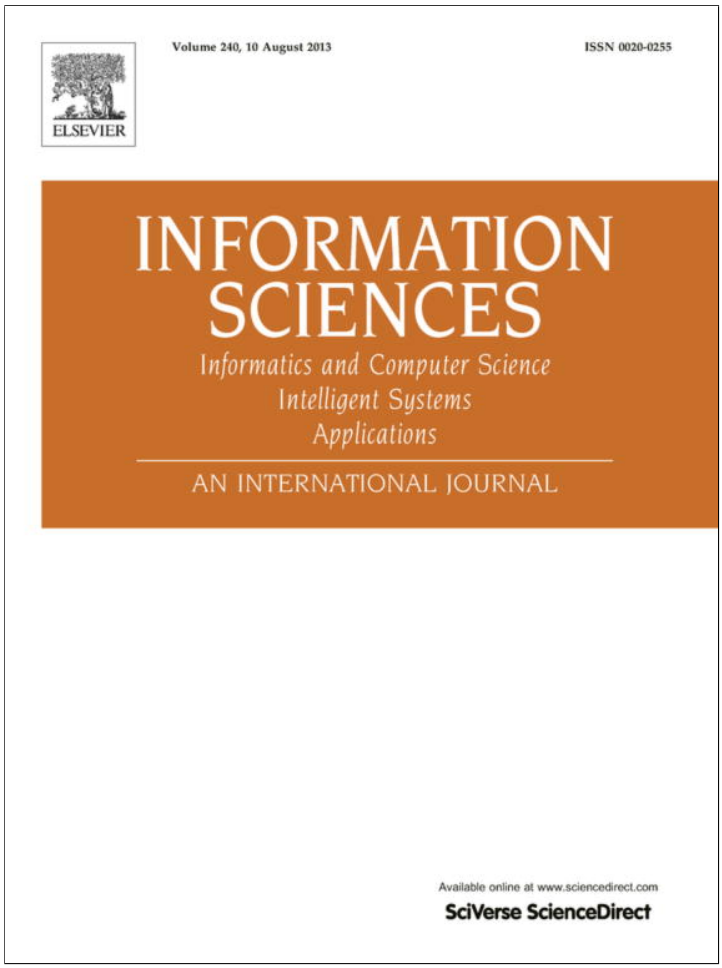

Information Sciences 240 (2013) 161–172

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes

Mihai Barzu [a], Ferucio Laurenţiu Ţiplea [a,*], Constantin Cătălin Drăgan [a,1]

[a] Department of Computer Science, "Al.I.Cuza" University of Iaşi, Romania

ARTICLE INFO

Article history:
Received 15 December 2011
Received in revised form 19 March 2013
Accepted 29 March 2013
Available online 6 April 2013

Keywords:
Secret sharing scheme
Chinese remainder theorem
Entropy
(asymptotic) Perfectness
(asymptotic) Idealness
Perfect zero-knowledge

ABSTRACT

CRT-based threshold secret sharing schemes use sequences of pairwise co-prime positive integers in their construction. If these sequences are not "compact", then the CRT-based threshold secret sharing schemes may have a weak security in the sense of a massive loss of entropy or an arbitrarily large information rate.

In this paper, *compact sequences of co-primes* are introduced, and their applications to the security of CRT-based threshold secret sharing schemes is throughout investigated. It is shown that all the results regarding the security of CRT-based threshold secret sharing schemes that use sequences of consecutive primes also hold for threshold secret sharing schemes that use compact sequences of co-primes. Moreover, 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.

1. Introduction

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. Any $(t+1, n)$-threshold secret sharing scheme should satisfy some *security properties* with respect to the secret reconstruction from less than $t+1$ shares. Ideally, less than $t+1$ shares should give no information on the secret from an information theoretic point of view (*idealness* property) and complexity theoretic point of view (*perfect zero-knowledge* property).

Threshold secret sharing schemes (threshold schemes, for short) were independently proposed for the first time by Blakley [3] and Shamir [10]. Blakley's threshold scheme is based on hyperplane intersections, while Shamir's threshold scheme is based on polynomial interpolation. A novel class of threshold schemes is the one based on the Chinese Remainder Theorem (CRT) [1,6,5]. The schemes in this class 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.

The security of the CRT-based secret sharing schemes in [1,6] was argued by counting the number of possible solutions a group of less than $t+1$ users have to try in order to get the secret. The authors of [5] discuss the security of their threshold scheme 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". Starting from the security arguments

* Corresponding author.
E-mail addresses: mihai.barzu@info.uaic.ro (M. Barzu), fltiplea@info.uaic.ro (F.L. Ţiplea), constantin.dragan@info.uaic.ro (C.C. Drăgan).

[1] 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].

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.03.062

in [1,5], Quisquater et al. [8] have introduced two modern concepts in order to study the security of a threshold scheme, namely *asymptotic perfectness* and *asymptotic idealness*. Then, they proved that the threshold scheme in [5] is asymptotically ideal (and, therefore, asymptotically perfect) and perfect zero-knowledge, provided that it uses sequences of consecutive primes.

Contribution. Looking again at the security arguments in [5], we can see 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 [5], although they did not define the term "same magnitude"). Sequences of sufficiently large consecutive prime numbers, as considered in [8], are examples of sequences of prime numbers of the same magnitude. However, "integers of the same magnitude" should mean more than "consecutive primes". Moreover, with a suitable definition for the "same magnitude", one should expect similar results to those developed in [8] for CRT-based threshold schemes based on sequences of co-primes of the same magnitude. This is in fact the aim of our paper. More precisely:

1. we introduce 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 $\theta \in (0, 1)$;
2. we show that all the results established in [8] hold if the threshold scheme in [5] is based on compact sequences of co-primes instead of sequences of consecutive primes;
3. we provide a very detailed analysis of the security of the threshold schemes proposed in [1,6] by using the concepts introduced in [8] (we emphasize that [8] mainly focuses on the threshold schemes in [1,5] and overviews [6], whereas we opt to perform a detaited analysis for the sake of completeness and formality). Two variants of the threshold scheme in [1], with better security properties, are also proposed.

As it will be shown in this paper, sequences of consecutive primes or sequences of *consecutive co-primes* are particular cases of compact sequences of co-primes. Moreover, 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 a better security for the 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 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.

Paper organization. The paper is organized into six sections. The rest of this section recalls some basic notations in number theory, while the second section introduces compact sequences of co-primes and some of their basic properties. The properties of asymptotic perfectness, idealness, and perfect zero-knowledge for the threshold scheme in [5] with compact sequences of co-primes are discussed in Section 3. The fourth section provides a detailed analysis of the threshold scheme in [1], while the fifth section does the same for the threshold scheme in [6]. We conclude in Section 6.

Notation. Throughout this paper, $\mathbb{Z}$ stands for the set of integers, and $\mathbb{N}$ is the set of positive integers. For two integers a and b, (a, b) stands for the greatest common divisor of a and b. The integers a and b are called *co-prime* if $(a, b) = 1$, and they are called *congruent modulo n*, denoted $a \equiv b \bmod n$, if n divides $a - b$ (n is an integer too). The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$. A positive integer $a > 1$ is a *prime* number if the only positive divisors of it are 1 and a. $p_1, p_2, \ldots$ stands for the infinite sequence of prime numbers. The prime counting function $\pi(x)$ is defined as the number of primes less than or equal to x. Given two random variables X and Y, $H(X)$ stands for the entropy of X, and $H(X|Y)$ stands for the entropy of X conditioned by Y. $\mathcal{O}$ stands for the "big O notation".

2. Compact sequences of co-primes

In this section we introduce *compact sequences of co-primes* and then study some of their basic properties. This concept of compact sequence of co-primes captures the idea of sequence of co-primes of the "same magnitude", and it will play an important role in defining CRT-based threshold schemes with good security properties.

The length of a sequence $m_0 < \cdots < m_n$ of integers is $n + 1$. An increasing sequence 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*. Similar concepts can be introduced for co-prime numbers as we see below.

Definition 1. An increasing sequence $m_0 < \cdots < m_n$ of positive integers, where $n \geqslant 1$, is called a *sequence of co-primes* if $(m_i, m_j) = 1$ for any $0 \leqslant i, j \leqslant n$ with $i \neq j$.

Any sequence of primes is a sequence of co-primes.

Definition 2. An increasing sequence $m_0 < \cdots < m_n$ of positive integers, where $n \geqslant 1$, is called a *sequence of consecutive co-primes* if, for any $1 \leqslant i \leqslant n$, m_i is the least integer greater than m_{i-1} and co-prime to each of $m_0, \ldots, m_{i-1}$.

Clearly, any sequence of consecutive co-primes is a sequence of co-primes. There are sequences of consecutive primes which are sequences of consecutive co-primes (such as 2, 3, 5, 7, 11, 13, 17, 19, 23) but, in general, a sequence of consecutive primes is not necessarily a sequence of consecutive co-primes.

Definition 3. A sequence $m_0 < \cdots < m_n$ of co-primes, where $n \geqslant 1$, is called a *compact sequence of co-primes* if $m_n < m_0 + m_0^\theta$, for some real number $\theta \in (0, 1)$.

Definition 4. A sequence $m_0 < \cdots < m_n$ of positive integers *covers* another sequence $q_0 < \cdots < q_s$ of positive integers if $m_0 \leqslant q_0$ and $q_s \leqslant m_n$.

Remark 5. If a sequence $q_0 < \cdots < q_s$ of co-primes is covered by a compact sequence $m_0 < \cdots < m_n$ of co-primes, then it is also compact. This is because

$$q_s \leqslant m_n < m_0 + m_0^\theta \leqslant q_0 + q_0^\theta$$

for any $\theta \in (0, 1)$ with $m_n < m_0 + m_0^\theta$.

Lemma 6. *For any integer $n \geqslant 1$ there exists $m \geqslant 0$ such that any sequence $m_0 < \cdots < m_n$ of consecutive primes or co-primes with $m_0 \geqslant m$ is a compact sequence of co-primes.*

Proof. Let $n \geqslant 1$. Consider first the case of consecutive prime sequences. It is known [9] that

$$\lim_{i\to\infty} \frac{p_{i+1} - p_i}{p_i} = 0$$

This shows that for any $\epsilon > 0$ there exists i_0 such that $p_{i+1} < (1 + \epsilon)p_i$, for any $i \geqslant i_0$. Therefore, $p_{i+j} < (1 + \epsilon)^j p_i$, for any $i \geqslant i_0$ and $j \geqslant 1$.

Let $\epsilon \in \left(\sqrt[n]{3/2} - 1, \sqrt[n]{2} - 1\right)$ and i_0 such that $p_{i+1} < (1 + \epsilon)p_i$ for any $i \geqslant i_0$. Consider $m = p_{i_0}$ and show that $p_i < p_{i+1} < \cdots < p_{i+n}$ is a compact sequence of co-primes, for any $i \geqslant i_0$. Indeed, because $\epsilon \in \left(\sqrt[n]{3/2} - 1, \sqrt[n]{2} - 1\right)$ it follows that

$$0 < 1 + \log_{p_i}((1 + \epsilon)^n - 1) < 1$$

which shows that if we choose θ in between $1 + \log_{p_i}((1 + \epsilon)^n - 1)$ and 1 we obtain

$$p_{i+n} < (1 + \epsilon)^n p_i < p_i + p_i^\theta$$

for any $i \geqslant i_0$. As a conclusion, for any $i \geqslant i_0$, $p_i < p_{i+1} < \cdots < p_{i+n}$ is a compact sequence of co-primes with $p_i \geqslant m$.

The case of consecutive co-prime sequences simply follows from the previous case. Indeed, let $m = p_{i_0}$ as it was obtained above and let $m_0 < \cdots < m_n$ be a sequence of consecutive co-primes with $m_0 \geqslant m$. Let i be the greatest positive integer such that $p_i \leqslant m_0$. It is easy to see that $p_{i+1} \geqslant m_1$ because, otherwise, p_{i+1} would be the least integer greater than m_0 and co-prime to m_0. Inductively, one obtains $m_j \leqslant p_{i+j}$, for any $1 \leqslant j \leqslant n$. This shows that $m_0 < \cdots < m_n$ is covered by $p_i < p_{i+1} < \cdots < p_{i+n}$. As $i \geqslant i_0$, $p_i < p_{i+1} < \cdots < p_{i+n}$ is a compact sequence of co-primes, showing that $m_0 < \cdots < m_n$ is a compact sequence of co-primes too (by Remark 5). □

Corollary 7. *For any $n \geqslant 1$ and $m \geqslant 0$ there exist compact sequences of co-primes of length $n + 1$ whose first element is greater than or equal to m.*

Proof. Directly from Lemma 6. □

Remark 8. Any sequence of consecutive primes of length $n + 1$ covers at least one sequence of consecutive co-primes of length $n + 1$. The proof of Lemma 6 shows that the converse of this holds as well: any sequence of consecutive co-primes of length $n + 1$ is covered by some sequence of consecutive primes of length $n + 1$.

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. The longest sequence of consecutive primes in the interval $(x, x + x^\theta)$ has length $\ell(x, \theta) = \pi(x + x^\theta) - \pi(x)$. According to [2], if $\theta \geqslant 0.54$ and x is sufficiently large, then

$$\ell(x, \theta) = \pi(x + x^\theta) - \pi(x) > \frac{2x^\theta}{5\log(x + x^\theta)} \tag{1}$$

Our goal next is to show that the interval $(x, x + x^\theta)$ contains sequences of co-primes significantly denser than the sequence of consecutive primes in this interval.

Lemma 9. *For any $k \geqslant 2$ there exist $\theta, \theta_2, \ldots, \theta_k \in (0, 1)$ and $x_0 > 0$ such that, for any $x \geqslant x_0$, the interval $(x, x + x^\theta)$ contains compact sequences of co-primes whose length ℓ satisfies*

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

Proof. Let $k \geqslant 2$ be an integer. The approach we follow is to count the number of prime powers that are in an interval of the form $(x, x + x^\theta)$, where $\theta \in (0, 1)$. That is, we will count the number of primes p such that $x < p^e < x + x^\theta$, for some $e \geqslant 1$. First, remark that if $x < p^e < x + x^\theta$ for some $e \geqslant 1$, then $p^{e+1} > x + x^\theta$ because

$$p^{e+1} = p \cdot p^e > 2x > x + x^\theta$$

That is, $(x, x + x^\theta)$ may contain at most one power of a given prime number. Therefore, the sequence of all prime powers in the interval $(x, x + x^\theta)$ forms a sequence of co-primes. In order to estimate the length of this sequence we shall use the function π^* from [7] which is given by

$$\pi^*(x) = |\{p \mid p \text{ is a prime and } p^e \leqslant x \text{ for some integer } e \geqslant 1\}|$$

for any $x > 0$. It is clear that $\pi^*(x)$ can be computed by

$$\pi^*(x) = \pi(x) + \pi(x^{1/2}) + \cdots + \pi(x^{1/s})$$

where $s = max\{1, [\log x/\log 2]\}$. Therefore, the number of prime powers in between x and $x + x^\theta$ is given by $\pi^*(x + x^\theta) - \pi^*(x)$ and satisfies

$$\pi^*(x + x^\theta) - \pi^*(x) \geqslant \sum_{i=1}^{s} (\pi((x + x^\theta)^{1/i}) - \pi(x^{1/i})) = \ell(x, \theta) + \sum_{i=2}^{s} (\pi((x + x^\theta)^{1/i}) - \pi(x^{1/i}))$$

where $s = max\{1, [\log x/\log 2]\}$. In order to obtain the result in the lemma, x should be large enough so that $s \geqslant k$.

We show now that there exists a sequence of positive real numbers

$$0.54 \leqslant \theta_k \leqslant \theta_{k-1} \leqslant \cdots \leqslant \theta_2 < \theta \tag{2}$$

such that $(x + x^\theta)^{1/i} > x^{1/i} + x^{\theta_i/i}$, for all $2 \leqslant i \leqslant k$.

For this, remark first that we have the inequalities

$$k(\theta - 1) + 1 < (k - 1)(\theta - 1) + 1 < \cdots < 2(\theta - 1) + 1 < \theta$$

Then, the binomial formula shows that

$$(x^{1/i} + x^{\theta_i/i})^i = x + \mathcal{O}(x^{(i-1+\theta_i)/i})$$

Therefore, for large enough x, if we choose $\theta_i < i(\theta - 1) + 1$, then one can easily see that $(x + x^\theta)^{1/i} > x^{1/i} + x^{\theta_i/i}$, for all $2 \leqslant i \leqslant k$. Moreover, if x is large enough and $\theta > 1 - 0.46/k$, then $k(\theta - 1) + 1 > 0.54$, showing that we can choose $\theta_2, \ldots, \theta_k$ satisfying (2).

Now, combining these with (1) we obtain

$$\begin{aligned}\pi^*(x + x^\theta) - \pi^*(x) &> \ell(x, \theta) + \sum_{i=2}^{k} (\pi((x + x^\theta)^{1/i}) - \pi(x^{1/i})) > \ell(x, \theta) + \sum_{i=2}^{k} (\pi(x^{1/i} + x^{\theta_i/i}) - \pi(x^{1/i})) \\ &> \ell(x, \theta) + \sum_{i=2}^{k} \frac{2x^{\theta_i/i}}{5\log(x^{1/i} + x^{\theta_i/i})} > \ell(x, \theta) + \sum_{i=2}^{k} \frac{2x^{\theta_i/i}}{5\log(x + x^\theta)^{1/i}} = \ell(x, \theta) + \sum_{i=2}^{k} \frac{2ix^{\theta_i/i}}{5\log(x + x^\theta)}\end{aligned}$$

for large enough x. This proves the lemma. □

Lemma 9 shows that any compact sequence of consecutive primes can be significantly enriched to a (compact) sequence of co-primes. As the next sections will show, this could play an important role in designing secure threshold schemes based on the Chinese Remainder Theorem.

3. Security of the GRS threshold scheme

The *Chinese Remainder Theorem* (CRT, for short) [4] is one of the fundamental tools in number theory, with many applications. It states that the system of congruences

$$x \equiv b_i \bmod m_i, \quad i \in I \tag{3}$$

where $I \subseteq \mathbb{N}$ is a finite non-empty set and b_i and m_i are integers for all $i \in I$, 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 $i \neq j$.

One of the main applications of CRT is in the design of threshold secret sharing schemes [1,6,5]. Given t and n such that $0 < t + 1 \leqslant n$, the main idea of constructing a *(t + 1, n)-threshold scheme* based on CRT is the following:

- consider first a sequence $m_0 < \cdots < m_n$ of co-primes. Depending on the scheme, this sequence may be subject to various constraints. The integers t, n, $m_0, \ldots, m_n$ are public parameters;
- define the *secret space* as being an interval $[\alpha, \beta)$, where α and β depend on the public parameters;
- define the *share space* of the ith participant as being $\mathbb{Z}_{m_i}$, for all $1 \leqslant i \leqslant n$;
- given a secret S in the secret space, share it by $S_i = S' \ mod \ m_i$, for all $1 \leqslant i \leqslant n$, where S' is obtained from S in some way (usually depending on t and on the scheme). Any $t + 1$ distinct shares should allow an easy reconstruction of the secret.

It is also expected that a $(t + 1, n)$-threshold scheme satisfies some *security properties* with respect to the secret reconstruction from less than $t + 1$ shares. Ideally, less than $t + 1$ shares should give no information on the secret (from both an information and complexity theoretic point of view).

The $(t + 1, n)$-threshold scheme in [5], called from now on the *GRS threshold scheme*, takes $\alpha = 0$ and $\beta = m_0$. Given a secret S, the integer S' is the unique solution modulo $m_0\prod_{i=1}^{t} m_i$ of the system

$$x \equiv r_i \ mod \ m_i, \quad 0 \leqslant i \leqslant t$$

where $r_0 = S$ and r_i is randomly chosen from $\mathbb{Z}_{m_i}$ for all $1 \leqslant i \leqslant t$. Any $t + 1$ distinct shares $S_{i_1}, \ldots, S_{i_{t+1}}$ can uniquely reconstruct the secret S by computing first the unique solution modulo $\prod_{j=1}^{t+1} m_{i_j}$ of the system

$$x \equiv S_{i_j} \ mod \ m_{i_j}, \quad 1 \leqslant j \leqslant t + 1$$

and then reducing it modulo m_0.

As with respect to the security of the GRS $(t + 1, n)$-threshold scheme, it was shown in [5] that at most $t - 1$ shares give no information on the secret from a complexity theoretic point of view, provided that the scheme is based on sequences of large enough primes of the same magnitude. This result was extended to t shares in [8]. In fact, in [8] it was shown that the GRS threshold scheme is asymptotically ideal (and, therefore, asymptotically perfect) and perfect zero-knowledge, provided that the scheme is based on sequences of consecutive primes.

The aim of this section is to show that all the results established in [8] also hold for the GRS threshold scheme based on compact sequences of co-primes. Recall that, as it has been shown in the previous section, a compact sequence of co-primes may be considerably more compact than a sequence of consecutive primes of the same length. This fact leads to better security properties if we base the secret sharing schemes on compact sequences of co-primes rather than on sequences of consecutive primes.

In order to reach the objective mentioned above we recall first, in a simplified way, a few concepts introduced in [8]. First, we will write $GRS(t, n, m_0, \ldots, m_n)$ to denote an instance of the GRS $(t + 1, n)$-threshold scheme as above with the public parameters t, n, and $m_0 < \cdots < m_n$. Then, assume that to any instance $GRS(t, n, m_0, \ldots, m_n)$ and any non-empty set $I \subseteq \{1, \ldots, n\}$, two random variables X and Y_I are associated. The first one takes values into the secret space $\mathbb{Z}_{m_0}$, while the second one into $\prod_{i\in I}\mathbb{Z}_{m_i}$. Given $y_I \in \prod_{i\in I}\mathbb{Z}_{m_i}$, define the *loss of entropy of GRS(t, n, m0, ..., mn) with respect to yI*, denoted $\Delta(y_I)$, by

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

The following result was obtained in [8] for the case of a GRS threshold scheme based on sequences of primes, but it holds equally for instances based on sequences of co-primes.

Lemma 10 [8]. *The loss of entropy of GRS(t, n, m0, ..., mn) with respect to $y_I \in \prod_{i\in I}\mathbb{Z}_{m_i}$ and a uniform distribution on the secret space satisfies the following relations:*

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

where

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

According to [8], the *GRS* $(t + 1, n)$-threshold scheme is called *asymptotically perfect* if, for any $\epsilon > 0$ there exists $m \geqslant 0$ such that for any sequence $m_0 < m_1 < \cdots < m_n$ of co-primes with $m_0 \geqslant m$ the following hold:

- $H(X) \neq 0$;
- $|\Delta(y_I)| < \epsilon$, for any non-empty subset $I \subseteq \{1, \ldots, n\}$ with $|I| \leqslant t$ and any $y_I \in \prod_{i\in I}\mathbb{Z}_{m_i}$.

Definition 11. A compact sequence of co-primes $m_0 < \cdots < m_n$ is called a *(t, Θ)-compact sequence of co-primes*, where $0 \leqslant t < n$ and $\Theta \in (0, 1)$, if $m_{t+1} \geqslant m_t + 2$ and $m_n < m_0 + m_0^{\theta}$ for some $\theta \in (0, \Theta]$.

Remark 12. Let $n \geqslant 1$, $0 \leqslant t < n$, $m \geqslant 0$, and $\Theta \in (0, 1)$.

The two constraints on (t, Θ)-compact sequences of co-primes (Definition 11) are technical and they will be used in proofs. A few words about them are in order:

1. the constraint "$m_{t+1} \geqslant m_t + 2$" is met by sequences of large consecutive primes, but not necessarily by sequences of co-primes. However, if $m_{t+1} = m_t + 1$, then $m_t \geqslant m_{t-1} + 2$ or $m_{t+2} \geqslant m_{t+1} + 2$, which shows that we can easily change the sequence $m_0 < \cdots < m_n$ into another sequence $m'_0 < \cdots < m'_n$ satisfying $m'_{t+1} \geqslant m'_t + 2$;
2. if in the proof of Lemma 6 we choose $\epsilon \in \left(\sqrt[n+1]{3/2} - 1, \sqrt[n+1]{1 + 2^{\Theta-1}} - 1\right)$, then one can show that there exist sequences $m_0 < m_1 < \cdots < m_n < m_{n+1}$ of co-primes of length $n + 2$ whose first element is greater than or equal to m and $m_{n+1} < m_0 + m_0^{\theta}$, for some $\theta \in (0, \Theta]$. Now, one can easily see that $m_0 < m_1 < \cdots < m_n$ or $m_1 < \cdots < m_n < m_{n+1}$ is a (t, Θ)-compact sequence of co-primes. Therefore, for any $n \geqslant 1$, $0 \leqslant t < n$, $m \geqslant 0$, and $\Theta \in (0, 1)$ there exist (t, Θ)-compact sequences of co-primes of length $n + 1$ whose first element is greater than or equal to m;
3. the constraint "$\theta \leqslant \Theta$" is required by the "asymptotic" nature of the security properties we are interested in (asymptotic perfectness and asymptotic idealness). Thus, this constraint assures that m_0^{θ}/m_0 converges to 0 as m_0 goes to infinity and, therefore, the information rate m_i/m_0 of the ith participant converges to 1 as m_0 goes to infinity (if $\theta = (m_0 - 1)/m_0$ then m_0^{θ}/m_0 would converge to 1 as m_0 goes to infinity and, therefore, the information rate would converge to 2).

In [8] it was shown that the GRS threshold scheme based on sequences of consecutive primes is asymptotically perfect when the secret is uniformly chosen. Following a similar proof line, we are able to show that this result also holds for a larger class of GRS threshold schemes, namely for GRS threshold schemes based on (t, Θ)-compact sequences of co-primes.

Theorem 13. *Let $0 < t + 1 \leqslant n$ and $\Theta \in (0, 1)$. Then, the GRS $(t + 1, n)$-threshold scheme based on (t, Θ)-compact sequences of co-primes is asymptotically perfect with respect to the uniform distribution on the secret space.*

Proof. Let $0 < t + 1 \leqslant n$ be positive integers, $m_0 < \cdots < m_n$ be a (t, Θ)-compact sequence of co-primes, and $I \subseteq \{1, \ldots, n\}$ with $|I| \leqslant t$. 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 10 and by using the inequalities $x - 1 < \lfloor x \rfloor \leqslant x$, one obtains

$$\Delta(y_I) \leqslant \log \frac{m_0 m_1 \cdots m_t + (m_0 + 1)\prod_{i \in I} m_i}{m_0 m_1 \cdots m_t - \prod_{i \in I} m_i}$$

As $m_0 < m_i < m_0 + m_0^{\theta}$ for any $1 \leqslant i \leqslant n$, and $|I| < t$, the fraction in the right hand side of the above inequality goes to 1 as m_0 goes to infinity (remark that θ cannot go to 1 as m_0 goes to infinity due to the fact that $\theta \leqslant \Theta < 1$ and Θ is fixed). This shows that for any $\epsilon > 0$ there exists m such that $\Delta(y_I) < \epsilon$ if $m_0 \geqslant m$. Moreover, according to Remark 12, there exist (t, Θ)-compact sequences of co-primes of length $n + 1$ whose first element is greater than or equal to m.

Case 2: $I = \{1, \ldots, t\}$. For any $S \in \mathbb{Z}_{m_0}$, we have $P(X = S | Y_I = y_I) = 1/m_0$. Therefore,

$$\Delta(y_I) = H(X) - H(X|Y_I = y_I) = \log m_0 - \sum_{S \in \mathbb{Z}_{m_0}} P(X = S|Y_I = y_I) \log \frac{1}{P(X = S|Y_I = y_I)} = 0$$

Case 3: $|I| = t$ and $I \neq \{1, \ldots, t\}$. Then,

$$m_0 \frac{m_1 \cdots m_t}{\prod_{i \in I} m_i} \leqslant m_0 \frac{m_t}{m_{t+1}} \leqslant m_0 \frac{m_t}{m_t + 2}$$

As $m_t \leqslant m_n - 2 < m_0 + m_0^{\theta} - 2 < 2m_0 - 2$, 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 10 and by using the inequality $x - 1 < \lfloor x \rfloor$ it follows

$$\Delta(y_I) \leqslant \log \frac{m_0}{C(I)} \leqslant \log \frac{m_0 \prod_{i \in I} m_i}{m_0 m_1 \cdots m_t - \prod_{i \in I} m_i}$$

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. □

According to [8], the *GRS* $(t+1, n)$-threshold scheme is called *asymptotically ideal* if it is asymptotically perfect and for any $\epsilon > 0$ there exists $m \geqslant 0$ such that for any sequence $m_0 < m_1 < \cdots < m_n$ of co-primes with $m_0 \geqslant m$ and any $1 \leqslant i \leqslant n$ the following holds:

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

($|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}|$ is the *information rate* of the ith participant).

In [8] it was shown that the GRS threshold scheme based on sequences of consecutive primes is asymptotically ideal when the secret is uniformly chosen. This result holds for instances based on (t, Θ)-compact sequences of co-primes as the following theorem shows.

Theorem 14. *Let $0 < t+1 \leqslant n$ and $\Theta \in (0, 1)$. Then, the GRS $(t+1, n)$-threshold scheme based on (t, Θ)-compact sequences of co-primes is asymptotically ideal with respect to the uniform distribution on the secret space.*

Proof. Let $m_0 < \cdots < m_n$ be a compact sequence of co-primes such that $m_n < m_0 + m_0^{\theta}$ for some $\theta \in (0, \Theta]$. Then,

$$\frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} = \frac{m_i}{m_0} < \frac{m_0 + m_0^{\theta}}{m_0} \leqslant \frac{m_0 + m_0^{\Theta}}{m_0}$$

for any $1 \leqslant i \leqslant n$. The right hand side of the last inequality goes to 1 as m_0 goes to infinity (remark that θ cannot go to 1 as m_0 goes to infinity due to the fact that $\theta \leqslant \Theta < 1$ and Θ is fixed). Therefore, for any $\epsilon > 0$ there exists m such that $|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}| < 1 + \epsilon$ if $m_0 \geqslant m$. Moreover, according to Remark 12, there exist (t, Θ)-compact sequences of co-primes of length $n+1$ whose first element is greater than or equal to m. □

Given a scheme $GRS(t, n, m_0, \ldots, m_n)$, $S \in \mathbb{Z}_{m_0}$, and a non-empty set $I \subseteq \{1, \ldots, n\}$, consider the random variable $Y_{S,I}$ which takes values $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ as possible shares for all $i \in I$ in the same process of sharing S.

According to [8], the *GRS* $(t+1, n)$-threshold scheme is called *perfect zero-knowledge* if, for any polynomial *poly* there exists $m \geqslant 0$ such that for any sequence $m_0 < m_1 < \cdots < m_n$ of co-primes with $m_0 \geqslant m$, any $S, S' \in \mathbb{Z}_{m_0}$, and any non-empty set $I \subseteq \{1, \ldots, n\}$ with $|I| \leqslant t$, the following holds:

$$\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{S,I} = y_I) - P(Y_{S',I} = y_I)| \leqslant \frac{1}{poly(m_0)} \tag{4}$$

That is, it is indistinguishable whether the shares $y_I = (y_i | i \in I)$ come from S or from S'.

In [8] it was shown that the GRS threshold scheme based on sequences of consecutive primes is perfect zero-knowledge when the secret is uniformly chosen. Following a similar proof line, we are able to show that this result also holds for instances based on (t, Θ)-compact sequences of co-primes.

Theorem 15. *Let $0 < t+1 \leqslant n$ and $\Theta \in (0, 1)$. Then, the GRS $(t+1, n)$-threshold scheme based on (t, Θ)-compact sequences of co-primes is perfect zero-knowledge with respect to the uniform distribution on the secret space.*

Proof. Let $0 < t+1 \leqslant n$ be positive integers, $m_0 < \cdots < m_n$ be a (t, Θ)-compact sequence of co-primes, $S, S' \in \mathbb{Z}_{m_0}$, and $I \subseteq \{1, \ldots, n\}$ with $|I| \leqslant t$.

If we denote by U_I a uniform random variable which takes values in $\prod_{i \in I} \mathbb{Z}_{m_i}$, then:

$$|P(Y_{S,I} = y_I) - P(Y_{S',I} = y_I)| \leqslant |P(Y_{S,I} = y_I) - P(U_I = y_I)| + |P(Y_{S',I} = y_I) - P(U_I = y_I)|$$

One can see now that, in order to prove (4), it is sufficient to look for a suitable upper bound for the term

$$\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{S,I} = y_I) - P(U_I = y_I)|$$

Due to the fact that there exists an isomorphism h from $\prod_{i \in I} \mathbb{Z}_{m_i}$ to $\mathbb{Z}_{\prod_{i \in I} m_i}$, 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 $h(y_I)$ with probability p. Based on the property that for any $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ there exists a unique $r \in \mathbb{Z}_{\prod_{i \in I} m_i}$ such that $y_i = (S + r \cdot m_0) \bmod m_i$ for all $i \in I$, we can define a random variable R_S with values into $\mathbb{Z}_{\prod_{i=1}^{t} m_i}$ and such that

$$\sum_{y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}} |P(Y_{S,I} = y_I) - P(U_I = y_I)| = \sum_{r \in \mathbb{Z}_{\prod_{i \in I} m_i}} |P(R_S \bmod \prod_{i \in I} m_i = r) - P(Z_I = r)|$$

To simplify the notation let $M_t = \prod_{i=1}^{t} m_i$ and $M_I = \prod_{i \in I} m_i$. Now, if $0 \leqslant r < (M_t \bmod M_I)$, then

$$P(R_S mod M_I = r) = \frac{\frac{M_t - (M_t \bmod M_I)}{M_I} + 1}{M_t}$$

and if $(M_t \bmod M_I) \leqslant r < M_I$ then

$$P(R_S \bmod M_I = r) = \frac{M_t - (M_t \bmod M_I)}{M_t M_I}$$

Combining these with $P(Z_I = r) = 1/M_I$, we obtain

$$\sum_{r \in \mathbb{Z}_{M_I}} |P(R_S \bmod M_I = r) - P(Z_I = r)| = 2\left(\frac{M_t \bmod M_I}{M_t} - \frac{(M_t \bmod M_I)^2}{M_t M_I}\right)$$

If $|I| = t$, then $M_I \geqslant M_t$. If $|I| < t$, then $M_I < m_0^t < M_t$ for sufficiently large m_0 because $m_0 < \cdots < m_n$ is a (t, Θ)-compact sequence of co-primes. From these, the result of the theorem easily follows. □

4. Security of the Asmuth-Bloom threshold scheme

The $(t + 1, n)$-threshold scheme proposed in [1], called from now on the *Asmuth-Bloom threshold scheme*, can be described using the formalism of Section 3 as follows:

- the sequence of co-primes $m_0 < m_1 < \cdots < m_n$ is subject to the constraint

$$\prod_{i=1}^{t+1} m_i > m_0 \prod_{i=0}^{t-1} m_{n-i} \tag{5}$$

- the secret space is $\mathbf{Z}_{m_0}$ and the share space of the ith participant is $\mathbb{Z}_{m_i}$, for all $1 \leqslant i \leqslant n$;
- $S' = S + rm_0$ for any secret S, where r is randomly chosen such that $S' < \prod_{i=1}^{t+1} m_i$.

We will discuss on the asymptotic perfectness of the Asmuth-Bloom threshold scheme. The loss of entropy $\Delta(y_I)$ in this scheme satisfies the same relations as those in Lemma 10 but with the difference that in this case $C(I)$ is given by

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

Let $I \subseteq \{1, \ldots, n\}$ be a non-empty subset of cardinal at most t. Two cases are to be considered:

Case 1: $|I| < t$. From Lemma 10 and by using $x - 1 < \lfloor x \rfloor \leqslant x$ we obtain

$$\Delta(y_I) \leqslant \log \frac{m_1 m_2 \cdots m_{t+1} + (m_0 + 1)\prod_{i \in I} m_i}{m_1 m_2 \cdots m_{t+1} - \prod_{i \in I} m_i}$$

From $|I| < t$ and (5) we deduce $\prod_{i=1}^{t+1} m_i > m_0^2 \prod_{i \in I} m_i$ and, therefore,

$$\Delta(y_I) < \log \frac{m_0^2 + m_0 + 1}{m_0^2 - 1}$$

As the fraction on the right hand side of the above inequality goes to 1 as m_0 goes to infinity, we have $\Delta(y_I) < \epsilon$ for any $\epsilon > 0$ and sufficiently large m_0.

Case 2: $|I| = t$. From (5) and Lemma 10 we easily obtain $m_0 < C(I) \leqslant m_{t+1}$ from which follows

$$\Delta(y_I) \leqslant \log \frac{m_0\left(\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1\right)}{C(I)} \leqslant \log \frac{C(I) + m_0 + 1}{C(I)} < \log\left(2 + \frac{1}{m_0}\right)$$

As one can see, the loss of entropy in the Asmuth-Bloom threshold scheme is upper bounded by a quantity which goes to log 2 as m_0 goes to infinity.

As the Asmuth-Bloom threshold scheme allows arbitrarily large gaps between m_0 and m_i, the information rate of the ith participant can be arbitrarily large, for any $1 \leqslant i \leqslant n$. One can also see that the Asmuth-Bloom threshold scheme is not perfect zero-knowledge.

If supplementary constraints are imposed regarding the "compactness" of the sub-sequence $m_1 < \cdots < m_n$, the Asmuth-Bloom threshold scheme can be transformed into an asymptotically perfect threshold scheme whose information rate converges to 2.

Definition 16. Let $\Theta \in (0, 1)$ be a real number. A sequence $m_0 < m_1 < \cdots < m_n$ of co-primes is called *almost Θ-compact* if $m_i \in (x, x + x^\theta)$ for all $1 \leqslant i \leqslant n$, where $\lceil x + x^\theta \rceil = 2m_0 - 2$ and $\theta \in (0, \Theta]$.

As we can see, an almost Θ-compact sequence $m_0 < m_1 < \cdots < m_n$ has the property that $m_1 < \cdots < m_n$ is a compact sequence of co-primes in the interval $(x, x + x^\theta)$, where x linearly depends on m_0. Also note that, for large enough m_0, the sequence $m_0 < m_1 < \cdots < m_n$ satisfies the constraint imposed by the Asmuth-Bloom threshold scheme. Indeed, for small enough $\epsilon > 0$ and large enough m_0 we have $m_1 > (1+\epsilon)m_0$ and $(1+\epsilon)\prod_{i=2}^{t+1} m_i > \prod_{i=0}^{t-1} m_{n-i}$, which shows that $\prod_{i=1}^{t+1} m_i > m_0 \prod_{i=0}^{t-1} m_{n-i}$.

All the results we prove below hold if we replace "$\lceil x + x^\theta \rceil = 2m_0 - 2$" by "$\lceil x + x^\theta \rceil = km_0 - 2$" in Definition 16, for any fixed integer $k \geqslant 2$. As a consequence, the information rate would converge to k instead of 2.

Theorem 17. *Let $0 < t+1 \leqslant n$ and $\Theta \in (0, 1)$. The Asmuth-Bloom $(t+1, n)$-threshold scheme based on almost Θ-compact sequences is asymptotically perfect if the secret is chosen uniformly from the secret space. Moreover, the information rate converges to 2.*

Proof. According to the discussion above, the only case we have to consider is $|I| = t$. In this case we have $C(I) \leqslant m_{t+1} < 2m_0 - 2$ and $\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor \leqslant 1$, for large enough m_0. Therefore,

$$\Delta(y_I) \leqslant \log \frac{m_0\left(\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1\right)}{C(I)} \leqslant \log \frac{2m_0}{C(I)}$$

Due to the fact that $x < m_i < x + x^\theta \leqslant 2m_0 - 2$, the right hand side of the above equality goes to 0 as m_0 goes to infinity. Therefore, the Asmuth-Bloom $(t+1, n)$-threshold scheme based on almost Θ-compact sequences is asymptotically perfect.

The result regarding the information rate follows directly from the definition of almost Θ-compactness. □

Theorem 18. *Let $0 < t+1 \leqslant n$ and $\Theta \in (0, 1)$. The Asmuth-Bloom $(t+1, n)$-threshold scheme based on almost Θ-compact sequences is perfect zero-knowledge if the secret is chosen uniformly from the secret space.*

Proof. This is similar to the proof of Theorem 15 but with the following differences:

- "(t, Θ)-compact" should be replaced by "almost Θ-compact";
- the random variable R_S takes values into $\mathbb{Z}_{\left\lfloor \prod_{i=1}^{t+1} m_i/m_0 \right\rfloor}$;
- $M_t = \left\lfloor \prod_{i=1}^{t+1} m_i/m_0 \right\rfloor$;
- in the last paragraph of the proof of Theorem 15, "$M_I \geqslant M_t$" should be replaced by "$M_I < M_t$", and "$M_I < m_0^t < M_t$", by "$M_I < m_1^t < M_t$".

All the other relations and conclusions in the proof of Theorem 15 remain unchanged. □

One may also try to use compact sequences of co-primes in the Asmuth-Bloom threshold scheme, instead of almost compact sequences of co-primes. However, it seems that the compactness property of a sequence of co-primes is not compatible with the constraint imposed by the Asmuth-Bloom threshold scheme (in the sense that either of them invalidates the other one). In such a case, one may try to use compact sequences in the Asmuth-Bloom threshold scheme and disregard the constraint imposed by this scheme. If this is the case, following a similar reasoning as above, one can prove the following results:

1. for any $\epsilon > 0$ and sufficiently large m_0, the loss of entropy satisfies $\Delta(y_I) \leqslant \log 2 + \epsilon$;
2. for any $\epsilon > 0$ and sufficiently large m_0, the information rate of the ith participant is less than $1 + \epsilon$, for any $1 \leqslant i \leqslant n$;
3. the scheme is perfect zero-knowledge.

Let us consider now the following variant of the Asmuth-Bloom $(t+1, n)$-threshold scheme:

- $m_0 < \cdots < m_n$ is a compact sequence of co-primes;
- the secret space is $\mathbb{Z}_{m_n}$ and the share space of the ith participant is $\mathbb{Z}_{m_i}$, for all $0 \leqslant i < n$;
- a secret S is shared among participants by computing first $S' = S + rm_n < \prod_{i=0}^{t} m_i$ for some random r, and then $S_i = S' \bmod m_i$ for all $0 \leqslant i < n$.

It is interesting to see then that this variant of the Asmuth-Bloom threshold scheme is asymptotically ideal and perfect zero-knowledge if it is based on compact sequences of co-primes (the asymptotic idealness of this variant of the Asmuth-Bloom threshold scheme is understood by the fact that the scheme is asymptotically perfect and the information rate $|\mathbb{Z}_{m_i}| / |\mathbb{Z}_{m_n}|$ goes to 1 as m_0 goes to infinity, for all $0 \leqslant i \leqslant n-1$).

Theorem 19. *Let $0 < t + 1 \leqslant n$ and $\Theta \in (0, 1)$. The above variant of the Asmuth-Bloom $(t + 1, n)$-threshold scheme based on $(n - 1, \Theta)$-compact sequences of co-primes is asymptotically ideal and perfect zero-knowledge if the secret is chosen uniformly from the secret space.*

Proof. This simply parallels the other proofs in the paper. We just mention that $C(I) \leqslant m_t$ and

$$\left\lfloor \frac{C(I)+1}{m_n} \right\rfloor = 0$$

if $|I| = t$. □

5. Security of the Mignotte threshold scheme

The threshold scheme proposed in [6], called from now on the *Mignotte threshold scheme*, can be described using the formalism at the beginning of Section 3 as follows:

- the sequences of co-primes $m_0 < m_1 < \cdots < m_n$ is subject to the constraint $\alpha \leqslant \beta$, where $\alpha = 1 + \prod_{i=0}^{t-1} m_{n-i}$ and $\beta = \prod_{i=1}^{t+1} m_i$;
- the secret space is $[\alpha, \beta)$, and the share space of the ith participant is $\mathbb{Z}_{m_i}$, for all $1 \leqslant i \leqslant n$;
- $S' = S$, for any secret $S \in [\alpha, \beta)$.

Remark that m_0 is not used in the Mignotte threshold scheme and, therefore, it can be omitted in our discussion below.

Our aim is to study the security of the Mignotte scheme when it is based on compact sequences of co-primes and the secret is uniformly chosen from the secret space. The first remark is that the compactness property of a sequence of co-primes is compatible with the constraints $\alpha \leqslant \beta$ in the sense that for large m_1, if $m_1 < \cdots < m_n$ is compact then it also satisfies $\alpha \leqslant \beta$. This can be easily seen from the fact that $\alpha = \mathcal{O}(m_1^t)$ and $\beta = \mathcal{O}(m_1^{t+1})$.

As with respect to asymptotic perfectness, let us consider a non-empty set $I \subseteq \{1, \ldots, n\}$ of cardinal at most t. By CRT, the system

$$x \equiv S_i \bmod m_i, \quad i \in I \tag{6}$$

has a unique solution x_0 in $\mathbb{Z}_{\prod_{i\in I} m_i}$. Therefore, the secret S should be of the form $S = x_0 + j\prod_{i\in I} m_i$, where j satisfies

$$\left\lfloor \frac{\alpha - x_0}{\prod_{i\in I} m_i} \right\rfloor < j \leqslant \left\lfloor \frac{\beta - x_0}{\prod_{i\in I} m_i} \right\rfloor$$

This means that j can take at most $\lfloor(\beta - \alpha + \prod_{i\in I} m_i)/\prod_{i\in I} m_i\rfloor$ and at least $\lfloor(\beta - \alpha - \prod_{i\in I} m_i)/\prod_{i\in I} m_i\rfloor$ values.

Consider now the loss of entropy $\Delta(y_I)$. Remark first that

$$P(X = S | Y_I = y_I) \geqslant \frac{1}{\left\lfloor \frac{\beta-\alpha+\prod_{i\in I} m_i}{\prod_{i\in I} m_i} \right\rfloor}$$

because j can take at most $\lfloor(\beta - \alpha + \prod_{i\in I} m_i)/\prod_{i\in I} m_i\rfloor$ values. Combining this with the fact that $P(X = S|Y_I = y_I)$ defines a probability distribution over $\prod_{i\in I}\mathbb{Z}_{m_i}$, one can obtain

$$\Delta(y_I) \geqslant \log(\beta - \alpha - 1) - \log\left\lfloor \frac{\beta - \alpha + \prod_{i\in I} m_i}{\prod_{i\in I} m_i} \right\rfloor = \log \frac{\beta - \alpha - 1}{\left\lfloor \frac{\beta-\alpha+\prod_{i\in I} m_i}{\prod_{i\in I} m_i} \right\rfloor}$$

It is rather trivial to observe that the right hand side of the above inequality goes to infinity as m_1 goes to infinity, because the numerator of the fraction is $\mathcal{O}(m_1^{t+1})$ while the denominator is $\mathcal{O}\left(m_1^{t+1-|I|}\right)$. As the loss of entropy cannot be bounded, we must conclude that the scheme is not asymptotically perfect.

As with respect to the asymptotic idealness of the Mignotte threshold scheme based on compact sequences of co-primes, one can see that the secret space is of size $\mathcal{O}(m_1^{t+1})$. This leads immediately to the fact that the information rate $m_i/(\beta - \alpha - 1)$ of the ith participant converges to 0 as m_1 goes to infinity. As a conclusion, the Mignotte threshold scheme is far from asymptotically ideal.

The Mignotte threshold scheme is not perfect zero-knowledge. Indeed, if we consider S and S' two distinct secrets and $I \subseteq \{1, \ldots, n\}$ with $|I| \leqslant t$, then

$$\sum_{y_I \in \prod_{i\in I}\mathbb{Z}_{m_i}} |P(Y_{S,I} = y_I) - P(Y_{S',I} = y_I)| = 2$$

which proves our claim.

Although the Mignotte threshold scheme does not satisfy any of the canonical security properties, some degree of security is provided. According to our discussion above about perfectness, the entropy of the secret when $|I| \leqslant t$ shares are pulled together is roughly

$$(t + 1 - |I|) \log m_1 \geqslant \log m_1$$

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).

6. Conclusions

In spite of the fact that the CRT-based threshold schemes proposed so far [1,6,5] are not perfect (and, therefore, not ideal), they assure some degree of security. Quisquater et al. have introduced in [8] two appropriate concepts, *asymptotic perfectness* and *asymptotic idealness*, to be used in order to evaluate the security of such schemes. Thus, they showed that the GRS threshold scheme [5] 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 [5], 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 [5]). If the primes are consecutive and large enough, as it was used in [8], they may be considered of the same magnitude. However, "same magnitude" should mean more than "consecutive primes". Starting from this remark, the aim of this paper was to define in a proper way the concept "same magnitude" and to study the security of the threshold schemes in [1,6,5] when they are based on sequences of co-primes of the same magnitude. A sequence of co-primes of the same magnitude has its elements in an interval of the form $(x, x + x^{\theta})$ for some positive integer x and real number $\theta \in (0, 1)$. Such sequences were called in our paper *compact sequences of co-primes*. We have proved that

- sequences of consecutive primes or consecutive co-primes are particular cases of compact sequences of co-primes;
- we can find arbitrarily long compact sequences of arbitrarily large co-primes, and
- any sequence of consecutive primes in an interval covers a denser sequence of co-primes in the same interval.

Then, we have shown that the GRS threshold scheme [5] is asymptotically ideal and perfect zero-knowledge if it is based on compact sequences of co-primes and the secret is uniformly chosen.

This paper also contributes to the understanding of the security of the Asmuth-Bloom threshold scheme [1] and Mignotte threshold scheme [6]. The Asmuth-Bloom threshold scheme based on arbitrary sequences of co-primes is not asymptotically perfect and its information rate can be arbitrarily large. When almost Θ-compact sequences are used, the Asmuth-Bloom threshold scheme becomes asymptotically perfect, its information rate converges to 2, and it is perfect zero-knowledge.

Our study indicates that the compactness property of a sequence of co-primes is incompatible with the Asmuth-Bloom constraint in the sense that the compactness property invalidates the Asmuth-Bloom constraint and vice versa. Therefore, the Asmuth-Bloom threshold scheme cannot be used with compact sequences of co-primes. In such a case, one may try to use compact sequences in the Asmuth-Bloom threshold scheme and disregard the constraint imposed by this scheme. The threshold scheme obtained is perfect zero-knowledge, its loss of entropy converges to 0 (when at most $t - 1$ shared are pulled together) or it is upper bounded by a quantity which converges to log 2 (when t shares are pulled together), and its information rate converges to 1. If one would further modify the threshold scheme above by changing the secret space from $\mathbb{Z}_{m_0}$ to $\mathbb{Z}_{m_n}$ (and considering the share spaces $\mathbb{Z}_{m_0}, \ldots, \mathbb{Z}_{m_{n-1}}$), the newly obtained $(t + 1, n)$-threshold scheme would be asymptotically ideal and perfect zero-knowledge if it was based on $(n - 1, \Theta)$-compact sequences of co-primes (and the secret was uniformly chosen from the secret space).

As with respect to the Mignotte secret sharing scheme, even if this scheme uses 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.

The security results obtained in this paper on CRT-based threshold schemes are mainly based on (t, Θ)-compact sequences of co-primes. The constraint referring to t means that $m_{t+1} \geqslant m_t + 2$ (Definition 11). We believe that this constraint can be removed by using better upper bounds for the loss of entropy.

It is our opinion that the class of compact sequences of co-primes is the largest class of sequences of co-primes under which the GRS and Asmuth-Bloom threshold schemes meet the security properties discussed in the paper.

References

[1] C.A. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Transactions on Information Theory 29 (1983) 208–210. The paper was presented at the National Telecommunications Conference, Houston, December 1980.
[2] R. Baker, G. Harman, The difference between consecutive primes, Proceedings of the London Mathematical Society 72 (1996) 261–280.

[3] G. Blakley, Safeguarding cryptographic keys, in: 1979 AFIPS National Computer Conference, AFIPS Press, 1979, pp. 313–317.
[4] C. Ding, D. Pei, A. Salomaa, Chinese Remainder Theorem, Applications in Computing, Coding, Cryptography, World Scientific Publishing, 1996.
[5] O. Goldreich, D. Ron, M. Sudan, Chinese remaindering with errors, IEEE Transactions on Information Theory 46 (2000) 1330–1338.
[6] M. Mignotte, How to share a secret? in: T. Beth (Ed.), Workshop on Cryptography, Lecture Notes in Computer Science, vol. 149, Burg Feuerstein, 1982, pp. 371–375.
[7] L. Panaitopol, Some of the properties of the sequence of powers of prime numbers, Rocky Mountain Journal of Mathematics 31 (2001) 1407–1415.
[8] M. Quisquater, B. Preneel, J. Vandewalle, On the security of the threshold scheme based on the Chinese remainder theorem, in: D. Naccache, P. Paillier (Eds.), Public Key Cryptography, Lecture Notes in Computer Science, vol. 2274, Springer, 2002, pp. 199–210.
[9] P. Ribenboim, The New Book of Prime Number Record, third ed., Springer-Verlag, 1996.
[10] A. Shamir, How to share a secret, Communications of the ACM 22 (1979) 612–613.