Alexandru Ioan Cuza University of Iaşi, Romania
Faculty of Computer Science

PhD thesis summary

# Security of CRT-based Secret Sharing Schemes

*Supervisor:*
Prof. Dr. Ferucio Laurenţiu **ŢIPLEA**

*Author:*
Constantin Cătălin **DRĂGAN**

August 2013

**Constantin-Cătălin Drăgan**
Faculty of Computer Science
Alexandru Ioan Cuza University of Iaşi
Iaşi, Romania
email: constantin.dragan@infoiasi.ro

**PhD commission**

Prof. Dr. Dorel Lucanu, Chairman
(Alexandru Ioan Cuza University of Iaşi)
Prof. Dr. Ferucio Laurenţiu Ţiplea, Supervisor
(Alexandru Ioan Cuza University of Iaşi)
Prof. Dr. Constantin Popescu
(University of Oradea)
Prof. Dr. Eng. Alin Suciu
(Technical University of Cluj-Napoca)
Prof. Dr. Cristian Masalagiu
(Alexandru Ioan Cuza University of Iaşi)

## List of Published and Submitted Papers

My personal contributions to this thesis have led to the following papers:

Papers already published [13, 3, 11, 15]:

1. **C.C. Drăgan**. Interactive Secret Share Management. In Eduardo Fernández-Medina, Manu Malek and Javier Hernando, editors, *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2009)*, pages 266–269, 2009.

2. M. Barzu, F.L. Ţiplea, **C.C. Drăgan**. Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes. *Information Sciences*, 240: 161–172, 2013.

3. F.L. Ţiplea, **C.C. Drăgan**. A Necessary and Sufficient Condition for the Asymptotic Idealness of the GRS Threshold Secret Sharing Scheme. *Information Processing Letters* (to appear)

4. **C.C. Drăgan**, F.L. Ţiplea. On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme. *Designs, Codes and Cryptography* (to appear)

Papers submitted [14]:

5. **C.C. Drăgan**, F.L. Ţiplea. Distributive Weighted Threshold Secret Sharing Schemes. *Information Sciences* (submitted on April 2013.)

# Contents

# Chapter 1

# Introduction

*A secret sharing scheme* is a method of partitioning a master secret among some participants by providing each participant with a share of the secret such that any *authorized set* of participants can uniquely reconstruct the secret by pulling together their shares. Furthermore, any secret sharing scheme should satisfy some *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 contain any partial information on the secret.

A novel category of threshold secret sharing schemes based on the Chinese Remainder Theorem (CRT) have independently been proposed by Asmuth and Bloom [1] and Mignotte [25], and later by Goldreich, Ron and Sudan [16] (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 threshold secret sharing schemes in [1, 25] 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 [16] 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 [29] have introduced two modern concepts: *asymptotic perfectness* and *asymptotic idealness*. Then, they proved that the threshold scheme in [16] 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 [16] satisfies the perfect zero-knowledge property for consecutive primes.

The results obtained in [29] 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 [29] 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 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 [29].

**Acknowledgements**

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

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

# Chapter 2

# Preliminaries

In this chapter we deal with the introduction of the most basic concepts used throught our thesis. The main directions are *sets*, *number theory* and *information theory*. In the first section we give a brief introduction to sets. Regarding number theory, in the second section we give a detailed overview of the following concepts: divisibility of integers, prime numbers, greatest common divisor, the euclidean algorithm, congruences and complexity. A special attention is given to the Chinese remainder theorem and algorithm. In the last section we concentrate on the definitions and properties of the concepts of probability and entropy.

# Chapter 3

# Secret Sharing Schemes

This chapter is mainly devoted to a formal introduction to secret sharing schemes.

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.

Security concepts associated to secret sharing schemes are discussed using

- the probabilistic approach, due to Brickell and Stinson [8] (later refined by Stinson in [35, 34]). It considers any scheme as a set of distribution rules, where a rule is a method through which a secret is shared.

- the information theoretic approach, due to Karmin et al. [22] and Kothari [24] (later refined by Capocelli et al. [9]). It views secret sharing schemes as a collection of random variables for which the recovery of the secret is measured by entropy.

Then, we shows that there are perfect realizations of access structures, while the next section focuses on ideal schemes. The

chapter ends by a classification of secret sharing schemes, where some of the types of secret sharing schemes consider in our thesis are:

**Weighted threshold secret sharing schemes** [31, 26, 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 [31] who also suggested a realization of it by using tuples of polynomial values associated to each participant.

**Multilevel secret sharing schemes** [32, 36, 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* [32] (DMAS, for short), where the set of participants satisfy the threshold *at some level* $i$, and *conjunctive multilevel schemes* [36], where the set of participants must satisfy the threshold *for all levels* $i$.

# Chapter 4

# CRT-based threshold schemes and their security

In this chapter we introduce the CRT-based threshold secret sharing schemes from [1, 16, 25], and present the security concepts introduced by Quisquater et al. [29] and their results concerning the security of the threshold scheme in [16] 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 [11, 15]) as the formal approach to "integers of the same magnitude" [16]. 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, 16, 25], for which we provide a more suitable bound [15] for the loss of entropy, and study the security of the schemes in [1, 16, 25] based on ($k$-)compact sequences of co-primes. Furthermore, for the schemes in [1] and [16] a necessary and sufficient condition is provided with respect to *asymptotic idealness*

## 4.1 Threshold secret sharing schemes

### 4.1.1 The 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*).

The *Asmuth-Bloom* $(t+1, n)$*-threshold scheme* [1] is defined as follows:

**Asmuth-Bloom scheme**

| | |
|---|---|
| **parameter setup** | 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; |
| **secret and share spaces** | 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 sharing** | given a secret $s$, generate a random $r$ such that $s' = s + rm_0 < \prod_{i=1}^{t+1} m_i$. Share $s$, by $s_i = s' \bmod m_i$ for all $1 \leq i \leq n$; |

**secret reconstruction** any set $A$ of participants with $|A| \geq t+1$ can uniquely reconstruct the secret $s$ 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 has to try to get the secret.

### 4.1.2 The Mignotte scheme

In the Mignotte scheme [25] 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:

- $m_1 < \cdots < m_n$;
- $\alpha \leq \beta$, 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* [25] is defined as follows:

**Mignotte scheme**

| | |
|---|---|
| **parameter setup** | 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 $s_i = s \bmod m_i$ 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.

### 4.1.3 The GRS scheme

The Goldreich, Ron and Sudan scheme [16], 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* [16] 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 $\lvert A \rvert \geq t + 1$ 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".

### 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, 16, 25] 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 setup** | 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; |
| **secret and share spaces** | 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 $1 \leq i \leq n$; |
| **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 computes 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. |

## 4.2 Security properties

Starting from the security arguments in [1, 25], Quisquater et al. [29] 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 [16] 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* [29] assigned to $y_I$, denoted $\Delta(y_I)$, as

$$\Delta(y_I) = H(X) - H(X \,|\, Y_I = y_I) \ ,$$

for any $y_I \in \prod_{i\in I}\mathbb{Z}_{m_i}$.

**Definition 4.2.1.** [29] Given a set of participants $U$ of cardinality $n$, a CRT $(t, n, m_0, m_1, \ldots, m_n)$-threshold scheme is called *asymptotically perfect* if, for any non-empty subset $I \subseteq U$ with $|I| \leq t$ and any $\epsilon > 0$, there exists $m \geq 0$ such that for any sequence of co-primes $m_0 < m_1 < \ldots < m_n$ with $m_0 \geq m$, the following hold:

- $H(X) \neq 0$;
- $|\Delta(y_I)| < \epsilon$ for any $y_I \in \prod_{i\in I}\mathbb{Z}_{m_i}$.

**Definition 4.2.2.** [29] Given a set of participants $U$ of cardinality $n$, a CRT $(t, n, m_0, m_1, \ldots, m_n)$-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:

$$\frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} < 1 + \epsilon.$$

Note that $|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}|$ is the *information rate* associated to the $i$th participant.

In [29] it was shown that the 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 4.2.3.** *[29] The loss of entropy of the GRS* $(t, n, m_0, m_1, \ldots, m_n)$*-threshold scheme with respect to the uniform distribution on the secret space satisfies the following relations:*

- $\Delta(y_I) \leq \log \dfrac{m_0 \left( \left\lfloor \dfrac{C(I)+1}{m_0} \right\rfloor + 1 \right)}{C(I)}$, *if* $C(I) \neq 0$,
- $\Delta(y_I) = \log m_0$, *if* $C(I) = 0$,

*for any* $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, *where*

$$C(I) = \left\lfloor \frac{m_0 \prod_{i=1}^{t} m_i}{\prod_{i \in I} m_i} \right\rfloor .$$

The following result is a straightforward adaptation of the previous lemma.

**Corollary 4.2.4.** *The loss of entropy of the Asmuth-Bloom* $(t, n, m_0, m_1, \ldots, m_n)$*-threshold scheme, satisfies the same relations as those in Lemma 4.2.3 for*

$$C(I) = \left\lfloor \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i \in I} m_i} \right\rfloor .$$

**Theorem 4.2.5.** *[29] 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 4.2.6.** *[29] The GRS $(t+1, n)$-threshold scheme based on sequences of consecutive primes is asymptotically ideal, under the uniform distribution on the secret space.*

Given the instance CRT $(t, n, m_0, m_1, \ldots, m_n)$, a secret $s \in \mathbb{Z}_{m_0}$, and a non-empty set $I \subseteq U$, we define $Y_{s,I}$ as the random variable that takes the value $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ as the combined shares of all $i \in I$ in the same process of sharing $s$.

**Definition 4.2.7.** [29] Given a set of participants $U$ of cardinality $n$, a CRT $(t, n, m_0, m_1, \ldots, m_n)$-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 $s, s' \in \mathbb{Z}_{m_0}$, and any non-empty set $I \subseteq U$ with $|I| \leq t$, the following holds:

$$\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{s,I} = y_I) - P(Y_{s',I} = y_I)| \leq \frac{1}{poly(m_0)}$$

In [29] 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 4.2.8.** *[29] 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.*

## 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 [29] 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 [16], 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 [11, 15] 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 $\theta \in (0, 1)$.

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.* 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 of co-primes is *almost* $\Theta$*-compact* if $m_i \in (x, x + x^\theta)$ for all $1 \leq i \leq n$, where $\lceil x + x^\theta \rceil = 2m_0 - 2$ and $\theta \in (0, \Theta]$. One can replace "$x = 2m_0 - 2$" by "$x = km_0 - 2$", for any fixed integer $k \geq 2$.

**Definition 4.3.2.** [11, 15]

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.

### 4.3.1 More on asymptotic idealness

The concepts of asymptotic perfectness and idealness 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.

**Definition 4.3.3.** [11, 15] 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 $I \subseteq U$ 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 4.3.4.** [11, 15] The information rate of the CRT $(t+1, n)$-threshold scheme based on $k$-compact sequences of co-primes *goes asymptotically to* $k$ 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:

$$\left| \frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} - k \right| < \epsilon \ .$$

**Definition 4.3.5.** [11, 15] 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.

### 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 4.3.6.** *[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.*

**Corollary 4.3.7.** *[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 $m$.*

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 $\ell(x, \theta) = \pi(x + x^\theta) - \pi(x)$ [1] denote the longest sequence of consecutive primes in between $x$ and $x + x^\theta$.

[1] $\pi(x)$ is defined as the number of primes less than or equal to $x$.

Baker et al. [2] have shown that, if $\theta \geq 0.54$ and $x$ is sufficiently large, then

$$\ell(x,\theta) = \pi(x + x^{\theta}) - \pi(x) > \frac{2x^{\theta}}{5\log(x + x^{\theta})} \tag{4.1}$$

**Lemma 4.3.8.** *[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*

$$\ell > \ell(x,\theta) + \left\lfloor \sum_{i=2}^{k} \frac{2ix^{\theta_i/i}}{5\log(x + x^{\theta})} \right\rfloor$$

## 4.4 Bounding the loss of entropy

Lemma 4.3.6 and Corollary 4.3.7 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 precis approximation of the loss of entropy in the Asmuth-Bloom threshold scheme. Furthermore, the same results can be extended to the GRS threshold scheme.

**Lemma 4.4.1.** *[15] Let $U$ be a set of $n$ participants, and $I \subseteq U$ a non-empty subset. The loss of entropy of the Asmuth-Bloom $(t, n, m_0, m_1, \ldots, m_n)$-threshold scheme under a uniform distribution over the secret space satisfies the following relations:*

- $\Delta(y_I) = \log m_0 + \delta_1 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I}$, *if* $C_I \neq 0$,

- $\Delta(y_I) = \log m_0$, *if* $C_I = 0$,

*for any* $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, *where* $\delta_1 + \delta_2 = m_0$, $\delta_2 = C_I \bmod m_0$, *and* $C_I$ *is either* $C(I)$ *or* $C(I) + 1$ *depending on* $I$ *(*$C(I)$ *is the one defined in Corollary 4.2.4).*

**Proposition 4.4.2.** *[15] Corollary 4.2.4 is a direct consequence of Lemma 4.4.1.*

**Corollary 4.4.3.** *Let* $C(I)$ *be defined as in Lemma 4.2.3. The result in Lemma 4.4.1, equally holds for the GRS* $(t, n, m_0, m_1, \ldots, m_n)$*-threshold scheme.*

## 4.5 Security of the GRS scheme

In [29] 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 [29] to include $(t, \Theta)$-compact sequences.

Then, in [11] with the introduction of $k$-compact sequence we proved there exists a necessary and sufficient condition regarding the asymptotic perfectness property of the GRS scheme. Meaning, the GRS $(t+1, n)$-threshold scheme is asymptotically perfect with the information rate asymptotically $k$ if and only if $k$-compact sequences are considered. Furthermore, the GRS scheme based on $k$-compact sequences is perfect zero-knowledge.

### 4.5.1 Based on compact sequences

**Theorem 4.5.1** (asymptotic perfectness). *[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.*

**Theorem 4.5.2** (asymptotic idealness). *[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.*

**Theorem 4.5.3** (perfect zero-knowledge). *[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.*

### 4.5.2 Based on $k$-compact sequences

**Theorem 4.5.4** (asymptotic perfectness). *[11] Let* $0 < t+1 \leq n$ *be two positive integes 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.*

**Corollary 4.5.5** (asymptotic idealness). *[11] Let* $0 < t+1 \leq n$ *be two positive integes. 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 compact sequences of co-primes.*

**Theorem 4.5.6** (perfect zero-knowledge)**.** *[11] 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.*

## 4.6 Security of the Asmuth-Bloom scheme

In [23] 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:

$$\prod_{i=1}^{t+1} m_i > m_0^2 \prod_{i=0}^{t-1} m_{n-i}$$

(The extended Asmuth-Bloom sequences of co-primes are Asmuth-Bloom sequences of co-primes.)

Our contribution consists of upper bounding the loss of entropy for the Asmuth-Bloom scheme based on Asmuth-Bloom sequences by asymptotically $\log 2$. Moreover, we proved that if one considers extended Asmuth-Bloom sequences, the Asmuth-Bloom scheme is asymptotically perfect.

We also introduction compact sequences of co-primes [3] and proved the Asmuth-Bloom scheme based on almost $\Theta$-compact

sequences is asymptotically perfect, and the information rate is asymptotically 2. By changing the secret space from the first element in the sequences of co-primes to the last element, we obtained a variant of the Asmuth-Bloom scheme that is asymptotically ideal if *quasi*-compact sequences are considered.

Then, in [15] with the introduction of $k$-compact sequence we proved there exists a necessary and sufficient condition regarding the asymptotic perfectness property of the Asmuth-Bloom scheme. Meaning, the Asmuth-Bloom $(t+1, n)$-threshold scheme is asymptotically perfect and the information rate goes asymptotically to $k$ if and only if $k$-compact sequences are considered.

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, on *quasi*-compact sequences and on $k$-compact sequences are perfect zero-knowledge.

### 4.6.1 Based on (extended) Asmuth-Bloom sequences

**Lemma 4.6.1** (loss of entropy)**.** *[3] The loss of entropy of the Asmuth-Bloom $(t, n, m_0, m_1, \ldots, m_n)$-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* $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, *and for any sub-set* $I \subseteq U$.

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** (asymptotic perfectness)**.** *[15] 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.*

**Remark 4.6.3.** 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 4.6.2 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 Based on compact sequences

#### Almost $\Theta$-compact

**Theorem 4.6.4** (asymptotic perfectness)**.** *[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.*

**Theorem 4.6.5** (asymptotic idealness)**.** *[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.*

**Theorem 4.6.6** (perfect zero-knowledge)**.** *[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.*

#### *Quasi*-compact

**Theorem 4.6.7** (asymptotic perfectness)**.** *[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.*

**Theorem 4.6.8** (asymptotic idealness)**.** *[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.*

**Theorem 4.6.9** (perfect zero-knowledge)**.** *[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.*

### 4.6.3 Based on $k$-compact sequences

**Theorem 4.6.10** (asymptotic perfectness)**.** *[15] 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.*

**Corollary 4.6.11** (asymptotic idealness)**.** *[15] 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 compact sequences of co-primes.*

**Theorem 4.6.12** (perfect zero-knowledge)**.** *[15] 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.*

## 4.7 Security of the Mignotte scheme

As far as we are concern, 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.

**Theorem 4.7.1.** *[3] The loss of entropy of the Mignotte $(t+1, n)$-threshold scheme cannot be bounded from above.*

Based on Theorem 4.7.1, we must conclude that the scheme is not asymptotically perfect.

**Theorem 4.7.2.** *[3] The information rate of the Mignotte $(t+1, n)$-threshold scheme converges to 0.*

As a conclusion, based on Theorem 4.7.2, the Mignotte threshold scheme is far from being asymptotically ideal.

**Theorem 4.7.3.** *[3] The Mignotte $(t+1, n)$-threshold scheme is not perfect zero-knowledge.*

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

In this chapter we deal with the construction of other CRT-based schemes that satisfy the security properties of Section 4.2.

In [14] 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

**Definition 5.1.1.** [14] 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. $w : U \to \mathbb{R}$ 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. $\Gamma = \{A \subseteq U | w(A) \geq 1\}$.

**Lemma 5.1.2.** *[14] DWTAS are strict extensions of DMAS.*

**Theorem 5.1.3.** *[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. *$\Gamma$ 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 5.1.4.** *[14] There are DWTAS that are not ideal.*

**Definition 5.1.5.** [14] Given $A \subseteq U$, the *characteristic vector of $A$ w.r.t.* $(w, \bar{t}, \Gamma)$ is a vector $c_A = (c_1, \ldots, c_q)$ which satisfies

$$c_i = \left|\{a \in A \,|\, w(a) = 1/t_i\}\right| ,$$

for all $1 \leq i \leq q$.

**Lemma 5.1.6.** *[14] Let $(w, \bar{t}, \Gamma)$ 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* $t_l < \sum_{i=l}^{r} c_i \leq t_r$.

## 5.2 DWTSSS

**Definition 5.2.1.** [14] Let $0 < \epsilon \leq 1$ be a real number and $\bar{t} = (t_1, \ldots, t_q)$ and $\overline{n} = (n_1 \ldots, n_q)$ 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 $(\epsilon, \bar{t}, \overline{n})$-*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 $x, y \in \cup_{i=1}^{q} L_i$ 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 $\beta = \min\{x^{t_i} | 1 \leq i \leq q,\ x \in L_i\}$.

**Theorem 5.2.2.** *[14] There are $(\epsilon, \bar{t}, \overline{n})$-sequences with arbitrarily large security parameters, for any $\epsilon$, $\bar{t}$, and $\overline{n}$ as in Definition 5.2.1.*

**DWTSSS**

**parameter setup** choose an $(\epsilon, \bar{t}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i \mid 1 \leq i \leq q))$, where $n_i = |U_i|$ for all $1 \leq i \leq q$ ($\mathcal{L}$ will be called an $(\epsilon, \bar{t}, \overline{n})$-*sequence associated to* $(w, \bar{t}, \Gamma)$). The integers $\bar{t}, \overline{n}, m_0, m_{1,1}, \ldots, m_{q,n_q}$ are public parameters;

**secret and share spaces** 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;

**secret sharing** given a secret $s$, generate a random $r$ such that $s' = s + rm_0 < \beta$ is computed (Recall that $\beta = \min_{i=1}^{q}\{m_{i,1}^{t_i}\}$). Share $s$, by $s_{i,j} = s' \bmod m_{i,j}$ 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 $s$ by computing the unique solution modulo $\prod_{(i,j)\in A} m_{i,j}$ of the system

$$x \equiv s_{i,j} \bmod m_{i,j}, \quad \forall (i,j) \in A \ .$$

and then reducing it modulo $m_0$.

## 5.3 Security issues of DWTSSS

**Theorem 5.3.1** (asymptotic perfectness)**.** *[14] The* $(w, \bar{t}, \Gamma)$*-DWTSSS over a set* $U$ *is asymptotically perfect with respect to the uniform distribution over the secret space.*

**Theorem 5.3.2** (asymptotic idealness)**.** *[14] The* $(w, \bar{t}, \Gamma)$*-DWTSSS over a set* $U$*, under the uniform distribution over the secret space, cannot be asymptotically ideal.*

**Theorem 5.3.3** (perfect zero-knowledge)**.** *[14] The* $(w, \bar{t}, \Gamma)$*-DWTSSS over a set* $U$ *is perfect zero-knowledge with respect to the uniform distribution over the secret space.*

# Chapter 6

# Conclusion and Future work

The authors of [16], 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 [16]). If the primes are consecutive and large enough, as it was used in [29], they may be considered of the same magnitude. However, "same magnitude" should mean more that "consecutive primes".

Starting from this remark, the 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, 25, 16] when they are based on sequences of co-primes of the same magnitude. We proved that

- sequences of consecutive primes or consecutive co-primes are particular cases of ($k$-)compact sequences of co-primes;
- we can find arbitrarily long ($k$-)compact sequences of arbitrarily large co-primes, and
- 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.

One may identify the following open problems:

**Open problem OP5'** aimed at the construction of CRT-based schemes for other classes of access structures.

**Open problem OP6** focuses on the comparison between *compact sequences* and *epsilon sequences with one level*.

**Open problem OP7** deals with the difference between perfectness and asymptotic perfectness ensured by *(1-)compact sequences* of co-primes.

# Bibliography


[1] C. A. Asmuth and J. Bloom. A Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, 29(2):208–210, Mar. 1983. (also in the National Telecommunications Conference, Houstan, Dec. 1980).

[2] R. Baker and G. Harman. The Difference Between Consecutive Primes. *Proceedings of the London Mathematical Society*, 72(3):261–280, 1996.

[3] M. Barzu, F. L. Ţiplea, and C. C. Drăgan. Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes. *Information Sciences*, 240:161–172, 2013.

[4] A. Beimal, T. Tassa, and E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. In *2nd International Conference on the Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 600–619, 2005.

[5] A. Beimal, T. Tassa, and E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *SIAM Journal of Discrete Mathematics*, 22(1):360–397, 2008.

[6] M. Belenkiy. Disjunctive Multi-level Secret Sharing. Technical report, Brown University, 2008. http://eprint.iacr.org/2008/018.

[7] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). In J. Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1–10. ACM, 1988.

[8] E. F. Brickell and D. R. Stinson. Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes. *J. Cryptology*, 5(3):153–166, 1992.

[9] R. M. Capocelli, A. D. Santis, L. Gargano, and U. Vaccaro. On the Size of Shares for Secret Sharing Schemes. *J. Cryptology*, 6(3):157–167, 1993. (a preliminary version of this paper appeared in "Advances in Cryptology CRYPTO '91", J. Feigenbaum, ed., Lecture Notes in Computer Science 576 (1992), 101-113).

[10] D. Chaum, C. Crépeau, and I. Damgård. Multiparty Unconditionally Secure Protocols (Extended Abstract). In J. Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–19. ACM, 1988.

[11] F. L. Ţiplea and C. C. Drăgan. A Necessary and Sufficient Condition for the Asymptotic Idealness of the GRS Threshold Secret Sharing Scheme. *Information Processing Letters*, submitted for publication, May 2013.

[12] Y. Desmedt and Y. Frankel. Shared Generation of Authenticators and Signatures (Extended Abstract). In *Advances*

*in Cryptology - CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer, 1992.

[13] C. C. Drăgan. Interactive Secret Share Management. In E. Fernández-Medina, M. Malek, and J. Hernando, editors, *SECRYPT*, pages 266–269. INSTICC Press, 2009.

[14] C. C. Drăgan and F. L. Ţiplea. Distributive Weighted Threshold Secret Sharing Schemes. *Information Sciences*, submitted for publication, Apr. 2013.

[15] C. C. Drăgan and F. L. Ţiplea. On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme. *Designs, Codes and Cryptography*, submitted for publication, June 2013.

[16] O. Goldreich, D. Ron, and M. Sudan. Chinese Remaindering with Errors. *IEEE Transactions on Information Theory*, 46(4):1330–1338, Mar. 2000.

[17] S. Goldwasser, S. Jarecki, and A. Lysyanskaya. Cryptography and Information Security Group Research Project: Threshold Cryptology. http://groups.csail.mit.edu/cis/cis-threshold.html, cited July 2013.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, (CCS 2006)*, pages 89–98. ACM, 2006.

[19] L. Harn and C. Lin. Authenticated Group Key Transfer Protocol Based on Secret Sharing. *IEEE Trans. Computers*, 59(6):842–846, 2010.

[20] S. Iftene. *Secret Sharing Schemes with Applications in Security Protocols*. PhD thesis, "Alexandru Ioan Cuza" University of Iasi, Romania, 2007.

[21] M. Iwamoto. *General Construction Methods of Secret Sharing Schemes and Visual Secret Sharing Schemes*. PhD thesis, Univ. of Tokyo, Mar. 2004.

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

[23] K. Kaya and A. A. Selcuk. Threshold cryptography based on Asmuth-Bloom secret sharing. *Information sciences*, 177(19):4148–4160, 2007.

[24] S. C. Kothari. Generalized Linear Threshold Scheme. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 231–241, 1985.

[25] M. Mignotte. How to Share a Secret? In T. Beth, editor, *Workshop on Cryptography*, volume 149 of *Lecture Notes in Computer Science*, pages 371–375, Burg Feuerstein, 1982.

[26] P. Morillo, C. Padr, G. Sez, and J. Villar. Weighted threshold secret sharing schemes. *Information Processing Letters*, 70(5):211–216, 1999.

[27] M. Naor and A. Wool. Access Control and Signatures via Quorum Secret Sharing. *IEEE Trans. Parallel Distrib. Syst.*, 9(9):909–922, 1998.

[28] A. Patra. *Studies on Verifiable Secret Sharing, Byzantine Agreement and Multiparty Computation*. PhD thesis, Indian Institute of Technology, Department of Computer Science and Engineering, Madras, May 2010.

[29] M. Quisquater, B. Preneel, and J. Vandewalle. On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. In D. Naccache and P. Paillier, editors, *Public Key Cryptography*, volume 2274 of *Lecture Notes in Computer Science*, pages 199–210. Springer, 2002.

[30] M. O. Rabin. Randomized Byzantine Generals. In *24th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 403–409. IEEE Computer Society, 1983.

[31] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[32] G. J. Simmons. How to (Really) Share a Secret. In S. Goldwasser, editor, *8th Annual International Cryptology Conference on Advances in Cryptology (CRYPT '88)*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer, 1988.

[33] A. Sreekumar. *Secret Sharing Schemes using Visual Cryptography.* PhD thesis, Cochin University of Science and Technology, Department of Computer Applications, June 2009.

[34] D. Stinson. *Cryptography: Theory and Practice.* Chapman and Hall/CRC, 3 edition, 2005.

[35] D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.

[36] T. Tassa. Hierarchical Threshold Secret Sharing. *Journal of Cryptology*, 20(2):237–264, 2007.

[37] T. Tassa. Generalized oblivious transfer by secret sharing. *Des. Codes Cryptography*, 58(1):11–21, 2011.