Asymptotically Ideal CRT-based Secret Sharing Schemes for Multilevel and Compartmented Access Structures

Ferucio Laurenţiu Ţiplea[a], Constantin Cătălin Drăgan[b]

[a] *Department of Computer Science, "Alexandru Ioan Cuza" University of Iaşi, Romania*
[b] *Department of Computer Science, Faculty of Engineering and Physical Sciences, University of Surrey, UK*

Abstract

Multilevel and compartmented access structures are two important classes of access structures where participants are grouped into levels/compartments with different degrees of trust and privileges. The construction of secret sharing schemes for such access structures has been in the attention of researchers for a long time. Two main approaches have been taken so far: one of them is based on polynomial interpolation and the other one is based on the Chinese Remainder Theorem (CRT).

In this paper we propose the first asymptotically ideal CRT-based secret sharing schemes for (disjunctive, conjunctive) multilevel and compartmented access structures. Our approach is compositional and it is based on a variant of the Asmuth-Bloom secret sharing scheme where some participants may have public shares. Based on this, we show that the proposed secret sharing schemes for multilevel and compartmented access structures are asymptotically ideal if and only if they are based on 1-compact sequences of co-primes.

Keywords: Access structure, secret sharing scheme, Chinese remainder theorem, entropy, asymptotic idealness

1. Introduction and preliminaries

Secret sharing schemes (SSS) are a fundamental tool in cryptography and information security. Their systematic study has began with the introduction of secret sharing for threshold access structures [23, 5]. Threshold access structures are suitable when participants have the same degree of trust. However, many real-world applications need more complex access structures based on different degrees of trust and privileges associated to participants. *Multilevel* (also called *hierarchical*) [24, 13] and *compartmented* [24] access structures are two important classes of access structures proposed to cope with this problem. In both of them, the set of participants is partitioned into groups called *levels* (in the case of multilevel access structures) or *compartments* (in the case of compartmented

Email addresses: `ferucio.tiplea@uaic.ro` (Ferucio Laurenţiu Ţiplea), `c.dragan@surrey.ac.uk` (Constantin Cătălin Drăgan)

access structures). To these groups thresholds are assigned on whose basis authorized sets are defined.

Designing secret sharing schemes for multilevel and compartmented access structure is of crucial importance. Two main approaches along this direction have been taken so far: one of them is based on polynomial interpolation and the other one is based on CRT. In this paper we will focus on the second approach.

CRT was intensively used in the design of secret sharing schemes [1, 20, 14, 22, 19, 2, 7]. As a standard procedure, a sequence of pairwise co-prime positive integers with special properties is first computed. Then, the private shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders. To recover the secret, the CRT is applied on a number of congruences defined by some private shares.

The security of the CRT-based secret sharing schemes has been poorly understood for a quite long time. In 2002, Quisquater et al. [22] have introduced the concepts of *asymptotic perfectness* and *asymptotic idealness*, and initiated the study of security of the CRT-based secret sharing schemes through these concepts. Their results were greatly improved in [2, 7, 11, 10], were necessary and sufficient conditions for the asymptotic idealness of some threshold and distributive secret sharing schemes have been established.

Contribution. In this paper we continue the study of CRT-based secret sharing schemes by considering multilevel and compartmented access structures. Thus, we propose the first asymptotically ideal CRT-based secret sharing schemes for such access structures. To do that, a variant of the Asmuth-Bloom threshold secret sharing scheme is firstly introduced, that allow participants to publish some information about their private shares. We prove that this scheme is asymptotically ideal and then we use it to reason about the security of all the other schemes proposed in our paper. More precisely, we show that our schemes are asymptotically ideal if and only if they are based on 1-compact sequences of co-primes. Taking into account that these kind of sequences can be very efficiently generated (see our Section 5), we conclude that our schemes are not only the most secure but also among the most efficient CRT-based secret sharing schemes.

Paper structure. Our paper is organized into seven sections. The rest of this section fixes the basic concepts and notation used through our paper. The second section is dedicated to the Asmuth-Bloom secret sharing scheme with public shares. Then, in the third section, we propose CRT-based secret sharing schemes for disjunctive and conjunctive multilevel, and compartmented, access structures. We also study their security. The fourth section discusses the possibility of changing the Asmuth-Bloom threshold secret sharing scheme with other threshold secret sharing schemes. The efficiency of implementing our schemes is the topic of the fifth section. An extensive discussion on related work is taken in Section 6. We conclude the paper in the last section.

Preliminaries. The set of integers (positive integers) is denoted by $\mathbb{Z}$ ($\mathbf{N}$). A positive integer $a > 1$ is a *prime* number if the only positive divisors of it are 1 and a. Given two integers a and b, the notation (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 $a \equiv b \bmod n$ or $a \equiv_n b$, 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 $\mathbb{Z}_n$.

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

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

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

Recall a few notations regarding the Shannon entropy (for details, the reader is referred to [6]). Given a random variable X with outcomes in a set V, the (Shannon) *entropy* of X, denoted $H(X)$, is defined by

$$H(X) = \sum_{v \in V} P(X = v) \log \frac{1}{P(X = v)}$$

with the mathematical convention $0 \log 0 = 0$ ($P(X = v)$ is the probability mass function of the outcome v).

Given two random variables X and Y, $H(X|Y)$ stands for the entropy of X conditioned by Y.

2. Asmuth-Bloom Secret Sharing with Public Shares

We propose in this section a new variant of the Asmuth-Bloom secret sharing scheme [1]. The main idea is to partition the set U of participants into two disjoint subsets U_1 and U_2 (not necessarily both of them non-empty). The participants in U_1 receive private shares computed as in the Asmuth-Bloom secret sharing scheme. The participants in U_2 choose private shares by themselves and then make public some information about these shares.

We will prove that this new variant of the Asmuth-Bloom secret sharing scheme is asymptotically ideal if and only if it is based on *1-compact sequences of co-primes* (this is similar to the result established in [10] on the original Asmuth-Bloom secret sharing scheme).

Adding public shares to threshold secret sharing schemes might not appear relevant at a first sight. However, as we will see in Section 3, we are sometimes in the position of combining several Asmuth-Bloom secret sharing schemes with common participants. Each common participant will be assigned exactly one private share for one of the schemes. The private share will then be used to derive public shares for the other schemes, allowing the participant to take part in those schemes.

2.1. Description of the Scheme

We begin by fixing the terminology and notation with respect to threshold access structures and sequences of co-primes.

A *threshold access structure* (TAS) is a triple $(U, t+1, \Gamma)$ consisting of a finite set U of *participants*, an integer $t + 1$ satisfying $0 < t + 1 \leq |U|$, and a set Γ defined by

$$\Gamma = \{A \subseteq U \mid |A| \geq t + 1\}.$$

The integer $t+1$ is called the *threshold* of the access structure, and each set $A \in \Gamma$ is called an *authorized set.* Sometimes, Γ is called the $(t+1)$-*threshold access structure over* U.

It is customary in secret sharing to consider the set U of participants of the form $U = \{1, \ldots, n\}$. In such a case, Γ is also referred to as the $(t+1, n)$-*threshold access structure.*

A *sequence of co-primes* is a sequence $m_0, m_1, \ldots, m_n$ (sometimes written as a vector $L = (m_0, m_1, \ldots, m_n)$ or even $L : m_0, m_1, \ldots, m_n$) of pairwise co-prime strictly positive integers, where $n \geq 1$. The *length* of this sequence is $n+1$. An element of this sequence is referred to as a *co-prime.*

An *Asmuth-Bloom* $(t+1, n)$-*threshold sequence of co-primes*, where t and n are two integers with $0 < t+1 \leq n$, is a sequence of co-primes $m_0, m_1, \ldots, m_n$ that satisfies the following properties:

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

(one has to remark that the Asmuth-Bloom constraint also implies $m_0 < m_1$).

Now, we are in a position to introduce our first scheme. Let $(t+1, \Gamma)$ be a threshold access structure over $U = \{1, \ldots, n\}$ and (U_1, U_2) be a partition of U $(U_1, U_2 \subseteq U$, $U_1 \cap U_2 = \emptyset$, and $U_1 \cup U_2 = U)$.

Scheme 1: Asmuth-Bloom SSS for $(U_1, U_2, t+1, \Gamma)$

Parameter setup: choose $L : m_0, m_1, \ldots, m_n$ an Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes. The integers t and n, and the the sequence L are public parameters. Define the *secret space* as $\mathbb{Z}_{m_0}$ and the *share space* of the ith participant as $\mathbb{Z}_{m_i}$, for all $1 \leq i \leq n$;

Secret sharing: given $s \in \mathbb{Z}_{m_0}$, randomly generate $r \geq 0$ such that $s' = s + rm_0 < \prod_{i=1}^{t+1} m_i$. Then, share s as follows:

1. for each $i \in U_1$, $s_i = s' \bmod m_i$ is computed and distributed as a private share of the participant i;
2. for each $i \in U_2$ a positive integer $s_i \in \mathbb{Z}_{m_i}$ is chosen uniformly at random as a private share of i, and $w_i = (s' - s_i) \bmod m_i$ is computed and broadcast as public information;

Secret reconstruction: any $A \in \Gamma$ can uniquely reconstruct the secret s by computing first the unique solution modulo $\prod_{i \in I} m_i$ of the system

$$\begin{cases} x \equiv s_i \bmod m_i, & i \in A \cap U_1 \\ x \equiv (s_i + w_i) \bmod m_i, & i \in A \cap U_2 \end{cases} \tag{2}$$

and then reducing it modulo m_0.

We would like to emphasize that the private shares for participants in U_1 are computed by a modular reduction of the secret s', while the private shares for participants in U_2 are randomly generated from the share space. One may also think as follows. For a participant $i \in U_2$ a secret value $\overline{s}$ is first computed as for participants in U_1, namely $\overline{s} = s' \bmod m_i$. Then, $\overline{s}$ is randomly split into two parts, s_i and w_i; s_i is kept as a private share, while w_i is made public.

It is straightforward to prove soundness of the secret reconstruction in Scheme 1. Assume $A \in \Gamma$. Then,

- The congruence $w_i \equiv (s' - s_i) \bmod m_i$ is equivalent to the congruence $s' \equiv (s_i + w_i) \bmod m_i$, for all $i \in U_2$. As a conclusion, the system (2) of congruences has the unique solution s' modulo $\prod_{i \in I} m_i$;

- As $s' = s + rm_0 < \prod_{i=1}^{t+1} m_i$ for some $r \geq 0$, it follows $s = s' \bmod m_0$.

When U_2 is the empty set in Scheme 1, the Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over $(U, \emptyset)$ is in fact the original *Asmuth-Bloom secret sharing scheme for* $(t+1, \Gamma)$ *over* U [1].

An *Asmuth-Bloom secret sharing scheme with public shares* is an Asmuth-Bloom secret sharing scheme for some threshold access structure $(t+1, \Gamma)$ over a partition (U_1, U_2) of a set $U = \{1, \ldots, n\}$ of participants.

Scheme 1 is a generic secret sharing scheme in the sense that it consists of formal parameters. When these parameters are assigned specific values we obtain what is called a *realization* of Scheme 1. We will frequently make use of this terminology in the rest of the paper.

Example 2.1. *We present here a realization of Scheme 1 with artificially small actual parameters. Let* $U = \{1, 2, 3, 4, 5\}$ *be the set of participants,* $U_1 = \{1, 2, 3\}$*,* $U_2 = \{4, 5\}$*, and let* $t + 1 = 3$ *be the threshold. Consider the following Asmuth-Bloom (3,5)-threshold sequence of co-primes*

$$7,\ 17,\ 19,\ 23,\ 29,\ 31$$

(one may easily check that it fulfills the Asmuth-Bloom constraint).

To share the secret $s = 4 \in \mathbb{Z}_7$*, we first generate a random* r*, say* $r = 999$*, and compute* $s' = 4 + 7 \cdot 999 = 6997$*. Then,*

- *the participants in* U_1 *receive the private shares* 10, 5, 5 *(in this order);*

- *the participants in* U_2 *may receive the private shares* 11 *and* 19*, while their public shares are* 26 *and* 3 *(in this order).*

The set $A = \{1, 2, 4\}$ *is authorized. To recover the secret, the system (3) of congruences is solved:*

$$\begin{cases} x \equiv 10 \bmod 17 \\ x \equiv 5 \bmod 19 \\ x \equiv (11 + 26) \bmod 29 \end{cases} \tag{3}$$

The unique solution modulo $17 \cdot 19 \cdot 29 = 9367$ *of the system (3) is* $s' = 6997$*, from which* $s = 4$ *is obtained by a reduction modulo* 7*.*

2.2. Security Concepts and Results

We will focus now on the security of the Asmuth-Bloom secret sharing scheme with public shares. The concepts and results we prove are natural extensions of the ones in [10, 22].

Given $m_0, m_1, \ldots, m_n$ a sequence of co-primes, (U_1, U_2) a partition of $U = \{1, \ldots, n\}$, $I \subseteq U$, and $J \subseteq U_2$, consider three random variables X, Y_I, and W_J which take values as follows:

- X takes values into $\mathbb{Z}_{m_0}$;
- Y_I takes values into $\overline{\Pi}_I = \prod_{i \in I} \overline{\mathbb{Z}}_{m_i}$, where
$$\overline{\mathbb{Z}}_{m_i} = \begin{cases} \mathbb{Z}_{m_i}, & \text{if } i \in I \cap U_1 \\ \mathbb{Z}_{m_i} \times \mathbb{Z}_{m_i}, & \text{if } i \in I \cap U_2; \end{cases}$$
- W_J takes values into $\Pi_J = \prod_{i \in J} \mathbb{Z}_{m_i}$.

The meaning of these variables is the next one. The variable X returns secret values $s \in \mathbb{Z}_{m_0}$. An output of Y_I gives information about the private shares of the participants in $I \cap U_1$ and of the pairs (private share, public share) of the participants in $I \cap U_2$. Finally, an output w_J of W_J gives information of the public shares of the participants in J.

Given these random variables define the *loss of entropy* $\Delta(y_I)$ with respect to $y_I \in \overline{\Pi}_I$ by

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

and the *loss of entropy* $\Delta(y_I, w_J)$ with respect to $y_I \in \overline{\Pi}_I$ and $w_J \in \Pi_J$ by

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

Of course, $\Delta(y_I, w_J)$ makes sense only for non-empty subsets $J \subseteq U_2 \setminus I$.

Now we are ready to introduce the security concepts for the Asmuth-Bloom secret sharing scheme with public shares. We follow a similar line to the one in [10, 22] and introduce the concepts of asymptotic perfectness, asymptotic information rate, and asymptotic idealness.

The asymptotic perfectness of a secret sharing scheme means that unauthorized sets of participants can obtain no information, in the asymptotic sense, about the secret.

Definition 2.1. *Let (U_1, U_2) be a partition of $U = \{1, \ldots, n\}$, t be an integer such that $0 < t + 1 \leq n$, and Γ be the $(t+1)$-threshold access structure over U. The Asmuth-Bloom secret sharing scheme for $(t + 1, \Gamma)$ over (U_1, U_2) is called* asymptotically perfect *if, for any non-empty subset $I \subseteq U$ 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:*

- *$H(X) \neq 0$;*
- *$|\Delta(y_I, w_{U_2 - I})| < \epsilon$, for any $y_I \in \overline{\Pi}_I$ and $w_{U_2 - I} \in \Pi_{U_2 - I}$.*

If the information rate of the participants in a secret sharing scheme goes to r, we say that the information rate of the scheme goes to r.

Definition 2.2. *Let (U_1, U_2) be a partition of $U = \{1, \ldots, n\}$, t be an integer such that $0 < t+1 \leq n$, and Γ be the $(t+1)$-threshold access structure over U. We say that the information rate of the Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over (U_1, U_2)* goes asymptotically to r, *where $r > 0$ is a real number, 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:*

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

Combining Definitions 2.1 and 2.2 we obtain:

Definition 2.3. *Let (U_1, U_2) be a partition of $U = \{1, \ldots, n\}$, t be an integer such that $0 < t+1 \leq n$, and Γ be the $(t+1)$-threshold access structure over U. The Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over (U_1, U_2) is* asymptotically ideal *if it is asymptotically perfect and its information rate goes asymptotically to* 1.

When $U_2 = \emptyset$, Definitions 2.1, 2.2, and 2.3 give the security concepts in [10] for the original Asmuth-Bloom secret sharing scheme.

We prove next that the security of the Asmuth-Bloom secret sharing scheme with public shares is equivalent to the security of the original Asmuth-Bloom secret sharing scheme. We begin by a few results that establish a connection between the loss of entropy in the original Asmuth-Bloom secret sharing scheme and the Asmuth-Bloom secret sharing scheme with public shares.

Lemma 2.1. *Let (U_1, U_2) be a partition of $U = \{1, \ldots, n\}$, t be an integer such that $0 < t+1 \leq n$, and Γ be the $(t+1)$-threshold access structure over U. The loss of entropy of the Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over (U_1, U_2), under a uniform distribution on the secret space, satisfies*

$$\Delta(y_I, w_J) = \Delta(y_I),$$

for any non-empty subset $I \subseteq U$, any $J \subseteq U_2 \setminus I$, any Asmuth-Bloom $(t+1, n)$-threshold sequence of co-primes $m_0, m_1, \ldots, m_n$, any $y_I \in \overline{\Pi}_I$, and any $w_J \in \Pi_J$.

Proof. According to the definition of loss of entropy, it is sufficient to show that $H(X|Y_I = y_I) = H(X|Y_I = y_I, W_J = w_J)$. This comes down to proving that, for any $s \in \mathbb{Z}_{m_0}$, the following holds:

$$P(X = s|Y_I = y_I) = P(X = s|Y_I = y_I, W_J = w_J). \tag{4}$$

When $|I| \geq t+1$, both probabilities in equation (4) are 1 because the secret is uniquely recovered by at least $t+1$ participants.

Assume $|I| \leq t$ and $J \neq \emptyset$. Let $y_I(i) = y_i \in \mathbb{Z}_{m_i}$ for $i \in I \cap U_1$, and $y_I(i) = (y_i, w_i) \in \mathbb{Z}_{m_i} \times \mathbb{Z}_{m_i}$ for $i \in I \cap U_2$. Consider now the following systems of equations:

$$\begin{cases} x \equiv y_i \bmod m_i & \forall i \in I \cap U_1 \\ x \equiv y_i + w_i \bmod m_i & \forall i \in I \cap U_2 \end{cases} \tag{5}$$

and

$$\begin{cases} x \equiv y_i \bmod m_i & \forall i \in I \cap U_1 \\ x \equiv y_i + w_i \bmod m_i & \forall i \in I \cap U_2 \\ x \equiv z_j + w_J(j) \bmod m_j & \forall j \in J \end{cases} \tag{6}$$

where z_j is a variable for the private share of the participant $j \in J$ (the participants in I do not know the private shares of the participants in J).

The only variable (non-determinate) of (5) is x, while the variables of (6) are x and z_j for all $j \in J$. According to the way private shares where computed for participants in U_2, z_j may take any value in $\mathbb{Z}_{m_j}$ with equal probability, for all $j \in J$.

Any solution α to the system (5) leads to a unique solution (α, β_J) to the system (6), where $\beta_J(j) = \alpha - w_J(j) \bmod m_j$, for all $j \in J$. Conversely, if (α, β_J) is a solution to the system (6), then α is a solution to the system (5). Moreover, for a given vector β_J of solutions to the vector z_J of variables, there exists exactly one solution α to x.

As a consequence, the number of solutions to (5) equals the number of solutions to (6), and the number of solutions to (5) with $x = s$ equals the number of solutions to (6) with $x = s$. As the probabilities in (4) are computed as a fraction of the number of solutions with $x = s$ by the total number of solutions, we deduce that (4) must hold. ■

Lemma 2.2. *For any realization of the Asmuth-Bloom secret sharing scheme with public shares there exists a realization with the same loss of entropy of the Asmuth-Bloom secret sharing scheme (without public shares) and vice-versa.*

Proof. Let (U_1, U_2) be a partition of $U = \{1, \ldots, n\}$, t be an integer such that $0 < t + 1 \leq n$, and Γ be the $(t+1)$-threshold access structure over U.

If a sequence $m_0, m_1, \ldots, m_n$ of co-primes defines a realization of the Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over (U_1, U_2), then the same sequence of co-primes defines a realization of the Asmuth-Bloom secret sharing scheme over $U = U_1 \cup U_2$. Given $I \subseteq U$, $J \subseteq U_2 \setminus I$, $y_I \in \overline{\Pi}_I$, and $w_J \in \Pi_J$, consider $y'_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ defined as follows:

- $y'_I(i) = y_I(i)$, for all $i \in I \cap U_1$;
- $y'_I(i) = (y_i + w_i) \bmod m_i$, for all $i \in I \cap U_2$, where $y_I(i) = (y_i, w_i)$.

It is clear that $\Delta(y_I) = \Delta(y'_I)$ (the same system (6) of congruences is used to compute the loss of entropy both in the case when $m_0, m_1, \ldots, m_n$ defines a realization of the Asmuth-Bloom secret sharing scheme with public shares for $(t+1, \Gamma)$ over (U_1, U_2) and in the case when $m_0, m_1, \ldots, m_n$ defines a realization of the Asmuth-Bloom secret sharing scheme for $(t + 1, \Gamma)$ over U). Lemma 2.1 leads to $\Delta(y_I, w_J) = \Delta(y_I)$ and, therefore, $\Delta(y_I, w_J) = \Delta(y'_I)$.

Vice-versa, if $m_0, m_1, \ldots, m_n$ defines a realization of the Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over U, then the same sequence of co-primes defines a realization of the Asmuth-Bloom secret sharing scheme for $(t+1, \Gamma)$ over (U_1, U_2). Given $I \subseteq U$, $J \subseteq U_2 \setminus I$, consider $y'_I \in \overline{\Pi}_I$ defined as follows:

- $y'_I(i) = y_I(i)$, for all $i \in I \cap U_1$;
- $y'_I(i) = (y_i, w_i)$, where y_i is randomly chosen from $\mathbb{Z}_{m_i}$ and $w_i \in \mathbb{Z}_{m_i}$ is computed such that $y_I(i) \equiv (y_i + w_i) \bmod m_i$, for all $i \in I \cap U_2$.

To prove soundness of y'_I we need to show $w_i \equiv (s' - y_i) \bmod m_i$, where s' is the secret used to define y_I (that is, $y_I(i) = s' \bmod m_i$), for all $i \in I \cap U_2$. This is simply obtained as follows:

$$w_i \equiv_{m_i} (y_I(i) - y_i) \equiv_{m_i} s' - y_i.$$

Now, exactly as in the first part of the proof, using Lemma 2.1, we obtain

$$\Delta(y_I) = \Delta(y'_I) = \Delta(y'_I, w_J),$$

for any $w_J \in \Pi_J$. ■

In [10] it was shown that the Asmuth-Bloom secret sharing scheme is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes. We intend to prove the same result for the Asmuth-Bloom secret sharing scheme with private shares. Recall first a few concept and results from [10].

Definition 2.4. *Let $L = (m_0, m_1, \ldots, m_n)$ be a sequence of co-primes.*

1. *The sequence L is called* (k, θ)-compact, *where $k \geq 1$ and $\theta \in (0,1)$ are real numbers, if $m_0 < m_1 < \cdots < m_n$ and $km_0 < m_i < km_0 + m_0^\theta$, for all $1 \leq i \leq n$.*
2. *The sequence L is called* k-compact *if it is (k, θ)-compact for some real $\theta \in (0,1)$.*

For the sake of terminology, 1-compact sequences of co-primes will also be called *compact sequences of co-primes.*

Remark 2.1. *For sufficiently large m_0, k-compact sequences $m_0, m_1, \cdots, m_n$ of co-primes with $k > 1$ satisfy the Asmuth-Bloom constraint. Indeed, let $\theta \in (0,1)$ be such that $m_0 < m_1 < \cdots < m_n$ and $km_0 < m_i < km_0 + m_0^\theta$, for all $1 \leq i \leq n$. As*

$$\lim_{m_0 \to \infty} \frac{m_0(km_0 + m_0^\theta)^t}{(km_0)^{t+1}} = \frac{1}{k} < 1$$

it follows that $(km_0)^{t+1} > m_0(km_0 + m_0^\theta)^t$ for sufficiently large m_0. Then,

$$\prod_{i=1}^{t+1} m_i > (km_0)^{t+1} > m_0(km_0 + m_0^\theta)^t > m_0 \prod_{i=0}^{t-1} m_{n-i},$$

which shows that $m_0, m_1, \cdots, m_n$ is an Asmuth-Bloom sequence of co-primes for sufficiently large m_0.

The Asmuth-Bloom secret sharing scheme (with or without public shares) can be changed by replacing the Asmuth-Bloom sequences of co-primes in the parameter setup phase by k-compact sequences of co-primes. We will refer to the scheme such obtained as being the *Asmuth-Bloom secret sharing scheme (with or without public shares) based on k-compact sequences of co-primes.*

The previous results and remarks do not depend on the sequence type of co-primes under which the Asmuth-Bloom secret sharing scheme (with or without public shares) is based on. That is, they all hold as well if the Asmuth-Bloom secret sharing scheme (with or without public shares) is based on k-compact sequences of co-primes.

The following important result was established in [10].

Theorem 2.2 ([10]). *Let $k \geq 1$ be an integer.*

1. *The Asmuth-Bloom secret sharing 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.*

2. *The Asmuth-Bloom secret sharing 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.*

As a conclusion, we obtain the following important results.

Corollary 2.1. *The Asmuth-Bloom secret sharing scheme with public shares 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. Directly from Theorem 2.2 and Lemma 2.2. ■

Remark 2.2. *It was shown in [9] (Proposition 4.6.7 on page 118) that the Asmuth-Bloom secret sharing scheme is not asymptotically perfect if it is based on k-compact sequences of co-primes where $k > 1$ is real but not an integer. In the view of Lemma 2.2, this remark holds true for the Asmuth-Bloom secret sharing scheme with public shares as well.*

Remark 2.3. *The utilization of compact sequences to define realizations of the Asmuth-Bloom secret sharing scheme (with or without public shares) instead of Asmuth-Bloom sequences of co-primes has not only the advantage of providing good security. It also provides important advantages when one wants to add new participants to or change the threshold of some current realization.*

Assume that we want to add a new participant to an Asmuth-Bloom secret sharing realization given by a compact sequence L of co-primes. We may assume that m_0 and θ are chosen so that the interval $(m_0 - m_0^\theta, m_0 + m_0^\theta)$ accommodates much larger sequences of co-primes than L (in practice, L might consist of a few hundred co-primes, while $(m_0 - m_0^\theta, m_0 + m_0^\theta)$ may easily accommodate sequences of tens of thousand co-primes). Therefore, what we have to do in order to add a new participant is to extend L by a new modulus. This can *be simply done by repeatedly incrementing the last co-prime of L until a new co-prime is reached (see Algorithm 1 in Section 5 for details on how this can be done). For Asmuth-Bloom sequences, this methodology of adding new participants might easily violate the Asmuth-Bloom constraint and so, it might require the generation of a new Asmuth-Bloom sequence.*

Changing the threshold of the scheme does not require modification of the current sequence of co-primes if it is compact (but it does if it is an Asmuth-Bloom sequence).

3. Applications

Threshold access structures are suitable when participants have the same degree of trust. However, many real-world applications need more complex access structures based on partitioning the participants into groups with different privileges. *Multilevel* (also called *hierarchical*) [24, 13] and *compartmented* [24] access structures are two important classes of access structures proposed to cope with this problem. In both of them, the set of participants is partitioned into groups called *levels* (in the case of multilevel access structures) or *compartments* (in the case of compartmented access structures). To these groups thresholds are assigned on whose basis authorized sets are defined.

In this section we illustrate how the Asmuth-Bloom secret sharing scheme with public shares can be used to define efficient CRT-based secret sharing schemes for multilevel and compartmented access structures.

3.1. Multilevel Access Structures: the Disjunctive Case

In a multilevel access structure [24, 13] the users are distributed on levels. A threshold is assigned to each level and the increasing order of thresholds defines a total order on levels. The level with the least threshold is the highest privileged level, while the level with the highest threshold is the least privileged level. A participant in some level can act in any level less privileged than his/her own level. The *disjunctive* and the *conjunctive* access structures are two main approaches to define authorized sets in multilevel access structures. The first one is the topic of this sub-section, while the second one will be considered in the next sub-section.

A *disjunctive multilevel access structure* (DMAS) over a finite set U of participants [24] [1] is a tuple $(\overline{U}, \bar{t}, \Gamma)$, where:

- $\overline{U} = (U_1, \ldots, U_q)$ is a partition of U into $q \geq 1$ non-empty subsets called *levels* (the number of participants in U_i is n_i, for all $1 \leq i \leq q$, and n is the number of all participants in U);
- $\bar{t} = (t_1 + 1, \ldots, t_q + 1)$ is a vector of strictly positive integers called *thresholds* that satisfy $0 \leq t_1 < \cdots < t_q$ and $\sum_{i=1}^{\ell} n_i \geq t_\ell + 1$ for all $1 \leq \ell \leq q$;

[1] Simmons [24] called them *multilevel access structures*. Later, Tassa [25] and Beimel et al. [3] called them *hierarchical threshold access structures* (HTAS), and Belenkiy [4] called them *disjunctive multilevel access structures* and used *conjunctive multilevel access structures* for the access structures introduced by Tassa.

- Γ is the set of all *authorized sets* defined by

$$\Gamma = \{A \subseteq U | (\exists 1 \leq \ell \leq q)(|A \cap (\cup_{i=1}^{\ell} U_i)| \geq t_\ell + 1)\}.$$

As one can see, the participants on the levels $U_1, \ldots, U_{\ell-1}$ can act as participants on level ℓ in authorized sets A with $|A \cap (\cup_{i=1}^{\ell} U_i)| \geq t_\ell + 1$, in order to recover the secret.

In what follows in this section, the notation for any DMAS $(\overline{U}, \bar{t}, \Gamma)$ over U is as above. Moreover, given $A \subseteq U$ we abuse notation and write $(i,j) \in A$ instead of $j \in A \cap U_i$ to denote the jth participant of U_i.

We will provide CRT-based realizations of DMASs $(\overline{U}, \bar{t}, \Gamma)$ by sequences of co-primes of length $n+1$

$$L: \quad m_0, m_{1,1}, \ldots, m_{1,n_1}, \ldots, m_{q,1}, \ldots, m_{q,n_q} \tag{7}$$

with the following two properties:

1. m_0 is the least element of the sequence L;

2. $m_{i,1} < \cdots < m_{i,n_i}$, for all $1 \leq i \leq q$.

The integer $m_{i,j}$ is the *modulus associated to* (i,j).

Two important notations with respect to the sequence L of co-primes and a level i, $1 \leq i \leq q$, are in order:

1. L_i denotes the sub-sequence of L given by

$$L_i: \quad m_0, m_{1,1}, \ldots, m_{1,n_1}, \ldots, m_{i,1}, \ldots, m_{i,n_i}; \tag{8}$$

2. $min(t_i + 1, L_i)$ denotes the set of the least $t_i + 1$ integers in $L_i \setminus \{m_0\}$.

Now we are able to describe our CRT-based secret sharing scheme for a DMAS $(\overline{U}, \bar{t}, \Gamma)$. The main idea is to give a private share to each participant (i,j), and to compute public shares for (i,j) on each level $\ell > i$.

Scheme 2: CRT-DMAS SSS for $(\overline{U}, \bar{t}, \Gamma)$

(1) *parameter setup:* consider L a sequence of co-primes as in (7). L and $\bar{t}$ are public parameters. Define the *secret space* as $\mathbb{Z}_{m_0}$. For each (i,j), $\mathbb{Z}_{m_{i,j}}$ is the *private share space* of the participant (i,j) and the *public share space* of the participant (i,j) on the level ℓ, for each $i < \ell \leq q$;

(2) *secret sharing:* each secret s is shared to the participants as follows:

(a) for each level i, $1 \leq i \leq q$, a *level secret* s_i is computed in the form

$$s_i = s + r_i m_0 < \prod_{x \in min(t_i+1, L_i)} x,$$

where $r_i \geq 0$ is randomly chosen;

(b) each participant (i,j) receives a private share $s_{i,j} = s_i \bmod m_{i,j}$ and $q-i$ shares $w_{i,j}^{i+1}, \ldots, w_{i,j}^{q}$ corresponding to the levels $i+1, \ldots, q$, respectively, are broadcast as public information. These public shares are computed by

$$w_{i,j}^{\ell} = (s_\ell - s_{i,j}) \bmod m_{i,j},$$

for all $i+1 \leq \ell \leq q$;

(3) *secret reconstruction:* assume $A \in \Gamma$ and ℓ is a level such that $|A \cap (\cup_{i=1}^{\ell} U_i)| \geq t_\ell + 1$. The participants in A can uniquely reconstruct the secret s by computing first the unique solution modulo $\prod_{(i,j)\in A} m_{i,j}$ of the system

$$\begin{cases} x \equiv s_{\ell,j} \bmod m_{\ell,j}, & \forall(\ell,j) \in A \\ x \equiv (s_{i,j} + w_{i,j}^{\ell}) \bmod m_{i,j}, & \forall(i,j) \in A \\ & \text{with } i < \ell \end{cases}$$

and then reducing it modulo m_0.

It is straightforward to prove the soundness of our CRT-DMAS secret sharing scheme (s_ℓ is recovered as in the Asmuth-Bloom secret sharing scheme with public shares; then, s is obtained by modulo m_0 reduction).

Any DMAS $(\overline{U}, \overline{t}, \Gamma)$ gives rise to a *level* $(t_\ell + 1)$*-threshold access structure* Γ_ℓ over $(U_\ell, \cup_{i=1}^{\ell-1} U_i)$,

$$\Gamma_\ell = \{A \subseteq \cup_{i=1}^{\ell} U_i \mid |A| \geq t_\ell + 1\},$$

for each $1 \leq \ell \leq q$.

Any realization of the CRT-DMAS for $(\overline{U}, \overline{t}, \Gamma)$ gives rise to a realization for the Asmuth-Bloom secret sharing scheme for $(t_\ell + 1, \Gamma_\ell)$ over $(U_\ell, \cup_{i=1}^{\ell-1} U_i)$, for all $1 \leq \ell \leq q$. Namely, this realization uses the sequence L_ℓ of co-primes and takes into account the private shares of the participants on the levels $U_1, \ldots, U_\ell$, as well as the public shares on level ℓ of the participants in $U_1, \ldots, U_{\ell-1}$.

The security of the CRT-DMAS secret sharing scheme can be similarly introduced as for the Asmuth-Bloom secret sharing scheme with public shares. The only thing we have to do is to redefine the ranges for the random variables Y_I and W_J. Thus, using the notation in Scheme 2, we assume that:

- Y_I takes values into $\overline{\Pi}_I = \prod_{(i,j)\in I} \overline{\mathbb{Z}}_{m_{i,j}}$, where $\overline{\mathbb{Z}}_{m_{i,j}} = \mathbb{Z}_{m_{i,j}}^{q-i+1}$;
- W_J takes values into $\tilde{\Pi}_J = \prod_{(i,j)\in J} \tilde{\mathbb{Z}}_{m_{i,j}}$, where $\tilde{\mathbb{Z}}_{m_{i,j}} = \mathbb{Z}_{m_{i,j}}^{q-i}$.

An output of Y_I gives information about the private shares and the public shares of the participants in I, while an output of W_J gives information about the public shares of the participants in J. As an example, if y_I is an output of Y_I and $(i,j) \in I$, then $y_I(i,j)$ has the form $y_I(i,j) = (s_{i,j}, w_{i,j}^{i+1}, \ldots, w_{i,j}^{q})$ (see Scheme 2 for notation).

Then, the loss of entropy, asymptotic perfectness, and asymptotic idealness can be defined as in Section 2.2. The next theorem establishes the security of our CRT-DMAS scheme.

Theorem 3.1. *The CRT-DMAS secret sharing 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. We will prove first that, given a level $1 \leq \ell \leq q$ and a unauthorized set A, the public information corresponding to the levels $r \neq \ell$ do not leak any supplementary information to A in order to recover the secret s_ℓ (using the same notation as in the CRT-DMAS scheme description).

The system of equations corresponding to A and to the level ℓ is

$$\begin{cases} x_\ell \equiv s_{i,j} + w^\ell_{i,j} \bmod m_{i,j} & \forall (i,j) \in A,\ i < \ell \\ x_\ell \equiv s_{\ell,j} \bmod m_{\ell,j} & \forall (\ell,j) \in A \\ x_\ell \equiv z_{i,j} + w^\ell_{i,j} \bmod m_{i,j} & \forall (i,j) \notin A,\ i < \ell \\ x_\ell \equiv z_{\ell,j} \bmod m_{\ell,j} & \forall (\ell,j) \notin A \end{cases} \tag{9}$$

while the system of equations corresponding to A in the entire scheme is

$$\begin{cases} x_\ell \equiv s_{i,j} + w^\ell_{i,j} \bmod m_{i,j} & \forall (i,j) \in A,\ i < \ell \\ x_\ell \equiv s_{\ell,j} \bmod m_{\ell,j} & \forall (\ell,j) \in A \\ x_\ell \equiv z_{i,j} + w^\ell_{i,j} \bmod m_{i,j} & \forall (i,j) \notin A,\ i < \ell \\ x_\ell \equiv z_{\ell,j} \bmod m_{\ell,j} & \forall (\ell,j) \notin A \\ x_r \equiv s_{i,j} + w^r_{i,j} \bmod m_{i,j} & \forall (i,j) \in A,\ r \neq \ell,\ i < r \\ x_r \equiv s_{r,j} \bmod m_{r,j} & \forall (r,j) \in A,\ r \neq \ell \\ x_r \equiv z_{i,j} + w^r_{i,j} \bmod m_{i,j} & \forall (i,j) \notin A,\ r \neq \ell,\ i < r \\ x_r \equiv z_{r,j} \bmod m_{r,j} & \forall (r,j) \notin A,\ r \neq \ell \end{cases} \tag{10}$$

where x's are level secret variables and z's are private share variables.

A solution to (9) has the form

$$(\overline{x}_\ell, (\overline{z}_{i,j} \mid (i,j) \notin A,\ i \leq \ell))$$

and a solution to (10) has the form

$$((\overline{x}_i \mid 1 \leq i \leq q), (\overline{z}_{i,j} \mid (i,j) \notin A)).$$

If $(\overline{x}_\ell, (\overline{z}_{i,j} \mid (i,j) \notin A,\ i \leq \ell))$ is a solution to (9), then one may simply obtain a solution to (10) as follows: assign values to all variables $z_{i,j}$ with $(i,j) \notin A$ and $i > \ell$, and then use CRT to get unique values for all x_i with $i \neq \ell$. Moreover, distinct assignments to the variables $z_{i,j}$ as above give rise to distinct values for at least one variable x_i with $i \neq \ell$ (this follows from the CRT).

There is one more important property that we need, namely: distinct solutions to (9) leads to the same number of solutions to (10). Let α be the number of solutions to (10) obtained from a solution to (9), $Sol(n)$ be the number of solutions to the system (n) of equations, and $Sol(n, x_\ell) = s_\ell)$ be the number of solutions with $x_\ell = s_\ell$ to the system (n) of equations, where $n = 9, 10$. Then,

$$\frac{Sol(10, x_\ell = s_\ell)}{Sol(10)} = \frac{Sol(9, x_\ell = s_\ell) \cdot \alpha}{Sol(9) \cdot \alpha} = \frac{Sol(9, x_\ell = s_\ell)}{Sol(9)}$$

This property shows that the probability of computing s_ℓ by means of (10) is exactly the probability of computing s_ℓ by means of (9). Plugging this into the definition of loss of entropy, we obtain that the loss of entropy associated to A in the CRT-DMAS scheme when recovering s_ℓ is exactly the loss of entropy associated to A in the Asmuth-Bloom scheme with public shares for the level ℓ.

As a consequence of the above discussion, we obtain:

Fact 1: The CRT-DMAS secret sharing scheme for $(\overline{U}, \overline{t}, \Gamma)$ is asymptotically ideal if and only if the Asmuth-Bloom secret sharing schemes with public shares for its level threshold access structures, are all asymptotically ideal.

We need one more remark before developing the proof of the theorem, namely:

Fact 2: A sequence L of co-prime integers as in (7) is 1-compact if and only if the sub-sequences L_i as in (8), $1 \leq i \leq q$, are all 1-compact.

Now, the proof of the theorem works as follows. If the CRT-DMAS secret sharing scheme for $(\overline{U}, \overline{t}, \Gamma)$ is based on 1-compact sequences of co-primes, then the Asmuth-Bloom secret sharing schemes with public shares for its level threshold access structures are all based on 1-compact sequences of co-primes (Fact 2). Then, Corollary 2.1 shows that all these Asmuth-Bloom secret sharing schemes with public shares are asymptotically ideal, and Fact 1 leads to the asymptotic idealness of the CRT-DMAS secret sharing scheme for $(\overline{U}, \overline{t}, \Gamma)$.

Conversely, if the CRT-DMAS secret sharing scheme for $(\overline{U}, \overline{t}, \Gamma)$ is asymptotically ideal, then the Asmuth-Bloom secret sharing schemes with public shares for the level threshold access structures are asymptotically ideal (Fact 1). Corollary 2.1 shows then that these schemes are based on 1-compact sequences of co-primes. We apply now Fact 2 and deduce that CRT-DMAS secret sharing scheme for $(\overline{U}, \overline{t}, \Gamma)$ is based on 1-compact sequences of co-primes. ■

3.2. Multilevel Access Structures: the Conjunctive Case

Conjunctive multilevel access structures have been proposed in [25] under the name of hierarchical threshold access structures. The terminology of conjunctive access structures was coined in [4] to make distinction between them and disjunctive access structures (both conjunctive and disjunctive access structures being sub-families of the family of hierarchical access structures).

Unlike disjunctive access structures, authorized sets in conjunctive access structures must exceed each threshold level. This means that authorized sets must be able to recover all level secrets. As a conclusion, conjunctive access structures are suitable when the master secret is firstly shared on levels and then, each level secret is shared to participants.

A *conjunctive multilevel access structure* (CMAS) over a finite set U of participants is a tuple $(\overline{U}, \overline{t}, \Gamma)$, where:

- $\overline{U} = (U_1, \ldots, U_q)$ is a partition of U into $q \geq 1$ non-empty subsets called *levels* (the number of participants in U_i is n_i, for all $1 \leq i \leq q$, and n is the number of all participants in U);
- $\overline{t} = (t_1 + 1, \ldots, t_q + 1)$ is a vector of strictly positive integers called *thresholds* that satisfy $0 \leq t_1 < \cdots < t_q$ and $n_i \geq t_i + 1$ for all $1 \leq i \leq q$;
- Γ is the set of all *authorized sets* defined by

$$\Gamma = \{A \subseteq U | (\forall 1 \leq \ell \leq q)(|A \cap (\cup_{i=1}^{\ell} U_i)| \geq t_\ell + 1)\}.$$

We will further use the same terminology and notation as introduced in Section 3.1 to propose and analyze our CRT-based secret sharing scheme for conjunctive access structures.

Scheme 3: CRT-CMAS SSS for $(\overline{U}, \bar{t}, \Gamma)$

(1) *parameter setup:* consider L a sequence of co-primes as in (7). L and $\bar{t}$ are public parameters. Define the *secret space* as $\mathbb{Z}_{m_0}$. For each (i,j), $\mathbb{Z}_{m_{i,j}}$ is the *private share space* of the participant (i,j) and the *public share space* of the participant (i,j) on the level ℓ, for each $i \leq \ell \leq q$;

(2) *secret sharing:* each secret s is shared to the participants as follows:

(a) split the secret into q pieces

$$s = s_1 + \cdots + s_q \bmod m_0$$

by means of the Karnin-Greene-Hellman scheme [18]. That is, $s_1, \ldots, s_{q-1}$ are randomly and independently chosen from $\mathbb{Z}_{m_0}$, and s_q is computed as

$$s_q = (s - s_1 - \cdots - s_{q-1}) \bmod m_0;$$

(b) for each level i, $1 \leq i \leq q$, a *level secret* s'_i is computed in the form

$$s'_i = s_i + r_i m_0 < \prod_{x \in min(t_i+1, L_i)} x,$$

where $r_i \geq 0$ is randomly chosen;

(c) each participant (i,j) receives the private share $s_{i,j} = s'_i \bmod m_{i,j}$ and $q-i$ shares $w_{i,j}^{i+1}, \ldots, w_{i,j}^{q}$ corresponding to the levels $i+1, \ldots, q$, respectively, are broadcast as public information. These shares are computed by

$$w_{i,j}^{\ell} = (s'_\ell - s_{i,j}) \bmod m_{i,j},$$

for all $i+1 \leq \ell \leq q$;

(3) *secret reconstruction:* assume $A \in \Gamma$. Then, $|A \cap (\cup_{i=1}^{\ell} U_i)| \geq t_\ell + 1$ for all $1 \leq \ell \leq q$. The participants in A can uniquely reconstruct the secret s as follows:

- for each $\ell \in \{1, \ldots, q\}$, s_ℓ is recovered by computing first the unique solution modulo $\prod_{(i,j) \in A, \, i \leq \ell} m_{i,j}$ of the system

$$\begin{cases} x \equiv s_{\ell,j} \bmod m_{\ell,j}, & \forall (\ell,j) \in A \\ x \equiv (s_{i,j} + w_{i,j}^{\ell}) \bmod m_{i,j}, & \forall (i,j) \in A \\ & \text{with } i < \ell \end{cases}$$

and then reducing it modulo m_0;

- the secret s is obtained then by

$$s = (s_1 + \cdots + s_q) \bmod m_0.$$

It is straightforward to prove that our CRT-CMAS secret sharing scheme is sound. As with respect to its security, this can be defined as we did for the CRT-DMAS scheme. Then, we have the following result.

Theorem 3.2. *The CRT-CMAS secret sharing 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. Recall first that the Karnin-Greene-Hellman secret sharing scheme is ideal (Theorem 41 in [21]). Therefore, when a secret s is shared into q pieces (see the CRT-CMAS scheme description), then:

1. each share is uniformly at random distributed in the secret space (assuming that s is uniformly at random chosen from the secret space);

2. less than q shares do not leak any information about s.

Now, the proof follows a similar line to the proof of Theorem 3.1. ■

3.3. Compartmented Access Structures

A *compartmented access structure* (CAS) [24] over a finite set U of participants is a tuple $(\overline{U}, \overline{t}, t+1, \Gamma)$, where:

- $\overline{U} = (U_1, \ldots, U_q)$ is a partition of U into $q \geq 1$ non-empty subsets called *compartments* (the number of participants in U_i is n_i, for all $1 \leq i \leq q$, and n is the number of all participants in U);

- $\overline{t} = (t_1+1, \ldots, t_q+1)$ is a vector of strictly positive integers called *thresholds* that satisfy $0 < t_i + 1 \leq n_i$ for all $1 \leq i \leq q$;

- t is a global threshold satisfying $\sum_{i=1}^{q}(t_i+1) \leq t+1 \leq \sum_{i=1}^{q} n_i$;

- Γ is the set of all *authorized sets* defined by

$$\Gamma = \{A \subseteq U | (\forall 1 \leq i \leq q)(|A \cap U_i| \geq t_i + 1) \ \wedge \ (|A| \geq t+1)\}.$$

The requirement "$(\forall 1 \leq i \leq q)(|A \cap U_i| \geq t_i + 1)$" says that A should include enough participants from each compartment U_i in order to recover some "compartment secret"; the requirement "$|A| \geq t+1$" says that A should be large enough in order to recover some "global secret".

We will provide CRT-based realizations of CASs by sequences L of co-primes as in (7). Unlike the notation used in Section 3.1, the sub-sequence L_i in this case is

$$L_i : \quad m_0, m_{i,1}, \ldots, m_{i,n_i}$$

for any $1 \leq i \leq q$. Moreover, define $L_{q+1} = L$.

Now we are able to describe our proposal of a CRT-based secret sharing scheme for a CAS $(\overline{U}, \overline{t}, t+1, \Gamma)$. The main idea is to split the secret into $q+1$ pieces. The first q pieces must be reconstructed along the q level, while the last piece must be reconstructed on the level $q+1$ where the threshold is $t+1$. Due to the fact that a participant is allowed to recover the secret only on his level, each participant will have only two public shares, one to recover the secret on his level and the other one to recover the secret on the level $q+1$.

Scheme 4: CRT-CAS SSS for $(\overline{U}, \bar{t}, t+1, \Gamma)$

(1) *parameter setup:* consider L a sequence of co-primes as in (7). L, $\bar{t}$, and t are public parameters. Define the *secret space* as $\mathbb{Z}_{m_0}$. For each (i,j), $\mathbb{Z}_{m_{i,j}}$ is both the *private* and *public share space* of the participant (i,j);

(2) *secret sharing:* each secret s is shared to the participants as follows:

(a) split the secret into $q+1$ pieces

$$s = s_1 + \cdots + s_{q+1} \bmod m_0$$

by means of the Karnin-Greene-Hellman scheme [18]. That is, $s_1, \ldots, s_q$ are randomly and independently chosen from $\mathbb{Z}_{m_0}$, and s_q is computed as

$$s_{q+1} = (s - s_1 - \cdots - s_q) \bmod m_0;$$

(b) for each i, $1 \leq i \leq q+1$, a *secret* s'_i is computed in the form of

$$s'_i = s_i + r_i m_0 < \prod_{x \in min(t_i+1, L_i)} x,$$

where $r_i \geq 0$ is randomly chosen;

(c) each participant (i,j) receives the private share $s_{i,j} = s'_i \bmod m_{i,j}$ and the public share

$$w_{i,j} = (s'_{q+1} - s_{i,j}) \bmod m_{i,j}$$

is broadcast as public information;

(3) *secret reconstruction:* assume $A \in \Gamma$. Then, $|A \cap U_i| \geq t_i + 1$ for all $1 \leq i \leq q$ and $|A| \geq t+1$. The participants in A can uniquely reconstruct the secret s as follows:

- for each $i \in \{1, \ldots, q\}$, s_i is recovered by computing first the unique solution modulo $\prod_{(i,j) \in A,\, j \in U_i} m_{i,j}$ of the system

$$\left\{ x \;\equiv\; s_{i,j} \bmod \; m_{i,j}, \quad \forall j \in U_i \,:\, (i,j) \in A \right.$$

and then reducing it modulo m_0;

- s_{q+1} is recovered by computing first the unique solution modulo $\prod_{(i,j) \in A} m_{i,j}$ of the system

$$\left\{ x \;\equiv\; (s_{i,j} + w_{i,j}) \bmod \; m_{i,j}, \quad (i,j) \in A \right.$$

and then reducing it modulo m_0;

- the secret s is obtained then by

$$s = (s_1 + \cdots + s_{q+1}) \bmod m_0$$

It is straightforward to prove that our CRT-CAS secret sharing scheme is sound.

Any CAS $(\overline{U}, \bar{t}, t+1, \Gamma)$ gives rise to $q+1$ threshold access structures as follows:

1. a (t_i+1)-threshold access structure Γ_i over $(U_i, \emptyset)$,
$$\Gamma_i = \{A \subseteq U_i \mid |A| \geq t_i + 1\},$$
for all $1 \leq i \leq q$;
2. a $(t+1)$-threshold access structure Γ_{q+1} over $(\emptyset, U)$,
$$\Gamma_{q+1} = \{A \subseteq U \mid |A| \geq t + 1\}.$$

Any realization of the CRT-CAS $(\overline{U}, \bar{t}, t+1, \Gamma)$ gives rise to a realization for the Asmuth-Bloom secret sharing scheme for $(t_\ell+1, \Gamma_\ell)$ over $(U_\ell, \emptyset)$, if $1 \leq \ell \leq q$, and over $(U, \emptyset)$, if $\ell = q+1$, where $t_{q+1} = t$. Namely, this realization uses the sequence L_ℓ of co-primes and takes into account only the private shares for $\ell \leq q$, and the private and public shares for $\ell = q+1$.

The security of the CRT-CAS secret sharing scheme is settled by the following theorem (the corresponding concepts are introduced as for the CRT-DMAS scheme).

Theorem 3.3. *The CRT-CAS secret sharing 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. It follows a similar line to the proof of Theorem 3.1 or Theorem 3.2, by taking also in the account the fact that the Karnin-Greene-Hellman secret sharing scheme is ideal (Theorem 41 in [21]). ■

4. Extensions

In Section 2, the Asmuth-Bloom secret sharing scheme has been extended so that some participants to the scheme can broadcast "parts" of their shares as public information. We have proved that this scheme extension, called the Asmuth-Bloom secret sharing scheme with public information, is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes. Although this extension might not be relevant for threshold access structures, it is however important because it allows a unitary and elegant development of asymptotically ideal CRT-based secret sharing schemes for multilevel and compartmented access structures (Section 3).

There is another well-known CRT-based secret sharing scheme for threshold access structures that is asymptotically ideal when it is based on 1-compact sequences of co-primes. Namely, this is the Goldreich-Ron-Sudan (GRS) secret sharing scheme [7]. In this context, the question is whether or not this scheme can be extended to accommodate public shares and then if it can be used to develop asymptotically ideal CRT-based secret sharing schemes for multilevel and compartmented access structures. The answer to this question is positive and we will detail it here. Let us recall first the GRS secret sharing scheme as it is described in [7]. Assume Γ is a $(t+1)$-threshold access structure over a set U of n participants, where $0 < t+1 \leq n$.

Scheme 5: GRS SSS for $(U, t+1, \Gamma)$

(1) *parameter setup:* choose an increasing sequence of co-primes $m_0 < m_1 < \cdots < m_n$. The integers $t, n, m_0, m_1, \ldots, m_n$ are public parameters. The secret space is $\mathbb{Z}_{m_0}$ and the private share space of the ith participant is $\mathbb{Z}_{m_i}$, for all $1 \leq i \leq n$;

(2) *secret sharing:* given $s \in \mathbb{Z}_{m_0}$, randomly choose r_i from $\mathbb{Z}_{m_i}$ for all $1 \leq i \leq t$ and compute s' the unique solution modulo $m_0 \prod_{i=1}^{t} m_i$ of the system

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

where $r_0 = s$. Then, share s by $s_i = s' \; mod \; m_i$, for all $1 \leq i \leq n$;

(3) *secret reconstruction:* any $A \in \Gamma$ can uniquely reconstruct the secret s by computing first the unique solution modulo $\prod_{i \in A} m_i$ of the system

$$x \equiv s_i \; mod \; m_i, \quad i \in A, \tag{11}$$

and then reducing it modulo m_0.

The correctness of the reconstruction step above is as follows: by solving the system (11) of congruences one obtains the unique solution s' modulo $\prod_{i \in A} m_i$. As $\prod_{i \in A} m_i > m_0 \prod_{i=1}^{t} m_i$ and s' is a solution to the system (11) of congruences, it follows $s = s' \bmod m_0$.

It has been shown in [7] that the GRS secret sharing scheme is asymptotically ideal if and only if it is based on 1-compact sequences of co-primes.

The differences between the Asmuth-Bloom and GRS secret sharing schemes consists of:

1. the Asmuth-Bloom secret sharing scheme uses Asmuth-Bloom sequences of co-primes while the GRS secret sharing scheme uses strictly increasing sequences of co-primes;

2. the schemes make use of different probabilistic procedures in the secret sharing phase to map secrets from $\mathbb{Z}_{m_0}$ to integers into a larger space ($\prod_{i=1}^{t+1} m_i$ in the case of the Asmuth-Bloom scheme and $m_0 \prod_{i=1}^{t} m_i$ in the case of the GRS scheme).

None of these two differences prevent the extension of the GRS scheme to accommodate public shares or its usability to develop secret sharing schemes for multilevel or compartmented access structures. Therefore, one may develop similar results to those in Sections 2 and 3 by simply replacing the Asmuth-Bloom secret sharing scheme by the GRS secret sharing scheme.

One may also think to use the Mignotte secret sharing scheme [20] instead of the Asmuth-Bloom secret sharing scheme in Section 2. Although this is possible, we do not recommend it because the Mignotte secret sharing scheme has poor security properties [2].

5. Implementation Issues

The efficient implementation of the schemes proposed in this paper depend on the efficiency of the following operations:

1. generation of 1-compact sequences of co-primes;
2. generation of random numbers;
3. performing modular reduction;
4. computing solutions to systems of congruences (by CRT).

Efficient algorithms are already known for the last three operations; as for the generation of compact sequences of co-primes, the following simple Algorithm 1 turns out to be quite efficient.

Algorithm 1 Generation of 1-compact sequences of co-primes

```
procedure COMPACT_GEN($m_0, \theta, n$)        ▷ $m_0$ is odd, $\theta \in (0,1)$, and $n \geq 1$
    $i := 0$
    $L(0) := m_0$
    $current := m_0 + 2$
    $exit := m_0 + m_0^\theta$
    repeat
        if $current$ co-prime to $L(0), \ldots, L(i)$ then
            $i := i + 1$
            $L(i) := current$
            $current := current + 2$
        else
            $current := current + 2$
        end if
    until $i = n$ or $current \geq exit$
    return $L(0), \ldots, L(i)$
end procedure
```

We have coded this algorithm in `C++` with the NTL library for large integers (`http://www.shoup.net/ntl/`) and we have performed a few tests on a laptop Intel Core I3 at 2.40GHz with 4GB RAM. We have counted the time needed to generate compact sequences of various lengths, the dispersion of the sequence (i.e., the maximum difference between two consecutive co-primes in sequence), and the average dispersion. The results are reported in Table 1. On our laptop, the generation of a 512-bit prime took on average 0.4509 seconds. This is more than the generation of a length 100 compact sequence of co-primes.

Due to the fact that the realizations of our secret sharing schemes are based on compact sequences of co-primes, adding new participants to or changing the thresholds in a given realization is very easy. The arguments are similar to the ones in Remark 2.3. Additionally, we remark that in a given realization based on a compact sequence L of co-primes we have imposed total orders only on the moduli of the participants on the same level; otherwise, the moduli may be interleaved. As a conclusion, if we want to add a new participant to the level i, we simply extend L to the right by a new co-prime. Changing any thresholds does not require modification of L.

Length	256-bit integers			512-bit integers		
	time	max. disp.	av. disp.	time	max. disp.	av. disp.
100	0.16s	52	28	0.3s	58	28
200	0.54s	66	38	1.16s	70	37
500	3.416s	108	52	7.347s	82	53

Table 1: 256-bit and 512-bit integers, $\theta = 2^{-4}$

6. Related Work

In this section we discus previous work on the design of CRT-based secret sharing schemes for DMAS, CMAS, and CAS, and compare them with our proposed schemes.

Disjunctive Multilevel Access Structures (DMAS). The first CRT-based secret sharing scheme for disjunctive multilevel access structures was proposed in [15]. We will use the notation in Section 3.1 to describe this scheme (called Scheme 6).

Scheme 6: Harn-Fuyou SSS for $(\overline{U}, \bar{t}, \Gamma)$

1. *parameter setup:* for each level i, $1 \leq i \leq q$, consider an Asmuth-Bloom $(t_i + 1, n_i)$-threshold sequence of co-primes $L_i = (m_0, m_{i,1}, \ldots, m_{i,n_i})$ (remark that m_0 is common to all levels). The secret space is $\mathbb{Z}_{m_0}$ and the private share space of the participant (i,j) is $\mathbb{Z}_{m_{i,j}}$, for all $1 \leq i \leq q$ and $1 \leq j \leq n_i$;

2. *secret sharing:* each secret s is shared to participants as follows:

   (a) for each i, $1 \leq i \leq q$, randomly chosen $r_i \geq 0$ and compute $s_i = s + r_i m_0 < \prod_{j=1}^{t_i+1} m_{i,j}$;

   (b) each participant (i,j) receives a secret share $s_{i,j}$ corresponding to its level i, computed by

   $$s_{i,j} = s_i \bmod m_{i,j},$$

   and $q - i$ shares $w_{i,j}^{i+1}, \ldots, w_{i,j}^{q}$ corresponding to the levels $i+1, \ldots, q$, respectively, are broadcast as public information. These are computed as follow:

      i. choose $m_{i,j}^{\ell}$ such that $m_{\ell,t_\ell+1} < m_{i,j}^{\ell} < m_{\ell,n_\ell-t_\ell+1}$;

      ii. compute $w_{i,j}^{\ell} = (s_\ell - s_{i,j}) \bmod m_{i,j}^{\ell}$,

   for all ℓ with $i + 1 \leq \ell \leq q$;

3. *secret reconstruction:* assume $A \in \Gamma$ and ℓ is a level such that $|A \cap \big(\cup_{i=1}^{\ell} U_i\big)| \geq t_\ell + 1$. The participants in A can uniquely reconstruct the secret s by computing first the unique solution

modulo $\prod_{(\ell,j)\in A} m_{\ell,j} \prod_{(i,j)\in A, i<\ell} m^{\ell}_{i,j}$ of the system

$$\begin{cases} x \equiv s_{\ell,j} \bmod m_{\ell,j}, & \forall(\ell,j)\in A \\ x \equiv (s_{i,j}+w^{\ell}_{i,j}) \bmod m^{\ell}_{i,j}, & \forall(i,j)\in A \\ & \text{with } i<\ell \end{cases}$$

and then reducing it modulo m_0.

It is straightforward to check the soundness of this scheme.

As one can see, each sequence L_ℓ is enriched in the secret sharing phase by new co-primes in between $m_{\ell,t_\ell+1}$ and $m_{\ell,n_\ell-t_\ell+1}$. The sequence newly obtained is still an Asmuth-Bloom sequence of co-primes. However, to enrich L_ℓ in this way, two more constraints must be fulfilled:

- $2t_\ell < n_\ell$ (because $t_\ell+1$ must be less than $n_\ell - t_\ell + 1$) and,
- the interval $(m_{\ell,t_\ell+1}, m_{n_\ell-t_\ell+1})$ must be sufficiently large to accommodate at least $\sum_{i=1}^{\ell-1} n_i$ new co-primes.

In the view of these, we may say that the Harn-Foyou secret sharing scheme has the following disadvantages:

1. it cannot accommodate all practical cases as its thresholds t_i are bounded from above by $n_i/2$;
2. the scheme uses sequences of co-primes of length $1+\sum_{i=1}^{q}(q-i+1)n_i$, which is quite large;
3. being based on Asmuth-Bloom sequences of co-primes, adding new participants to or changing the thresholds of a given realization of the scheme suffer from the same issues discussed in Remark 2.3;
4. being based on Asmuth-Bloom sequences of co-primes, its security is at most as good as the security of the Asmuth-Bloom secret sharing scheme (see also Section 4 in [15]). However, the Asmuth-Bloom secret sharing scheme is not asymptotically perfect [2, 9, 10].

The Harn-Fuyou secret sharing scheme was refined in [12]. It was shown that there is no need for more co-primes in the secret sharing phase. Thus, the scheme needs only q Asmuth-Bloom sequences of co-primes as in the parameter setup phase. Moreover, the authors of [12] considered just one sequence of co-primes

$$p_0 < p_1 < \cdots < p_n$$

(n is the number of participants, p_0 defines the secret space, and each p_i is associated to some participant), subject to the constraint

$$\prod_{i=1}^{\lfloor n/2\rfloor} p_i > p_0^2 \prod_{i=1}^{\lfloor n/2\rfloor-1} p_{n-i+1}. \qquad (12)$$

This constraint implies that each sub-sequence of co-primes associated to the participants of the same level is an Asmuth-Bloom sequence of co-primes [12].

In this way, the solution proposed in [12] alleviates the first two disadvantages of the Harn-Foyou secret sharing scheme.

In order to provide good security properties for their scheme, the authors of [12] considered only sequences of primes and computed the public information of the participant (i, j) by

$$w_{i,j}^{\ell} = (s_\ell - h_j(s_{i,j}, \ell)) \bmod p_{i,j}$$

where h_j is a hash function associated to (i, j) (that depends only on the participant and not of its level) and $p_{i,j}$ is the prime modulus associated to (i, j), for all $\ell > i$.

Under the hypothesis that all hash functions behave like random oracles, it was shown in [12] that the scheme thus obtained does not leak any information (about the secret) to unauthorized sets of participants.

Although the scheme in [12] greatly improve over the Harn-Fuyou scheme, we consider that it still has several disadvantages:

1. it uses sequences of primes that may be very dispersed (it is well-known that the distance between consecutive primes may be arbitrarily large);

2. generating sequences of primes fulfilling (12) is costly. Moreover, adding new participants to or changing the thresholds of a given realization of the scheme still remain costly (Remark 2.3). It might even be more costly because the sequence consists of primes;

3. the scheme uses hash functions that have to be modeled as random oracles for security reasons;

4. the information rate is very large because (12) implies $p_0^2 < p_1$ and then $|\mathbb{Z}_{p_1}|/|\mathbb{Z}_{p_0}| > p_0$. Therefore, the information rate of all participants is larger than p_0.

The CRT-DMAS secret sharing scheme proposed by us (and based on compact sequences of co-primes) alleviates all the disadvantages mentioned above:

- the scheme is based on compact sequences of co-primes that can be efficiently generated (see Table 1);

- the dispersion rate among consecutive co-primes in the sequence is very small (see Table 1);

- adding new participants to some realization of the scheme is very efficient and consists of generating new co-primes at the end of the sequence; changing the thresholds does not require modification of the sequence (see Section 5);

- the scheme is asymptotically ideal (with respect to the uniform distribution on the secret space).

Conjunctive Multilevel Access Structures (CMAS). The only known so far CRT-based secret sharing scheme for conjunctive multilevel access structures was proposed in [12] by simply modifying their scheme for DMAS (see above). More precisely, for conjunctive multilevel access structures, the secret is firstly partitioned by the Karnin-Greene-Hellman scheme (which is perfect) and then each share is further shared in a similar way to the method presented above for disjunctive multilevel access structures. The scheme obtained in this way has the same disadvantages as those above. Our proposal in Section 3.2, which parallelizes the CRT-DMAS scheme in Section 3.1, removes all these disadvantages as discussed above.

Compartmented Access Structures (CAS). Compartmented access structures have been proposed in [24]. The first (and the only known so far) CRT-based secret sharing scheme for compartmented access structures was proposed in [16, 17]. Its main idea is to associate two private shares to each participant. One of the shares is used to recover the participant's compartment secret while the other one is used to recover the global secret (please see Section 3.3 for more details). Moreover, the Mignotte secret sharing scheme [20] was employed in [16, 17] in order to derive the compartmented scheme. Unfortunately, this scheme has the following disadvantages:

1. being based on the Mignotte secret sharing scheme, its security is poor [2]. Even if we replace the Mignotte scheme by the Asmuth-Bloom scheme, the resulting scheme is not asymptotically perfect; moreover, its information rate is greater than two because each participant has two private shares;

2. the scheme uses sequences of co-primes for each compartment and another sequence of co-primes for all participants. That is, each participant has associated two distinct moduli and not only one as in the other CRT-based secret sharing schemes;

3. adding new participants to or changing the thresholds of a given realization of the scheme is costly (as it was discussed in the previous paragraphs of this section).

Our scheme in Section 3.3 alleviates all these disadvantages. First, our scheme is based on compact sequences of co-primes and it is asymptotically ideal. The scheme uses just one sequence of co-primes of length $n + 1$, where n is the number of participants. Adding new participants to some realization of the scheme is very efficient and consists of generating new co-primes at the end of the sequence; changing the thresholds does not require modification of the sequence.

7. Conclusions

The design of secret sharing schemes for multilevel and compartmented access structures attracted the researchers' attention for quite many years [24, 13, 16, 17, 25, 3, 4, 15, 12]. The techniques used so far falls in one of the two classed: polynomial interpolation techniques and CRT-based techniques. The first class of techniques usually lead to ideal schemes, while the second class may produce at most asymptotically ideal schemes. The CRT-based schemes (for multilevel and compartmented access structure) proposed miss a consistent security analysis or simply they are neither efficient nor secure (see our Section 6 for a detailed discussion).

Our paper is the first one that proposes asymptotically ideal secret sharing schemes for multilevel and compartmented access structures. Moreover, we have shown that this level of security can be achieved if and only if the schemes are based on 1-compact sequences of co-primes. As these kind of sequences can very efficiently be generated (see our Section 5), we strongly believe that our schemes are among the most efficient schemes based on CRT.

There is one more innovative aspect that our paper brings. Namely, it introduces a variant of the Asmuth-Bloom secret sharing scheme where the participants may have public shares. These schemes can then be "composed" in order to define secret sharing schemes for access structures where the participants are divided into groups. Moreover, the security of the schemes such obtained easily follows from the security of the component schemes. This is a kind of compositional design and reasoning for secret sharing schemes.

8. References

[1] Asmuth, C. A. and Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 29(2):208–210. The paper was presented at the National Telecommunications Conference, Houstan, Dec. 1980.

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

[3] Beimal, A., Tassa, T., and Weinreb, E. (2008). Characterizing ideal weighted threshold secret sharing. *SIAM Journal of Discrete Mathematics*, 22(1):360–397.

[4] Belenkiy, M. (2008). Disjunctive multi-level secret sharing. Technical report, Brown University.

[5] Blakley, G. (1979). Safeguarding cryptographic keys. In *1979 AFIPS National Computer Conference*, pages 313–317. AFIPS Press.

[6] Cover, T. and Thomas, J. (2006). *Elements of Information Theory*. John Wiley and Sons, second edition.

[7] Ţiplea, F. L. and Drăgan, C. C. (2014). A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme. *Information Processing Letters*, 114(6):299 – 303.

[8] Ding, C., Pei, D., and Salomaa, A. (1996). *Chinese Remainder Theorem. Applications in Computing, Coding, Cryptography*. World Scientific Publishing.

[9] Drăgan, C. C. (2013). *Security of CRT-based Secret Sharing Schemes*. PhD thesis, "AL.I.Cuza" University of Iasi, Romania.

[10] Drăgan, C. C. and Ţiplea, F. L. (2018). On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme. *Information Sciences*, 463 - 464:75 – 85.

[11] Drăgan, C. C. and Ţiplea, F. L. (2016). Distributive weighted threshold secret sharing schemes. *Information Sciences*, 339:85 – 97.

[12] Ersoy, O., Kaya, K., and Kaskaloglu, K. (2016). Multilevel threshold secret and function sharing based on the chinese remainder theorem. *CoRR*, abs/1605.07988.

[13] Ghodosi, H., Pieprzyk, J., and Safavi-Naini, R. (1998). Secret sharing in multilevel and compartmented groups. In Boyd, C. and Dawson, E., editors, *Third Australasian Conference on Information Security and Privacy (ACISP '98)*, volume 1438 of *Lecture Notes in Computer Science*, pages 367–378. Springer.

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

[15] Harn, L. and Fuyou, M. (2014). Multilevel threshold secret sharing based on the Chinese remainder theorem. *Information Processing Letters*, 114(9):504 – 509.

[16] Iftene, S. (2005). Compartmented secret sharing based on the Chinese remainder theorem. *IACR Cryptology ePrint Archive*, 2005:408.

[17] Iftene, S. (2007). General secret sharing based on the Chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science*, 186(0):67 – 84. Proceedings of the First Workshop in Information and Computer Security (ICS 2006).

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

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

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

[21] Pieprzyk, J., Seberry, J., and Hardjono, T. (2003). *Fundamentals of Computer Security*. Springer-Verlag Berlin Heidelberg, Germany.

[22] Quisquater, M., Preneel, B., and Vandewalle, J. (2002). On the security of the threshold scheme based on the Chinese remainder theorem. In Naccache, D. and Paillier, P., editors, *Public Key Cryptography*, volume 2274 of *Lecture Notes in Computer Science*, pages 199–210. Springer.

[23] Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

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

[25] Tassa, T. (2007). Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264.