Information Processing Letters 114 (2014) 299–303

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme

Ferucio Laurenţiu Ţiplea *, Constantin Cătălin Drăgan [1]

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

ARTICLE INFO

Article history:
Received 8 April 2013
Received in revised form 2 September 2013
Accepted 21 January 2014
Available online 23 January 2014
Communicated by V. Rijmen

Keywords:
Cryptography
Secret sharing scheme
Chinese Remainder Theorem
Entropy
(Asymptotic) perfectness
(Asymptotic) idealness

ABSTRACT

The study of the asymptotic idealness of the Goldreich–Ron–Sudan (GRS, for short) threshold secret sharing scheme was the subject of several research papers, where sufficient conditions were provided. In this paper a necessary and sufficient condition is established; namely, it is shown that the GRS threshold secret sharing scheme is asymptotically ideal under the uniform distribution on the secret space if and only if it is based on *1-compact sequences of co-primes*.

1. Introduction

The Chinese Remainder Theorem (CRT) is a very useful tool in many areas of theoretical and practical cryptography. One of these areas is the theory of threshold secret sharing schemes. A $(t+1,n)$-threshold secret sharing scheme ($(t+1,n)$-threshold scheme, for short) is a method of partitioning a secret among n users by providing each user with a share of the secret such that any $t+1$ users can uniquely reconstruct the secret by pulling together their shares. Several threshold schemes based on CRT are known [1–3]. These schemes use sequences of pairwise co-prime positive integers with special properties. The shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders. The secret can be reconstructed by some sufficient number of shares by using CRT.

In order to study the security of the CRT-based threshold secret sharing schemes, Quisquater et al. [4] have introduced the concepts of *asymptotic perfectness* and *asymptotic idealness*, and proved that the Goldreich–Ron–Sudan (GRS) threshold scheme in [3] is asymptotically ideal (and, therefore, asymptotically perfect) under the uniform distribution on the secret space, provided that it uses sequences of consecutive primes. This result was later improved [5] by showing that the asymptotic idealness of this scheme is achieved not only for the class of sequences of consecutive primes but also for a larger class of sequences of co-primes, namely for the class of (t,Θ)-compact sequences of co-primes, where t defines the scheme threshold and Θ is any arbitrary real number in the interval $(0,1)$.

1.1. Contribution

Compact sequences of co-primes were introduced in [5] in an attempt to formalize the idea of sequences of positive integers of the "same magnitude" [3]. Both sequences of consecutive primes and (t,Θ)-compact sequences of co-primes are particular cases of compact sequences of co-

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

[1] 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].

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2014.01.008

primes [5]. Moreover, compact sequences of co-primes are much denser than sequences of consecutive primes [5]. Therefore, the results in [4] and [5] show that the GRS threshold scheme is asymptotically ideal under the uniform distribution on the secret space if it is based on some subclasses of the class of compact sequences of co-primes. In this context, the question is whether these results can be extended to the entire class of compact sequences of co-primes. Our paper answers this question. We introduce first the class of 1-compact sequences of co-primes as an extension of the class of compact sequences of co-primes and then we show that the GRS threshold scheme is asymptotically ideal under the uniform distribution on the secret space if and only of it is based on 1-compact sequences of co-primes.

We believe that our result is important from two points of view: first, it closes completely the security problem of the GRS threshold scheme, and secondly it emphasizes the importance of 1-compact sequences of co-primes in studying the security of the CRT-based threshold secret sharing schemes. Moreover, as far as we are concerned, this is the first time a necessary and sufficient condition for the asymptotic idealness of a CRT-based threshold secret sharing scheme is established.

2. The main result

In this section we recall the GRS threshold scheme [3] and then we prove our main result, namely that the GRS threshold scheme is asymptotically ideal under the uniform distribution on the secret space if and only if it is based on 1-compact sequences of co-primes.

2.1. The GRS scheme

Throughout this paper, $\mathbb{Z}$ stands for the set of 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.

The *Chinese Remainder Theorem* (CRT, for short) [6] states that the system of congruences

$$x\equiv b_i \bmod m_i,\quad i\in I, \tag{1}$$

where I is a finite non-empty set of positive integers 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 [1–3]. Given t and n positive integers with $0<t+1\leqslant n$, the GRS $(t+1,n)$-threshold scheme in [3] is defined as follows:

(1) *Parameter setup*: consider $m_0<m_1<\cdots<m_n$ a *sequence of co-primes* (that is, $m_0,m_1,\ldots,m_n$ are pairwise co-prime strictly positive integers in increasing order). The integers $t,n,m_0,m_1,\ldots,m_n$ are public parameters;

(2) *Secret and share spaces*: define the *secret space* as being $\mathbb{Z}_{m_0}$ and the *share space* of the ith participant as being $\mathbb{Z}_{m_i}$, for all $1\leqslant i\leqslant n$;

(3) *Secret sharing*: given a secret s in the secret space, share it by $s_i=s' \bmod m_i$, for all $1\leqslant i\leqslant n$, where s' is the unique solution modulo $m_0\prod_{i=1}^{t} m_i$ of the system

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

where $r_0=s$ and r_i is randomly chosen from $\mathbb{Z}_{m_i}$ for all $1\leqslant i\leqslant t$;

(4) *secret reconstruction*: 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

$$x\equiv s_{i_j} \bmod m_{i_j},\quad 1\leqslant j\leqslant t+1,$$

and then reducing it modulo m_0.

The correctness of the reconstruction step above is as follows: by solving the system of congruences from the step (4) one obtains the unique solution s' modulo $\prod_{j=1}^{t+1} m_{i_j}$. As $\prod_{j=1}^{t+1} m_{i_j} > m_0\prod_{i=1}^{t} m_i$ and s' is a solution to the system of congruences from the step (3) too, one obtains $s=s' \bmod m_0$.

2.2. Asymptotic idealness

Given the GRS $(t+1,n)$-threshold scheme, a sequence $m_0<m_1<\cdots<m_n$ of co-primes, and a non-empty set $I\subseteq\{1,\ldots,n\}$, consider X and Y_I two random variables associated to the secret space $\mathbb{Z}_{m_0}$ and to the combined share space $\prod_{i\in I}\mathbb{Z}_{m_i}$, respectively. For any $y_I\in\prod_{i\in I}\mathbb{Z}_{m_i}$, define the *loss of entropy with respect to* y_I [4], denoted $\Delta(y_I)$, by

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

where $H(X)$ stands for the entropy of X and $H(X|Y_I=y_I)$ stands for the entropy of X conditioned by $Y_I=y_I$.

The GRS $(t+1,n)$-threshold scheme is called *asymptotically perfect* [4] if for any non-empty subset $I\subseteq\{1,\ldots,n\}$ with $|I|\leqslant t$ 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 $m_0\geqslant m$, the following hold:

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

The GRS $(t+1,n)$-threshold scheme is called *asymptotically ideal* [4] 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 called the *information rate* of the ith participant.

Remark 1. One can easily see that the constraint "for any $\epsilon>0$" in the concepts of asymptotic perfectness and idealness can be equivalently replaced by "for any $0<\epsilon<1$".

It was shown in [4] that the GRS $(t+1,n)$-threshold scheme based on sequences of consecutive primes is asymptotically ideal with respect to the uniform distribution on the secret space. This result was improved in [5] by showing that the asymptotic idealness is preserved even if the scheme is based on (t,Θ)-compact sequences of co-primes which are denser than sequences of consecutive primes. Recall that a sequence $m_0 < m_1 < \cdots < m_n$ of co-primes is (t,Θ)-*compact* [5], where $\Theta \in (0,1)$, if $m_{t+1} \geqslant m_t + 2$ and $m_n < m_0 + m_0^\theta$ for some $\theta \in (0,\Theta]$. The sequence $m_0 < m_1 < \cdots < m_n$ of co-primes is called *compact* [5] if there exists $\theta \in (0,1)$ such that $m_i < m_0 + m_0^\theta$ for all $1 \leqslant i \leqslant n$.

Both sequences of consecutive primes and (t,Θ)-compact sequences of co-primes are particular cases of compact sequences of co-primes. Moreover, compact sequences of co-primes are much denser than sequences of consecutive primes (the reader is referred to [5] for more details about these statements).

2.3. Our main result

As it was defined in [3] and used in all subsequent papers, the GRS $(t+1,n)$-threshold scheme is based on sequences $m_0 < m_1 < \cdots < m_n$ of co-primes. The integer m_0, which defines the secret space, is the first element in this sequence. This leads to the fact that all the participants have associated larger share spaces than the secret space. In this context one may think that it would be better to choose m_0 in the "middle" of the sequence $m_1 < \cdots < m_n$. This would allow for a balanced distribution of the share spaces around the secret space, resulting in a balanced distribution of the participants information rates around 1.

According to this discussion and taking into account the results in [5], consider the following concept.

Definition 2.

1. A sequence $m_0, m_1, \ldots, m_n$ of pairwise co-primes is called (k,θ)-*compact*, where $k \geqslant 1$ and $\theta \in (0,1)$ are real numbers, if $m_1 < \cdots < m_n$ and $km_0 - m_0^\theta < m_i < km_0 + m_0^\theta$ for all $1 \leqslant i \leqslant n$.
2. A sequence $m_0, m_1, \ldots, m_n$ of pairwise co-primes is called k-*compact* if it is (k,θ)-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. To emphasize this we will often write this sequence in the form $m_0, m_1 < \cdots < m_n$.

It is clear that compact sequences of co-primes as defined in [5] (see also the previous subsection) are particular cases of 1-compact sequences of co-primes.

Now, we say that the *GRS $(t+1,n)$-threshold scheme is based on k-compact sequences of co-primes* if the parameter setup phase in GRS is changed into

(1′) *Parameter setup:* consider $m_0, m_1 < \cdots < m_n$ a k-compact sequence of co-primes. The integers $t, n, m_0, m_1, \ldots, m_n$ are public parameters,

and the constraint "$s' < \prod_{i=1}^{t+1} m_i$" is added to the secret sharing phase.

The correctness of this new variant of the GRS threshold scheme is obtained exactly as for the original one, but the asymptotic perfectness and idealness concepts should be adapted correspondingly.

Definition 3. Let $0 < t+1 \leqslant n$ be positive integers and $k \geqslant 1$ be a real number.

1. We say that the GRS $(t+1,n)$-threshold scheme based on k-compact sequences of co-primes is *asymptotically perfect* if for any non-empty subset $I \subseteq \{1,\ldots,n\}$ with $|I| \leqslant t$, any $\theta \in (0,1)$ and any $\epsilon > 0$, there exists $m \geqslant 0$ such that for any (k,θ)-compact sequence of co-primes $m_0, m_1 < \cdots < m_n$ with $m_0 \geqslant m$, the following hold:
   - $H(X) \neq 0$;
   - $|\Delta(y_I)| < \epsilon$, for any $y_I \in \prod_{i\in I} \mathbb{Z}_{m_i}$.
2. We say that the information rate of the GRS $(t+1,n)$-threshold scheme based on k-compact sequences of co-primes *goes asymptotically to r* if for any $\theta \in (0,1)$ and $\epsilon \in (0,1)$ there exists $m \geqslant 0$ such that for any (k,θ)-compact sequence of co-primes $m_0, m_1 < \cdots < m_n$ with $m_0 \geqslant m$ and any $1 \leqslant i \leqslant n$ the following holds:
$$\left| \frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} - r \right| < \epsilon.$$
3. We say that the GRS $(t+1,n)$-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.

The following result is a straightforward adaptation of a similar result obtained in [4], for the case of the GRS threshold scheme based on k-compact sequences of co-primes.

Lemma 4. *(See [4].) The loss of entropy of the GRS $(t+1,n)$-threshold scheme with respect to the uniform distribution on the secret space satisfies the following relations*:

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

for any non-empty set $I \subseteq \{1,\ldots,n\}$, any sequence $m_0, m_1, \ldots, m_n$ of co-primes, and any $y_I \in \prod_{i\in I} \mathbb{Z}_{m_i}$, where

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

Now, we are in a position to prove our main result.

Theorem 5. *Let $0 < t+1 \leqslant n$ be positive integers and $k \geqslant 1$ be a real number. Then, the GRS $(t+1,n)$-threshold scheme, under the uniform distribution on the secret space, is asymptotically perfect and its information rate goes asymptotically to k if and only if it is based on k-compact sequences of co-primes.*

Proof. Assume first that the GRS $(t+1,n)$-threshold scheme is asymptotically perfect and its information rate goes asymptotically to k. Therefore, for any $\epsilon \in (0,1)$ 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:

$$km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0.$$

We prove that for any $\epsilon \in (0,1)$ there exists $\theta \in (0,1)$ such that $\epsilon m_0 \leqslant m_0^{\theta}$, where m_0 is as above. Indeed, if $\epsilon \in (m_0^{-1}, 1)$, then $\theta = 1 + \log_{m_0} \epsilon$ satisfies the required property. If $\epsilon \in (0, m_0^{-1})$, then any $\theta \in (0,1)$ satisfies the required property.

Therefore, any sequence $m_0, m_1 < \cdots < m_n$ of co-primes which satisfies $km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0$ for all $1 \leqslant i \leqslant n$ and some $\epsilon \in (0,1)$ will also satisfy

$$km_0 - m_0^{\theta} \leqslant km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0 \leqslant km_0 + m_0^{\theta},$$

where $\theta \in (0,1)$ is defined as above (it depends on ϵ and m_0). This says that $m_0, m_1 < \cdots < m_n$ is k-compact.

We prove now that the GRS $(t+1,n)$-threshold scheme, under the uniform distribution on the secret space, is asymptotically perfect and its information rate goes asymptotically to k if it is based on k-compact sequences of co-primes.

Asymptotic perfectness

Let $I \subseteq \{1,\ldots,n\}$ be a non-empty set with $|I| \leqslant t$, $\theta \in (0,1)$, and $m_0, m_1 < \cdots < m_n$ be a (k,θ)-compact sequence of co-primes. The following cases are to be considered.

Case 1: $|I| < t$. Using Lemma 4 we obtain

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

As $|I| < t$ and $km_0 - m_0^{\theta} < m_i < km_0 + m_0^{\theta}$ for all $1 \leqslant i \leqslant n$, the fraction in the right hand side of the above inequality goes to 1 as m_0 goes to infinity. This shows that for any $\epsilon \in (0,1)$ there exists m such that $\Delta(y_I) < \epsilon$ if $m_0 \geqslant m$.

Case 2: $m_0 < m_{t+1}$ and $I = \{1,\ldots,t\}$. As the secret is uniformly chosen from the secret space, it follows $P(X=s) = 1/m_0$ and, therefore,

$$H(X) = \sum_{s\in\mathbb{Z}_{m_0}} P(X=s)\log\frac{1}{P(X=s)} = \log m_0.$$

Let $x_0 \in \mathbb{Z}_{\prod_{i\in I} m_i}$ be the unique solution in $\mathbb{Z}_{\prod_{i\in I} m_i}$ obtained by using the Chinese Remainder Theorem over the shares of the participants in I. Let

$$B = \left\{ x \in \mathbb{Z}_{\prod_{i=0}^{t} m_i} \;\middle|\; x \equiv x_0 \bmod \prod_{i\in I} m_i \right\}.$$

Clearly, $|B| = m_0$. Given $s \in \mathbb{Z}_{m_0}$, there exists a unique $x \in B$ such that $s \equiv x \bmod m_0$. This is because the congruential equation

$$r\prod_{i\in I} m_i \equiv (s - x_0) \bmod m_0$$

has a unique solution in r modulo m_0 [6].

According to these, $P(X=s|Y_I=y_I) = 1/|B| = 1/m_0$. Therefore,

$$\begin{aligned}\Delta(y_I) &= H(X) - H(X|Y_I=y_I)\\ &= \log m_0\\ &\quad - \sum_{s\in\mathbb{Z}_{m_0}} P(X=s|Y_I=y_I)\log\frac{1}{P(X=s|Y_I=y_I)}\\ &= 0.\end{aligned}$$

Case 3: $m_0 < m_{t+1}$ and $|I| = t$ and $I \neq \{1,\ldots,t\}$. Then,

$$\begin{aligned}C(I) &< m_0\frac{m_1\cdots m_t}{\prod_{i\in I} m_i}\\ &\leqslant m_0\frac{m_t}{m_{t+1}}\\ &\leqslant m_0\frac{m_t}{m_t+1} = m_0\left(1 - \frac{1}{m_t+1}\right).\end{aligned}$$

As $m_t + 1 < km_0 + m_0^{\theta}$ and $C(I)$ is a positive integer it follows that

$$C(I) \leqslant m_0 - 1.$$

The following sub-cases are considered.

Case 3.1: $C(I) = m_0 - 1$. Let x_0 denote the unique solution modulo $\mathbb{Z}_{\prod_{i\in I} m_i}$ over the shares of the participants in I, and let

$$B = \left\{ x \in \mathbb{Z}_{\prod_{i=0}^{t} m_i} \;\middle|\; x \equiv x_0 \bmod \prod_{i\in I} m_i \right\}.$$

Let $x_0 + r\cdot\prod_{i\in I} m_i$ be an element in B. If $x_0 \leqslant m_1\cdots m_{t-1}(m_t+1-m_0)$ then $r \leqslant m_0 - 1$, otherwise $r \leqslant m_0 - 2$. Therefore, $m_0 - 1 \leqslant |B| \leqslant m_0$.

If $|B| = m_0$ then it follows $P(X=s|Y_I=y_I) = 1/m_0$ in a similar way to Case 2. If $|B| = m_0 - 1$, then there exists at most one $x \in B$ such that $s \equiv x \bmod m_0$, for each secret s. As a conclusion, $P(X=s|Y_I=y_I)$ is either $1/(m_0-1)$ or 0.

These facts lead to

$$\log(m_0 - 1) \leqslant H(X|Y_I=y_I) \leqslant \log m_0$$

and, therefore,

$$0 \leqslant \Delta(y_I) \leqslant \log\frac{m_0}{m_0-1}.$$

This shows that for any $\epsilon \in (0,1)$ there exists m such that $|\Delta(y_I)| < \epsilon$ if $m_0 \geqslant m$.

Case 3.2: $C(I) < m_0 - 1$. Based on Lemma 4 and on the inequality $x - 1 < \lfloor x \rfloor$ we obtain

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

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 as in the first case.

Case 4: $m_0 > m_{t+1}$ and $|I| = t$. Then,

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

As one can easily see, the same analysis as in Cases 3.1 and 3.2 can be carried here (with the same conclusions).

Information rate

The following inequalities hold for all $1 \leqslant i \leqslant n$ and any (k,θ)-compact sequence $m_0, m_1 < \cdots < m_n$ of co-primes

$$\frac{km_0 - m_0^{\theta}}{m_0} < \frac{|\mathbb{Z}_{m_i}|}{|\mathbb{Z}_{m_0}|} = \frac{m_i}{m_0} < \frac{km_0 + m_0^{\theta}}{m_0},$$

which show that the information rate goes to k as m_0 goes to infinity. □

Corollary 6. *Let $0 < t+1 \leqslant n$ be positive integers. Then, the GRS $(t+1,n)$-threshold scheme, under the uniform distribution on the secret space, is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes.*

Proof. This is the case $k=1$ in Theorem 5. □

Remark 7. Choosing $m_1 < \cdots < m_n$ in a compact interval centered at m_0, offers the maximum of optimality with respect to the information rates of the participants in a GRS $(t+1,n)$-threshold scheme.

3. Conclusions

The GRS threshold scheme [3] was shown asymptotically ideal under the uniform distribution on the secret space if it is based on sequences of consecutive primes [4] or (t,Θ)-compact sequences of co-primes [5]. Both sequences of consecutive primes and (t,Θ)-compact sequences of co-primes are particular cases of compact sequences of co-primes [5]. Therefore, the following natural question arises: is the GRS threshold scheme asymptotically ideal under the uniform distribution on the secret space if it is based on compact sequences of co-primes?

This paper provides a complete answer to the above question:

1. First, we have defined the class of 1-compact sequences of co-primes which includes the class of compact sequences of co-primes. In an 1-compact sequence of co-primes, the element m_0 which defines the secret space may have any position with respect to the other elements in the sequence. The main advantage of this consists of the fact that the information rates of the participants may be uniformly distributed around 1;
2. Then, we have proved that the GRS threshold scheme under the uniform distribution on the secret space is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes.

It is worth to mention that the GRS threshold scheme variant in Section 2.3 was chosen so that it fits with the mobility of the element m_0 within the 1-compact sequences of co-primes. If the element m_0 is the first element of the sequence (as it was generally considered until now) then no modification is needed in the GRS threshold scheme.

Theorem 5 in our paper completely closes the security analysis of the GRS threshold scheme. The only question one may still ask is about the convergence rate to perfectness and idealness.

References

[1] C.A. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Trans. Inf. Theory 29 (2) (1983) 208–210, The paper was presented at the National Telecommunications Conference, Houston, December 1980.
[2] M. Mignotte, How to share a secret?, in: T. Beth (Ed.), Workshop on Cryptography, Burg Feuerstein, in: Lect. Notes Comput. Sci., vol. 149, 1982, pp. 371–375.
[3] O. Goldreich, D. Ron, M. Sudan, Chinese remaindering with errors, IEEE Trans. Inf. Theory 46 (4) (2000) 1330–1338.
[4] 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, in: Lect. Notes Comput. Sci., vol. 2274, Springer, 2002, pp. 199–210.
[5] M. Barzu, F.L. Ţiplea, C.C. Drăgan, Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes, Inf. Sci. 240 (2013) 161–172.
[6] C. Ding, D. Pei, A. Salomaa, Chinese Remainder Theorem. Applications in Computing, Coding, Cryptography, World Scientific Publishing, 1996.