On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme

Constantin Cătălin Drăgan * and Ferucio Laurenţiu Ţiplea

Department of Computer Science
"Al.I.Cuza" University of Iaşi
Iaşi 700506, Romania
e-mail: {fltiplea,constantin.dragan}@info.uaic.ro

Abstract. A necessary and sufficient condition for the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme is proposed. Apart from this, a comprehensive analysis of the known variants of the Asmuth-Bloom threshold secret sharing scheme is provided, clarifying the security properties achieved by each of them.

1 Introduction and Preliminaries

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. If less than $t+1$ shares give no information about the secret, from an information theoretic point of view, then the scheme is called *perfect*. In addition to this, if the share spaces have the same dimension with the secret space, the scheme is called *ideal*.

One of the techniques to construct threshold schemes is based on the Chinese Remainder Theorem (CRT) [1–5]. The main idea is to use sequences of pair-wise 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 CRT-based threshold schemes proposed so far are neither perfect nor ideal. However, they offer some security degree and, in order to study it, Quisquater et al. [6] have introduced the concepts of *asymptotic perfectness* and *asymptotic idealness*. They also proved that the threshold scheme in [3] is asymptotically ideal (and, therefore, asymptotically perfect) provided that it uses sequences of consecutive primes and the secret is uniformly chosen from the secret space. This result was later improved in [4] by showing that the asymptotic idealness of this scheme is achieved for a subclass of *compact sequences of co-primes* [4]. Compact sequences of co-primes capture very well the idea of sequence of numbers of the "same magnitude", and they are much denser than sequences of consecutive primes [4]. Moreover, [4] studies the security of the

* Constantin Cătălin Drăgan was 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]

Asmuth-Bloom threshold scheme [1] and also proposes some asymptotically perfect and ideal variants of it. Another variant of the Asmuth-Bloom threshold scheme was proposed in [7] which provides better security than the original Asmuth-Bloom threshold scheme.

Contribution This paper comes to complete a series of results regarding the security of CRT-based threshold schemes [6, 4, 5]. The main result of the paper is a necessary and sufficient characterization of the security of the Asmuth-Bloom threshold scheme (Theorem 1). Thus, we show that this scheme is asymptotically ideal with respect to the uniform distribution on the secret space if and only of it is based on *1-compact sequences of co-primes*. We believe that this result is important from two points of view: first, it closes completely the security problem of the Asmuth-Bloom threshold scheme, and secondly it emphasizes the importance of 1-compact sequences of co-primes in studying the security of the CRT-based secret sharing schemes. Apart from the above main result, our paper makes a comprehensive analysis of the Asmuth-Bloom threshold scheme variants proposed so far, clarifying and discussing the security properties achieved by each of them.

A similar characterization result to our Theorem 1 was obtained in [5] for the Goldreich-Ron-Sudan threshold scheme [3]. However, the proof of our Theorem 1 cannot be obtained as in [5] mainly because the estimate of the loss of entropy in [5] is to weak for the case of the Asmuth-Bloom threshold scheme (see also Section 4 in [4]). That is why in this paper we provide first a very precise estimate of the loss of entropy for the Asmuth-Bloom threshold scheme (Lemma 2), from which the upper bound in [6, 5] immediately follows.

Paper structure The paper is structured into six sections. The first one is an introduction to the theory of CRT-based threshold schemes. It also establishes the basic notation and terminology. The second section discusses the variants of the Asmuth-Bloom threshold scheme met in the literature. The basic security properties a CRT-based threshold scheme should fulfill are recalled in the third section. Moreover, an important result regarding the loss of entropy in a threshold scheme is also obtained. The fourth section establishes our main result regarding the security of the Asmuth-Bloom threshold scheme, while the fifth section clarifies the security of some variant of the Asmuth-Bloom threshold scheme. We conclude in Section 6.

Preliminaries Throughout this paper, $\mathbb{Z}$ stands for the set of integers. A positive integer $a > 1$ is a *prime* number if the only positive divisors of it are 1 and a. For two integers a and b, let (a, b) denote 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 $a \equiv b \mod n$, if n divides $a - b$ (n is an integer too). The notation $a = b \mod n$ means that a is the *remainder* of the integer division of b by n. The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$.

Given a random variable X with n outcomes $\{x_1, \ldots, x_n\}$, the (Shannon) *entropy* of X, denoted $H(X)$, is defined by

$$H(X) = \sum_{i=1}^{n} P(X = x_i) \log \frac{1}{P(X = x_i)}$$

with the mathematical convention $0 \log 0 = 0$ (here, $P(X = x_i)$ is the probability mass function of the outcome x_i, and the base of the logarithm is 2). Given two random variables X and Y, $H(X|Y)$ stands for the entropy of X conditioned by Y.

2 The Asmuth-Bloom secret sharing scheme and variations

Given a finite non-empty set I of positive integers and the integers b_i and m_i for all $i \in I$, the *Chinese Remainder Theorem* (CRT, for short) [8] states that the system of congruences

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

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 applications of CRT is the design of threshold schemes [2, 1, 3]. In this paper we will focus on the threshold scheme in [1] and some of its variants. As all of them are based on sequences of positive integers with special properties, we begin with a few notations and definitions regarding them.

A *sequence of co-primes* is a sequence

$$m_0, m_1, \ldots, m_n$$

of pair-wise co-prime strictly positive integers, where $n \geq 1$. The *length* of this sequence is $n + 1$.

Given two integers t and n with $0 < t+1 \leq n$, an *Asmuth-Bloom* $(t+1, n)$*-threshold sequence of co-primes* is a sequence of co-primes $m_0, m_1, \ldots, m_n$ which satisfies:

- $m_0 < m_1 < \cdots < m_n$;
- $\prod_{i=1}^{t+1} m_i > m_0 \prod_{i=0}^{t-1} m_{n-i}$ (this is called the *Asmuth-Bloom constraint*).

Let t and n be integers with $0 < t+1 \leq n$. The *Asmuth-Bloom* $(t+1, n)$*-threshold scheme* [1] is defined as follows:

(1) *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;
(2) *secret and share spaces:* define the secret space as $\mathbb{Z}_{m_0}$ and the share space of the ith participant as $\mathbb{Z}_{m_i}$, for all $1 \leq i \leq n$;
(3) *secret sharing:* given a secret s in the share space, randomly generate r such that $s' = s + rm_0 < \prod_{i=1}^{t+1} m_i$. Then, distribute s to the participants by computing $s_i = s' \bmod m_i$ for all $1 \leq i \leq n$ (s_i is the share of the ith participant, known only by him);

(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

$$x \equiv s_{i_j} \ mod \ m_{i_j}, \quad 1 \leq j \leq t+1$$

and then reducing it modulo m_0.

The ratio $|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}|$ is referred to as the *information rate* of the ith participant, for any $1 \leq i \leq n$.

For the sake of simplicity, we will use the terminology "Asmuth-Bloom sequence of co-primes" ("Asmuth-Bloom threshold scheme") instead of "Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes" ("Asmuth-Bloom $(t+1, n)$-threshold scheme") whenever it is not important to mention the integers t and n.

In order to obtain better security properties of the Asmuth-Bloom threshold scheme, several variants of it were proposed (details about their security will be given at the end of Section 3.1):

1. the variant in [7] considers *extended Asmuth-Bloom $(t+1, n)$-threshold sequences of co-primes* instead of Asmuth-Bloom $(t+1, n)$-threshold sequences of co-primes, which are simply defined by replacing the Asmuth-Bloom constraint by the following one:
$$\prod_{i=1}^{t+1} m_i > m_0^2 \prod_{i=0}^{t-1} m_{n-i} \tag{2}$$
2. one of the variants in [4] considers *almost Θ-compact sequences of co-primes* instead of Asmuth-Bloom sequences of co-primes, where $\Theta \in (0, 1)$. These are sequences of co-primes with the property $m_i \in (x, x + x^{\theta})$ for all i, where x linearly depends on m_0 and $\theta \in (0, \Theta]$;
3. another variation proposed in [4] considers the secret space as being $\mathbb{Z}_{m_n}$, while $\mathbb{Z}_{m_0}, \ldots, \mathbb{Z}_{m_{n-1}}$ are the share spaces. Moreover, the Asmuth-Bloom sequences of co-primes are replaced by $(n-1, \Theta)$-compact sequences of co-primes, where $\Theta \in (0, 1)$. These are sequences of co-primes $m_0, m_1, \ldots, m_n$ which satisfy $m_0 < m_1 < \cdots < m_n$, $m_n \geq m_{n-1} + 2$, and $m_n < m_0 + m_0^{\theta}$, for some $\theta \in (0, \Theta]$.

The Asmuth-Bloom threshold scheme and the first two variations above are based on sequences $m_0 < m_1 < \cdots < m_n$ of co-primes where the integer m_0 defines the secret space. In the third variation above the secret space is defined by m_n. In all these cases, all the participants have associated either larger share spaces than the secret space, or smaller 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, we will consider a new variation of the Asmuth-Bloom threshold scheme which is based on *k-compact sequences of co-primes* defined as below.

Definition 1 ([5]).

1. *A sequence $m_0, m_1, \ldots, m_n$ of pair-wise co-primes is called* (k, θ)-compact*, where $k \geq 1$ 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 $1 \leq i \leq n$.*
2. *A sequence $m_0, m_1, \ldots, m_n$ of pair-wise co-primes is called* k-compact *if it is (k, θ)-compact for some $\theta \in (0, 1)$.*

Remark that 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, larger than m_n, or in between m_1 and m_n.

Now, we define a new variation of the Asmuth-Bloom threshold scheme by changing the parameter setup phase into the following one:

(1') *parameter setup:* consider $m_0, m_1, \ldots, m_n$ a k-compact sequence of co-primes. The integers $t, n, m_0, m_1, \ldots, m_n$ are public parameters;

As we will see in Section 4, this new variant of the Asmuth-Bloom threshold scheme meets the best security properties among the variants of the Asmuth-Bloom threshold scheme known so far.

Remark 1. A few words about the relationships between the sequences of co-primes considered above are in order:

1. $(n-1, \Theta)$-compact sequences of co-primes are particular cases of almost Θ-compact sequences of co-primes which, in turn, are particular cases of k-compact sequences of co-primes.
2. In [4], *compact sequences of co-primes* were introduced as being sequences $m_0 < m_1 < \cdots < m_n$ of co-primes satisfying $m_i < m_0 + m_0^\theta$, for all $1 \leq i \leq n$ and some $\theta \in (0, 1)$. It is clear that compact sequences of co-primes are particular cases of 1-compact sequences of co-primes.
3. Extended Asmuth-Bloom sequences of co-primes are Asmuth-Bloom sequences of co-primes.
4. For sufficiently large m_0, k-compact sequences $m_0, m_1, \cdots, m_n$ of co-primes with $k > 1$ also satisfy the Asmuth-Bloom constraint. Indeed, the Asmuth-Bloom constraint is implied by the inequality
$$(km_0 - m_0^\theta)^{t+1} > m_0(km_0 + m_0^\theta)^t$$
As
$$\lim_{m_0 \to \infty} m_0 \frac{(km_0 + m_0^\theta)^t}{(km_0 - m_0^\theta)^{t+1}} = \frac{1}{k}$$
we conclude that the above inequality holds true for sufficiently large m_0.

We close this section by the following important convention: we use the terminology *Asmuth-Bloom threshold scheme based on extended Asmuth-Bloom* (*almost Θ-compact, $(n-1, \Theta)$-compact, k-compact*, resp.) *sequences of co-primes* for the Asmuth-Bloom threshold scheme where the Asmuth-Bloom sequences of co-primes are replaced by extended Asmuth-Bloom (almost Θ-compact, $(n-1, \Theta)$-compact, k-compact, resp.) sequences of co-primes.

3 Security Issues

In this section we discuss the security properties an Asmuth-Bloom threshold scheme variant would be desirable to satisfy.

3.1 Security Properties

Given the Asmuth-Bloom $(t+1, n)$-threshold scheme and a non-empty set $I \subseteq \{1, 2, \ldots, n\}$, 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.

The *loss of entropy* [6] with respect to $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, denoted $\Delta(y_I)$, is defined by

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

Under the uniform distribution on $\mathbb{Z}_{m_0}$, it follows $P(X = s) = 1/m_0$ for all $s \in \mathbb{Z}_{m_0}$ and, therefore,

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

Definition 2. *[6] The Asmuth-Bloom $(t+1, n)$-threshold scheme is called* asymptotically perfect *if, for any non-empty subset $I \subseteq \{1, \ldots, n\}$ with $|I| \leq t$ and any $\epsilon \in (0, 1)$, there exists $m \geq 0$ such that for any Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes $m_0, m_1, \ldots, m_n$ with $m_0 \geq m$, the following properties hold:*

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

The following definition is a slight variation of the asymptotic idealness concept in [6].

Definition 3. *Let $0 < t + 1 \leq n$ be positive integers and $r > 0$ be a real number.*

1. *We say that the information rate of the Asmuth-Bloom $(t+1, n)$-threshold scheme* goes asymptotically to *r if for any $\epsilon \in (0, 1)$ there exists $m \geq 0$ such that for any Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes $m_0, m_1, \ldots, m_n$ with $m_0 \geq m$ and any $1 \leq i \leq n$ the following holds:*

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

2. *We say that the Asmuth-Bloom $(t+1, n)$-threshold scheme is* asymptotically ideal *if it is asymptotically perfect and its information rate goes asymptotically to* 1.

Remark 2. Asymptotic perfectness and idealness can naturally be reformulated for the Asmuth-Bloom threshold scheme based on extended Asmuth-Bloom (almost Θ-compact, $(n-1,\Theta)$-compact, k-compact, respectively) sequences of co-primes. What we have to do is to replace "Asmuth-Bloom sequence of co-primes" by "extended Asmuth-Bloom sequence of co-primes" ("almost Θ-compact sequence of co-primes", "$(n-1,\Theta)$-compact sequence of co-primes", "k-compact sequence of co-primes", respectively).

Having introduced the concepts of asymptotic perfectness and idealness, we recall now some of the results previously obtained:

- the entropy loss in the Asmuth-Bloom threshold scheme is asymptotically upper bounded by 1 [4];
- the Asmuth-Bloom threshold scheme based on almost Θ-compact sequences of co-primes is asymptotically perfect and its information rate goes asymptotically to 2 [4];
- the Asmuth-Bloom $(t+1,n)$-threshold scheme based on $(n-1,\Theta)$-compact sequences of co-primes is asymptotically ideal [4].

In [7], Kaya and Selcuk have conjectured that replacing the Asmuth-Bloom sequences of co-primes by extended Asmuth-Bloom sequences of co-primes may increase the security of the Asmuth-Bloom threshold scheme. This will be proved in Section 5.

With respect to k-compact sequences of co-primes, we will prove our main result in Section 4 that these kind of sequences lead to a necessary and sufficient condition for asymptotic idealness of the Asmuth-Bloom threshold scheme.

3.2 Bounding the loss of entropy

This section is dedicated to finding good approximations for the loss of entropy in the Asmuth-Bloom threshold scheme. We begin by a technical notation intensively used in the rest of the paper.

Given a sequence $m_0, m_1, \ldots, m_n$ of co-primes and a non-empty subset $I \subseteq \{1,\ldots,n\}$, denote by $C(I)$ the integer

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

The following result is a straightforward adaptation of Lemma 1 in [6] for the case of the Asmuth-Bloom threshold scheme (the proof is omitted).

Lemma 1. *[6] The loss of entropy of the Asmuth-Bloom $(t+1,n)$-threshold scheme under a uniform distribution on the secret space satisfies the relations*

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

– $\Delta(y_I) = \log m_0$, *if* $C(I) = 0$,

for any non-empty subset $I \subseteq \{1, \ldots, n\}$, *any Asmuth-Bloom* $(t+1, n)$*-threshold sequence of co-primes* $m_0, m_1, \ldots, m_n$, *and any* $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$.

Lemma 1 is an important tool in studying the loss of entropy in the Asmuth-Bloom threshold scheme. The following result sharpens it by providing a more precise approximation of the loss of entropy in the Asmuth-Bloom threshold scheme.

Lemma 2. *The loss of entropy of the Asmuth-Bloom* $(t+1, n)$*-threshold scheme under a uniform distribution on the secret space satisfies the relation*

$$\Delta(y_I) = \begin{cases} \log m_0 + \delta_1 \dfrac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} \log \dfrac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \dfrac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \log \dfrac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I}, & \text{if } C_I \neq 0 \\ \log m_0, \text{ if } C_I = 0, \end{cases}$$

for any non-empty subset $I \subseteq \{1, \ldots, n\}$, *any Asmuth-Bloom* $(t+1, n)$*-threshold sequence of co-primes* $m_0, m_1, \ldots, m_n$, *any* $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$, *and some* $C_I \in \{C(I), C(I)+1\}$, *where* $\delta_2 = C_I \bmod m_0$ *and* $\delta_1 = m_0 - \delta_2$.

Proof. Let $I \subseteq \{1, \ldots, n\}$ be a non-empty set and $m_0, m_1, \ldots, m_n$ be an Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes.

If $|I| > t$, then $C(I) \in \{0, 1\}$ and $H(X|Y_I = y_I) = 0$, which leads to $\Delta(y_I) = H(X) = \log m_0$. The choice $C_I = C(I)$ concludes the proof in this case.

Let us assume now that $|I| \leq t$, and let x_0 denote the unique solution modulo $\prod_{i \in I} m_i$ obtained by using the CRT over the shares of the participants in I. Consider the set

$$B = \left\{ x \in \mathbb{Z}_{\prod_{i=1}^{t+1} m_i} \mid x = x_0 + r \cdot \prod_{i \in I} m_i,\ r \in \mathbb{Z} \right\}$$

and show that $|B| = C(I)$ or $|B| = C(I) + 1$. Indeed, if $x_0 + r \cdot \prod_{i \in I} m_i$ is an element of B, then

$$0 \leq r \leq \left\lfloor \frac{\prod_{i=1}^{t+1} m_i - x_0}{\prod_{i \in I} m_i} \right\rfloor.$$

As $0 \leq x_0 < \prod_{i \in I} m_i$, we obtain

$$C(I) - 1 \leq \left\lfloor \frac{\prod_{i=1}^{t+1} m_i - x_0}{\prod_{i \in I} m_i} \right\rfloor \leq C(I).$$

Therefore, $0 \leq r \leq C(I) - 1$ or $0 \leq r \leq C(I)$, depending on x_0. This shows that $|B| = C(I)$ or $|B| = C(I) + 1$.

Let $C_I = |B|$. Then, $B = \left\{x_0 + r \cdot \prod_{i \in I} m_i \mid 0 \leq r < C_I\right\}$. According to the division theorem, there exist unique $q \geq 0$ and $0 \leq \delta_2 < m_0$ such that $C_I = m_0 \cdot q + \delta_2$. We partition the set B into $B = B_1 \cup \cdots \cup B_q \cup C$, where

$$B_i = \left\{x_0 + (i-1)m_0 \cdot \prod_{i \in I} m_i, \ldots, x_0 + (im_0 - 1) \cdot \prod_{i \in I} m_i\right\}$$

for all $1 \leq i \leq q$, and

$$C = \left\{x_0 + qm_0 \cdot \prod_{i \in I} m_i, \ldots, x_0 + (qm_0 + \delta_2 - 1) \cdot \prod_{i \in I} m_i\right\}.$$

Any two elements in B_i, $1 \leq i \leq q$, are non-congruent modulo m_0. Indeed, if we consider

$$x_0 + ((i-1)m_0 + j_1) \cdot \prod_{i \in I} m_i \equiv x_0 + ((i-1)m_0 + j_2) \cdot \prod_{i \in I} m_i \bmod m_0$$

with $j_1, j_2 \in \mathbb{Z}_{m_0}$, then $j_1 = j_2$. Similarly, any two elements in C are non-congruent modulo m_0. As a conclusion, $\{x \bmod m_0 \mid x \in B_i\} = \mathbb{Z}_{m_0}$ for all $1 \leq i \leq q$, $\{x \bmod m_0 \mid x \in C\} \subset \mathbb{Z}_{m_0}$ and $|\{x \bmod m_0 \mid x \in C\}| = \delta_2$.

Denoting $\delta_1 = m_0 - \delta_2$, our conclusion so far is that there exist δ_1 elements in $\mathbb{Z}_{m_0}$ with the property that each of them is a residue modulo m_0 of exactly q elements in B, and the other δ_2 elements in $\mathbb{Z}_{m_0}$ have the property that each of them is a residue modulo m_0 of exactly $q+1$ elements in B. According to this,

$$P(X = s \mid Y_I = y_I) = \frac{q}{C_I}$$

for exactly δ_1 values $s \in \mathbb{Z}_{m_0}$, and

$$P(X = s \mid Y_I = y_I) = \frac{q+1}{C_I}$$

for exactly δ_2 values $s \in \mathbb{Z}_{m_0}$. Therefore,

$$\begin{aligned}
\Delta(y_I) &= H(X) - H(X|Y_I = y_I) \\
&= \log m_0 - \textstyle\sum_{s \in \mathbb{Z}_{m_0}} P(X = s \mid Y_I = y_I) \log \dfrac{1}{P(X = s \mid Y_I = y_I)} \\
&= \log m_0 + \textstyle\sum_{s \in \mathbb{Z}_{m_0}} P(X = s \mid Y_I = y_I) \log P(X = s \mid Y_I = y_I) \\
&= \log m_0 + \delta_1 \frac{q}{C_I} \log \frac{q}{C_I} + \delta_2 \frac{q+1}{C_I} \log \frac{q+1}{C_I},
\end{aligned}$$

and the lemma follows from the remark that $q = \left\lfloor \dfrac{C_I}{m_0} \right\rfloor$.

Remark 3. Lemma 1 is a direct consequence of Lemma 2:

$$\begin{aligned}
\Delta(y_I) &= \log m_0 + \delta_1 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \\
&\leq \log m_0 + \left(\delta_1 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \right) \log \frac{\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1}{C(I)} \\
&= \log m_0 + \frac{(\delta_1 + \delta_2) \left\lfloor \frac{C_I}{m_0} \right\rfloor + \delta_2}{C_I} \log \frac{\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1}{C(I)} \\
&= \log m_0 + \frac{m_0 \left\lfloor \frac{C_I}{m_0} \right\rfloor + \delta_2}{C_I} \log \frac{\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1}{C(I)} \\
&= \log m_0 + \log \frac{\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1}{C(I)} \\
&= \log \frac{m_0 \left(\left\lfloor \frac{C(I)+1}{m_0} \right\rfloor + 1 \right)}{C(I)}
\end{aligned}$$

if $C(I) \neq 0$ (the inequalities $C(I) \leq C_I \leq C(I) + 1$ were used).

Remark 4. One can easily see that the result in Lemma 2 (and Lemma 1 as well) does not depend on the type of sequence of co-primes under which the Asmuth-Bloom threshold scheme is based on. That is, both Lemma 2 and Lemma 1 hold as well if the Asmuth-Bloom threshold scheme is based on extended Asmuth-Bloom (almost Θ-compact, $(n-1, \Theta)$-compact, k-compact) sequences of co-primes.

4 The main result

In this section we present our main result. Recall first that the concepts of asymptotic perfectness and idealness in the case of the Asmuth-Bloom threshold scheme based on k-compact sequences of co-primes are that in Remark 2.

Theorem 1. *Let $k \geq 1$ be an integer. The Asmuth-Bloom 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. We prove first the converse of this theorem. Let $0 < t + 1 \leq n$ be positive integers. Assume that the Asmuth-Bloom $(t+1, n)$-threshold scheme is asymptotically perfect and its information rate goes asymptotically to k. Therefore, for any $\epsilon \in (0, 1)$

there exists $m \geq 0$ such that for any sequence $m_0, m_1, \ldots, m_n$ of co-primes with $m_0 \geq m$ and any $1 \leq i \leq n$ 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 $\epsilon m_0 \leq m_0^\theta$, 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 $m_0, m_1, \ldots, m_n$ of co-primes which satisfies $km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0$ for all $1 \leq i \leq n$ and some $\epsilon \in (0,1)$ will also satisfy

$$km_0 - m_0^\theta \leq km_0 - \epsilon m_0 < m_i < km_0 + \epsilon m_0 \leq km_0 + m_0^\theta,$$

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

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

Asymptotic perfectness. Let $I \subseteq \{1, \ldots, n\}$ denote a non-empty set with $|I| \leq t$, and let $\theta \in (0,1)$. The following cases are to be considered.

Case 1: $|I| < t$. For a given (k,θ)-compact sequence $m_0, m_1, \ldots, m_n$ of co-primes, the property $x - 1 < \lfloor x \rfloor \leq x$ and Lemma 1 lead to:

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

As, $km_0 - m_0^\theta < m_i < km_0 + m_0^\theta$ for any $1 \leq i \leq n$, and $|I| \leq t - 1$, 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 $\epsilon > 0$ there exists m such that $\Delta(y_I) < \epsilon$ if $m_0 \geq m$.

Case 2: $|I| = t$. We prove first the following Claim which establishes lower and upper bounds for C_I.

Claim 1. For any $\theta \in (0,1)$ there exists m such that any (k,θ)-compact sequence $m_0, m_1, \ldots, m_n$ with $m_0 \geq m$ satisfies

$$km_0 - (m_0^\theta + 1) < C_I < km_0 + (m_0^\theta + 1).$$

Proof of Claim 1. Let $\theta \in (0,1)$. For any (k,θ)-compact sequence $m_0, m_1, \ldots, m_n$ the following holds:

$$C_I \leq C(I) + 1 \leq \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i \in I} m_i} + 1 \leq \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i=1}^{t} m_i} + 1 = m_{t+1} + 1 < km_0 + (m_0^\theta + 1).$$

One can easily see that

$$\lim_{m_0 \to \infty} \frac{\prod_{i=1}^{t+1} m_i}{m_0 \prod_{i \in I} m_i} = k$$

and thus, for any $\epsilon > 0$ and sufficiently large m_0 we have

$$\frac{\prod_{i=1}^{t+1} m_i}{m_0 \prod_{i\in I} m_i} > k - \epsilon.$$

Therefore, for any $\epsilon > 0$ and sufficiently large m_0 the following holds:

$$C_I \geq C(I) \geq \frac{\prod_{i=1}^{t+1} m_i}{\prod_{i\in I} m_i} - 1 > km_0 - \epsilon m_0 - 1.$$

For $\epsilon < m_0^{\theta-1}$ we obtain the inequality in Claim 1.

Let $m_0, m_1, \ldots, m_n$ be a (k,θ)-compact sequence which satisfies Claim 1. The following two cases are in order:

Case 2.1: $km_0 - (m_0^\theta + 1) < C_I < km_0$. Then, $\left\lfloor \frac{C_I}{m_0} \right\rfloor = k-1$. As $C_I = m_0 \cdot \left\lfloor \frac{C_I}{m_0} \right\rfloor + \delta_2$, we obtain

$$m_0 - (m_0^\theta + 1) < \delta_2 < m_0$$

which shows that δ_2/m_0 goes to 1 and δ_1 goes to 0 as m_0 goes to infinity (recall that θ is fixed). Then, from Lemma 2 it follows

$$\begin{aligned}
\Delta(y_I) &= \log m_0 + \delta_1 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \\
&= \log m_0 + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k-1}{(k-1)m_0 + \delta_2} \\
&\quad + \delta_2 \frac{k}{(k-1)m_0 + \delta_2} \log \frac{k}{(k-1)m_0 + \delta_2} \\
&= \log m_0 + \Big(\delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} + \delta_2 \frac{k}{(k-1)m_0 + \delta_2}\Big) \log \frac{k}{(k-1)m_0 + \delta_2} \\
&\quad + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \Big(\log \frac{k-1}{(k-1)m_0 + \delta_2} - \log \frac{k}{(k-1)m_0 + \delta_2} \Big) \\
&= \log m_0 + \log \frac{k}{(k-1)m_0 + \delta_2} + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k-1}{k} \\
&= \log \frac{km_0}{(k-1)m_0 + \delta_2} + \delta_1 \frac{k-1}{(k-1)m_0 + \delta_2} \log \frac{k-1}{k} \\
&= \log \frac{km_0}{km_0 - \delta_1} + \delta_1 \frac{k-1}{km_0 - \delta_1} \log \frac{k-1}{k}
\end{aligned}$$

if $k > 1$, and

$$\begin{aligned}\Delta(y_I) &= \log m_0 + \delta_1 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \\ &= \log \frac{m_0}{\delta_2} \\ &= \log \frac{m_0}{m_0 - \delta_1}\end{aligned}$$

if $k = 1$ (the convention $0 \log 0 = 0$ was used).

As both $\delta_1/(km_0 - \delta_1)$ and δ_1/m_0 goes to 0 as m_0 goes to infinity, we deduce that $\Delta(y_I)$ goes to 0 as m_0 goes to infinity.

Case 2.2: $km_0 \leq C_I < km_0 + (m_0^\theta + 1)$. Then, $\left\lfloor \frac{C_I}{m_0} \right\rfloor = k$. As $C_I = m_0 \cdot \left\lfloor \frac{C_I}{m_0} \right\rfloor + \delta_2$, we obtain

$$0 \leq \delta_2 < m_0^\theta + 1$$

which shows that δ_2/m_0 goes to 0 and δ_1 goes to 1 as m_0 goes to infinity (recall that θ is fixed). Then, from Lemma 2 it follows:

$$\begin{aligned}\Delta(y_I) &= \log m_0 + \delta_1 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor}{C_I} + \delta_2 \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \log \frac{\left\lfloor \frac{C_I}{m_0} \right\rfloor + 1}{C_I} \\ &= \log m_0 + \delta_1 \frac{k}{km_0 + \delta_2} \log \frac{k}{km_0 + \delta_2} + \delta_2 \frac{k+1}{km_0 + \delta_2} \log \frac{k+1}{km_0 + \delta_2} \\ &= \log m_0 + \left(\delta_1 \frac{k}{km_0 + \delta_2} + \delta_2 \frac{k+1}{km_0 + \delta_2} \right) \log \frac{k}{km_0 + \delta_2} \\ &\quad + \delta_2 \frac{k+1}{km_0 + \delta_2} \left(\log \frac{k+1}{km_0 + \delta_2} - \log \frac{k}{km_0 + \delta_2} \right) \\ &= \log m_0 + \log \frac{k}{km_0 + \delta_2} + \delta_2 \frac{k+1}{km_0 + \delta_2} \log \frac{k+1}{k} \\ &= \log \frac{km_0}{km_0 + \delta_2} + \delta_2 \frac{k+1}{km_0 + \delta_2} \log \frac{k+1}{k}\end{aligned}$$

As $\delta_2/(km_0 + \delta_2)$ goes to 0 as m_0 goes to infinity, we deduce that $\Delta(y_I)$ goes to 0 as m_0 goes to infinity.

Information rate. Given $\theta \in (0, 1)$ and $m_0, m_1, \ldots, m_n$ a (k, θ)-compact sequence of co-primes, we have

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

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

Corollary 1. *The Asmuth-Bloom threshold scheme is asymptotically ideal with respect to the uniform distribution on the secret space if and only if it is based on 1-compact sequences of co-primes.*

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

Remark 5. Choosing $m_1 < \cdots < m_n$ in a compact interval centered at m_0, offers the maximum of optimality with respect to the asymptotic idealness of the Asmuth-Bloom $(t+1, n)$-threshold scheme.

5 Extended Asmuth-Bloom sequences of co-primes

In this section we focus on the Asmuth-Bloom threshold scheme based on extended Asmuth-Bloom sequences of co-primes [7].

Theorem 2. *The Asmuth-Bloom threshold scheme based on extended Asmuth-Bloom sequences of co-primes is asymptotically perfect under the uniform distribution on the secret space.*

Proof. Let $0 < t + 1 \leq n$ be positive integers and $I \subseteq \{1, \ldots, n\}$ be a non-empty set with $|I| \leq t$. Then, $C(I) > m_0^2$ for any extended Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes $m_0, m_1, \ldots, m_n$, and Lemma 1 (see also Remark 4) leads to

$$\Delta(y_I) \leq \log \frac{C(I) + 2m_0}{C(I)},$$

which shows that the entropy loss goes to zero as m_0 goes to infinity.

Remark 6. One may define extended Asmuth-Bloom $(t+1, n)$-threshold 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 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^{θ}.

6 Conclusions

In this paper we presented a necessary and sufficient condition for the asymptotic idealness of the Asmuth-Bloom threshold scheme. Namely, it was shown that this scheme is asymptotically ideal if and only if it is based on 1-compact sequences of

co-primes. Moreover, a comprehensive analysis of the known variants of the Asmuth-Bloom threshold scheme is provided, clarifying the security properties achieved by each of them.

Although the case $k = 1$ in Theorem 1 represents the main result regarding the security of the Asmuth-Bloom threshold scheme, it would be interesting to extend the characterization in this theorem to the case where $k > 1$ is a real number but not an integer one.

References

1. C. A. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, Mar. 1983, the paper was presented at the National Telecommunications Conference, Houstan, Dec. 1980.
2. M. Mignotte, "How to share a secret?" in *Workshop on Cryptography*, ser. Lecture Notes in Computer Science, T. Beth, Ed., vol. 149, Burg Feuerstein, 1982, pp. 371–375.
3. O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering with errors," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1330–1338, Mar. 2000.
4. 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*, vol. 240, pp. 161–172, 2013.
5. 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*, vol. 114, no. 6, pp. 299 – 303, 2014.
6. M. Quisquater, B. Preneel, and J. Vandewalle, "On the security of the threshold scheme based on the Chinese remainder theorem," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, D. Naccache and P. Paillier, Eds., vol. 2274. Springer, 2002, pp. 199–210.
7. K. Kaya and A. A. Selçuk, "Threshold cryptography based on Asmuth-Bloom secret sharing," *Information sciences*, vol. 177, no. 19, pp. 4148–4160, 2007.
8. C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem. Applications in Computing, Coding, Cryptography.* World Scientific Publishing, 1996.