w, l, \Gamma)$-DWTSSS over a set $U$ is asymptotically perfect with respect to the uniform distribution over the secret space.

**Proof.** Let $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ be an $(\epsilon, l, n)$-sequence associated to a DWTAS $(w, l, \Gamma)$ over a set $U$ of participants. Let $\alpha = \max_{i=1}^{q} m_i^{l_i-\epsilon}$ and $\beta = \min_{i=1}^{q} m_i^{l_i}$ as in Definition 5.1.1.

If $I$ is an unauthorized set, then $C(I) \neq 0$. Using that $x - 1 < \lfloor x \rfloor \leq x$ and $C(I) = \lfloor \beta / M_I \rfloor$, where $M_I = \prod_{(i,j) \in I} m_{i,j}$, we have:

$$\log \frac{m_0 \left( \frac{C(I) + 1}{m_0} \right) + 1}{C(I)} < \log \frac{C(I) + m_0 + 1}{C(I)} \leq \log \frac{\beta + m_0 M_I + M_I}{\beta - M_I} = \log \frac{1 + m_0 M_I / \beta + M_I / \beta}{1 - M_I / \beta}$$

As $m_0 \alpha < \beta$ and $M_I \leq \alpha^\theta$ for some $\theta < 1$ (by Corollary 5.3.4), we obtain:

$$\frac{m_0 M_I}{\beta} \leq \frac{m_0^\theta}{\beta} \leq \frac{m_0^{1-\theta}}{\beta^{1-\theta}} = \left( \frac{m_0}{\beta} \right)^{1-\theta} < \left( \frac{1}{\alpha} \right)^{1-\theta}$$

The last term of this sequence of inequalities goes to 0 as $m_0$ goes to infinity (remark that $1 - \theta$ is a fixed quantity). Therefore, $\frac{m_0 M_I}{\beta}$ goes to 0 as $m_0$ goes to infinity. This proves that $M_I / \beta$ goes to 0 too as $m_0$ goes to infinity. Putting all together, Corollary 5.3.4 shows that $\Delta(y_I)$ goes to 0 as $m_0$ goes to infinity. \qed

Recall from Theorem 5.1.6 that DWTAS, in general, does not admit ideal realizations. Regarding the asymptotic idealness, from the proof of Theorem 5.2.3 one can see that $m_{i,j}$ can be arbitrarily large in comparison with $m_0$. Furthermore, using Lemma 5.2.2 we can establish a lower bound for the information rate. Namely, it follows that $m_0 < m_{i,j}$, for any $1 \leq i \leq q$ and $1 \leq j \leq n_i$. Therefore,

$$\frac{|Z_{m_{i,j}}|}{|Z_{m_0}|} > m_0^{1/\epsilon - 1},$$

for any $i$ and $j$ (recall that $\epsilon < 1$ in the definition of the distributive weighted threshold secret sharing scheme).

In conclusion the $(w, l, \Gamma)$-DWTSSS over a set $U$ cannot be asymptotically ideal.
5.3. Security issues of DWTSSS

5.3.3 Perfect zero-knowledge

**Theorem 5.3.6.** [26] Let \( U \) be a finite set of participants. The \((\alpha, \varepsilon, \Gamma)\)-DWTSSS over a set \( U \) is perfect zero-knowledge with respect to the uniform distribution over the secret space.

**Proof.** Let \( \mathcal{L} = (m_0, (L_i \mid 1 \leq i \leq q)) \) be an \((\varepsilon, \Gamma, \pi)\)-sequence associated to \((\vec{y}, \vec{w}, \Gamma)\), and let \( \alpha = \max_{i=1}^{q} m_{i}^{k_i-i} \) and \( \beta = \min_{i=1}^{q} m_{i}^{k_i} \). Consider further an unauthorized set \( I \), and \( s \) and \( s' \) two secrets from the space \( \mathbb{Z}_{m_0} \).

If \( U_I \) is an uniform random variable on the space \( \prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}} \), then:

\[
\left| P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I) \right| \leq \left| P(Y_{s,I} = y_I) - P(U_I = y_I) \right| + \left| P(Y_{s',I} = y_I) - P(U_I = y_I) \right|
\]

In order to prove the theorem, it is sufficient to look for a suitable upper bound for the term

\[
\sum_{y_I \in \prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}}} \left| P(Y_{s,I} = y_I) - P(U_I = y_I) \right|.
\]

For simplicity, let \( M_I = \prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}} \). There exists an isomorphism \( h \) from \( \prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}} \) to \( \mathbb{Z}_{M_I} \), so let \( Z_I \) denote a new variable such that \( U_I \) takes the value \( y_I \) with probability \( p \) if and only if \( Z_I \) takes the value \( h(y_I) \) with probability \( p \). Given the property that for any \( y_I \in \prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}} \) there exists a unique \( r \in \mathbb{Z}_{M_I} \) such that \( y_{i,j} = (s + r \cdot m_0) \mod m_{i,j} \) for all \((i,j) \in I\), let \( R_S \) denote a random variable with values in \( \mathbb{Z}_{\beta} \) such that

\[
\sum_{y_I \in \prod_{(i,j) \in I} \mathbb{Z}_{m_{i,j}}} \left| P(Y_{s,I} = y_I) - P(U_I = y_I) \right| = \sum_{r \in \mathbb{Z}_{M_I}} \left| P(R_S \mod M_I = r) - P(Z_I = r) \right|
\]

If \( 0 \leq r < (\beta \mod M_I) \), then

\[
P(R_S \mod M_I = r) = \frac{\beta - (\beta \mod M_I)}{M_I} + 1
\]

and if \((\beta \mod M_I) \leq r < M_I \) then

\[
P(R_S \mod M_I = r) = \frac{\beta - (\beta \mod M_I)}{\beta M_I}
\]

Combining these with \( P(Z_I = r) = 1/M_I \), we obtain

\[
\sum_{r \in \mathbb{Z}_{M_I}} \left| P(R_S \mod M_I = r) - P(Z_I = r) \right| = 2 \left( \frac{M_I \mod M_I}{M_I} - \frac{(M_I \mod M_I)^2}{M_IM_I} \right)
\]

As \( w(A) < 1 \), we have \( M_I < \alpha \). Combining with \( m_0 \alpha < \beta \) the result of the theorem easily follows. □
Chapter 6

Conclusion and Future work

As we have noticed the CRT-based threshold schemes proposed so far (Chapter 4): the Asmuth-Bloom scheme [1], the Mignotte scheme [45], the GRS scheme [29], are not perfect or ideal, but they ensure some level of security. Quisquater et al. have introduced in [51] two appropriate concepts, \textit{asymptotic perfectness} and \textit{asymptotic idealness}, to be used in order to evaluate the security of such schemes. Thus, they showed that the GRS threshold scheme [29] is asymptotically ideal (and, therefore, asymptotically perfect) and perfect zero-knowledge if the scheme is based on sequences of consecutive primes and the secret is uniformly chosen from the secret space. That is, the GRS threshold scheme becomes more and more secure (from both an information and complexity theoretic point of view) once the first element of the sequence of consecutive primes on which the scheme is defined becomes larger and larger.

The authors of GRS scheme [29], studying the security of their threshold scheme, advised to use sequences of primes of the “same magnitude” in order to get better security (the term “same magnitude” was not defined in [29]). If the primes are consecutive and large enough, as it was used in [51], they may be considered of the same magnitude. However, “same magnitude” should mean more than “consecutive primes”.

Starting from this remark, the main aim of this thesis was to define in a proper way the concept “same magnitude” and to study the security of the threshold schemes in [1, 45, 29] when they are based on sequences of co-primes of the same magnitude. In [3] we defined a sequence of co-primes of the same magnitude by the fact that its elements are taken from an interval of the form \((x, x+x^\theta)\) for some positive integer \(x\) and real number \(\theta \in (0, 1)\). Later, in [21, 27] we have extended the interval to \((kx-x^\theta, kx+x^\theta)\) for some positive integers \(x, k\) and real number \(\theta \in (0, 1)\). Such sequences were called in our thesis \((k-)\text{compact sequences of co-primes}\). We proved that

\begin{itemize}
  \item sequences of consecutive primes or consecutive co-primes are particular cases of \((k-)\text{compact sequences of co-primes};\)
  \item we can find arbitrarily long \((k-)\text{compact sequences of arbitrarily large co-primes, and}\)
\end{itemize}
– any sequence of consecutive primes in an interval covers a denser sequences of co-primes in the same interval.

Regarding the security properties of the GRS scheme and Asmuth-Bloom, we have shown there exists a necessary and sufficient condition concerning the asymptotic idealness if and only if (1-)compact sequences of co-primes are considered. We believe our results close completely the security problems for the GRS scheme and the Asmuth-Bloom scheme. Furthermore, we proved that the GRS scheme and Asmuth-Bloom scheme based on k-compact sequences of co-primes are asymptotically perfect and perfect zero-knowledge.

As with respect to the Mignotte secret sharing scheme, even if this scheme uses (k-)compact sequences of co-primes its loss of entropy cannot be bounded from above, its information rate converges to 0, and it is not perfect zero-knowledge.

Concerning the construction of other CRT-based schemes, we proposed a realization of distributive weighted threshold access structures and we have shown that this realization is asymptotically perfect and perfect zero-knowledge. As with respect to asymptotic idealness, we proved that distributive weighted access structures do not generally have ideal realizations. Therefore, from this point of view, we may say that our scheme is all that can be achieved using CRT. In case of just one level, our CRT based realization of the distributive weighted threshold access structures can be viewed as an asymptotically perfect and perfect zero-knowledge variation of the Asmuth-Bloom secret sharing scheme.

From our thesis we identify the following future direction of research:

**Open problem (OP5’)** aimed at the construction of other CRT-based schemes that satisfy the security properties in [51], that may or may not take into consideration the mobility of the element which defines the secret space compared to the rest of the elements that define the share spaces.

**Open problem (OP6)** focuses on the comparison between **compact sequences** and **epsilon sequences with one level**. We believe that compact sequences are included in epilon sequences with one level. Furthermore, epsilon sequences with one level may be used to design CRT-based secret sharing schemes that satisfy the asymptotic perfectness property or perfect zero-knowledge property.

**Open problem (OP7)** deals with the difference between perfectness and asymptotic perfectness ensured by (1-)compact sequences of co-primes. We believe, the loss of entropy for the GRS scheme and the Asmuth-Bloom scheme based on (1-)compact sequences of co-primes is insignificantly small (without using very large co-primes).
List of Published and Submitted Papers

My personal contributions to this thesis have led to the following papers:

Papers already published or accepted for publication [25, 3, 21, 27]:


3. F.L. Țiplea, C.C. Drăgan. A Necessary and Sufficient Condition for the Asymptotic Idealness of the GRS Threshold Secret Sharing Scheme. Information Processing Letters (accepted with minor modifications)


Papers submitted for review[26]:

Bibliography


