Distributive Weighted Threshold Secret Sharing Schemes

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

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

Abstract

The concept of distributive weighted threshold access structure is introduced, which is an weighted threshold access structure where the participants are distributed on levels, the participants on the same level are assigned the same weight, and the threshold of the access structure is 1. The weight of the participants on the ith level is of the form $1/k_i$ and, therefore, the ith level induces a standard threshold access structure with threshold k_i.

We propose a CRT-based realization of distributive weighted threshold access structures, which is asymptotically perfect and perfect zero-knowledge. We also show that distributive weighted threshold access structures do not generally have ideal realizations. In case of just one level, our scheme can be viewed as an asymptotically perfect and perfect zero-knowledge variation of the Asmuth-Bloom secret sharing scheme.

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

1. Introduction

A secret sharing scheme is a method of partitioning a master secret among some users by providing each user with a share of the secret. The secret can be recovered only if a sufficient number of shares are combined together. Secret sharing schemes were independently proposed for the first time by Blakley [1] and Shamir [2]. Blakley's scheme is based on hyperplane intersections. The secret is an element of a k-dimensional vector space over a Galois field, and the shares are $(k-1)$-dimensional hyperplanes whose intersection is the secret. The secret can be obtained by intersecting any k shares. Shamir's scheme is based on polynomial interpolation. The secret is the free coefficient of a polynomial P of degree $k-1$ with coefficients in $\mathbb{Z}_p$ for some large prime p, and the shares are $P(i)$ for any $1 \leq i \leq n$, where $n \geq k$. Any k shares can recover the secret by computing the polynomial by interpolation.

*Corresponding author

Email addresses: constantin.dragan@info.uaic.ro (Constantin Cătălin Drăgan), fltiplea@info.uaic.ro (Ferucio Laurenţiu Ţiplea)

[1] Work supported by the European Social Fund in Romania, under the responsibility of the Managing Authority for the Sectoral Operational Programme for Human Resources Development 2007-2013 [grant POSDRU/CPP 107/DMI 1.5/S/78342]

Novel threshold secret sharing schemes based on the Chinese Remainder Theorem (CRT) have independently been proposed by Asmuth and Bloom [3] and Mignotte [4], and later by Goldreich, Ron and Sudan [5]. The schemes in this category, are based on sequences of co-prime positive integers with special properties. The shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders. The secret can be recovered from any k shares, where k depends on the sequence, by using CRT.

Weighted threshold secret sharing schemes are natural generalizations of threshold secret sharing schemes, where each participant is assigned a weight depending on his importance (role) in the group of all participants. The secret can be reconstructed if and only if the sum of the weights assigned to a set of participants is greater than or equal to a fixed threshold. This idea was first proposed by Shamir [2] who also suggested a realization of it by using tuples of polynomial values associated to each participant. In 1999, Morilo et al. [6] proposed a complete characterization of the weighted threshold access structures of rank two by using graph theory (the rank of a weighted threshold access structure is the maximum cardinality of the minimal authorized sets). Later, Beimel et al. [7, 8] have proposed a characterization of ideal weighted threshold access structures by showing that weighted threshold access structures are ideal if and only if they are either hierarchical threshold access structures of at most three levels, or tripartite access structures, or compositions of two ideal weighted threshold access structures.

As we have mentioned above, Shamir already sugested in [2] how weighted threshold secret sharing schemes can be obtained by using polynomial interpolation. Wang et al. [9] generalized Shamir's idea by proposing a weighted secret sharing scheme that creates the secret-dependent quantity in the same manner as Shamir, but computes the shares as the remainders obtain by polynomial reduction. The scheme uses a polynomial form of the CRT [10] to recover the secret (one may also see the last section in [3]). Another direction to design weighted threshold secret sharing schemes was to extend the Mignotte's and Asmuth-Bloom's schemes to weighted threshold access structures. A first step along this line was made in [11]. According to [11], each participant receives a number of shares depending on his weight. Unfortunately, [11] does not provide any security analysis of the proposed schemes (it is expected that these schemes are neither asymptotically perfect nor asymptotically ideal nor perfect zero-knowledge [12]).

Another class of secret sharing schemes closely related to our work is that of *multilevel secret sharing schemes* [13, 14, 8, 15] also called *hierarchical threshold secret sharing schemes* in [14, 8]. In such schemes, participants are divided into disjoint levels according to their importance. These levels are totally ordered and participants on lower levels are more important than participants on higher levels. In a standard scenario regarding the employes of a bank, the lowest level may consists of the board of directors. Two types of access structures for multilevel secret sharing schemes have been proposed so far, namely *disjunctive multilevel access structures* [13] and *conjunctive multilevel access structures* [14] (the terms *disjunctive* and *conjunctive* were proposed in [15]). To understand the difference between these two types of access structures let $U_1, \ldots, U_q$ denote the levels, where U_1 is the lowest one. To each level U_i a threshold k_i is associated such that $k_1 < \cdots < k_q$. In disjunctive multilevel access structures

a group of participants can reconstruct the secret if there exists i such that the group contains at least k_i participants taken from $\cup_{j=1}^{i} U_j$, while in conjunctive multilevel access structures the group of participants who want to reconstruct the secret must contain at least k_i participants taken from $\cup_{j=1}^{i} U_j$, for all i.

Contribution To understand the motivation of our work let us consider the case of a disjunctive multilevel access structure with just two levels U_1 and U_2 and thresholds $k_1 = 2$ and $k_2 = 4$. Assume that U_1 consists of directors, and U_2 of senior tellers, of a bank. The choice of these parameters tells that a bank vault can be opened by either any two directors or four senior tellers. According to the definition of a disjunctive multilevel access structure, the bank vault can also be opened by three senior tellers together with one director, but not by two senior tellers together with one director. This is somewhat contrary to our intuition that, according to the choice of the parameters, one director can be replaced by any two senior tellers.

This small example leads us to consider multilevel access structures where each participant has associated a weight and where each participant in an authorized set can be replaced by any number of participants whose weights can compensate the weight of that participant. These new multilevel access structure are introduced via weighted threshold access structures and are called *distributive weighted threshold access structures*. With such a structure, all the participants are distributed over a fixed number of levels $U_1, \ldots, U_q$. The participants on the same level U_i are assigned the same weight which is of the form $1/k_i$ for some positive integer k_i. The scheme threshold is 1; that is, any set of participants whose sum of weights exceeds 1 should be able to recover the secret. In particular, any set of k_i participants on the level U_i are able to recover the secret. Therefore, the integer k_i acts as a threshold for the level U_i showing that distributive weighted threshold access structures can also be viewed as methods of combining disjoint threshold access structures. The authorized sets are either the authorized sets of the component threshold access structures or sets of participants on different levels whose sum of weights exceeds 1.

Distributive weighted threshold access structures are "extension" of disjunctive multilevel access structures in the sense that for any disjunctive multilevel access structures Γ one can construct a distributive weighted threshold access structures Γ' such that $\Gamma \subseteq \Gamma'$.

We propose a CRT based realization of the distributive weighted threshold access structures and we show that this realization is asymptotically perfect and perfect zero-knowledge. As with respect to idealness, we prove that distributive weighted access structures do not generally have ideal realizations. Therefore, from this point of view, we may say that our scheme is all that can be achieved using CRT. In case of just one level, our CRT based realization of the distributive weighted threshold access structures can be viewed as an asymptotically perfect and perfect zero-knowledge variation of the Asmuth-Bloom secret sharing scheme.

Paper organization The paper is organized into six sections. The rest of this section recalls some basic notations and results in number theory. Section 2 introduces the concept of a distributive weighted threshold access structure, while Section 3 shows that distributive weighted threshold access structures do not generally have ideal realizations. The fourth section proposes a CRT-based realization of the distributive weighted access structures, while Section

5 provides a detailed security analysis of it, focusing on *asymptotic perfectness* and *perfect zero-knowledge*. We conclude in Section 6.

Preliminaries The set of integers is denoted by $\mathbb{Z}$ and the subset of positive integers, also called natural numbers, is $\mathbf{N}$. For an positive integer $n > 0$, $\mathbb{Z}_n$ stands for the set $\{0, \ldots, n-1\}$. The integers a and b are called *co-prime* if their greatest common divisor is 1. Two integers are called *congruent modulo* m, denoted $a \equiv b \bmod m$, if m divides $a - b$(m is an integer too). The *Chinese Remainder Theorem* (CRT) [16] states that the system of congruences

$$x \equiv b_i \bmod m_i \text{ for all } 1 \leq i \leq n$$

has a unique solution in $\mathbb{Z}_{m_1 \cdots m_n}$, if $m_1, \ldots, m_n$ are pairwise co-prime.

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

2. Distributive weighted threshold access structure

Motivated by the example in the contribution paragraph in Section 1, we introduce the concept of *distributive weighted threshold access structure*. Recall first that [17], given a non-empty finite set U whose elements are called *participants*, an *access structure* (AS) over U is a set $\Gamma \subseteq \mathcal{P}(U)$ which satisfies the following monotonicity property:

$$(\forall B \in \mathcal{P}(U))((\exists A \in \Gamma)(A \subseteq B) \Rightarrow B \in \Gamma)$$

The elements of Γ are called *authorized sets*, while those of $\mathcal{P}(U) - \Gamma$, *unauthorized sets*. An authorized set A is *minimal* if there is no $B \in \Gamma$ such that $B \subset A$.

A *weighted threshold access structure* (WTAS) over U [6] is a triple (w, t, Γ), where:

1. $w : U \to \mathbb{R}$ is a function called the *weight function*;
2. $t > 0$ is a positive real number called *threshold*;
3. $\Gamma = \{A \in \mathcal{P}(U) | w(A) \geq t\}$, where $w(A) = \sum_{x \in A} w(x)$, for any A.

Clearly, any WTAS over U is an AS over U. In what follows we focus on a special sub-class of weighted threshold access structures where the participants are distributed on $q \geq 1$ levels. The participants on the same level have the same weight.

Definition 1. *Let U be a non-empty finite set. A* distributive weighted threshold access structure *(DWTAS) over U is a triple $(\overline{k}, w, \Gamma)$, where:*

1. $\overline{k} = (k_1, \ldots, k_q) \in \mathbb{Z}^q$ *satisfies* $0 < k_1 < \cdots < k_q$, *where* $q \geq 1$;
2. $w : U \to \mathbb{R}$ *is the weight function which enjoys the properties:*
   (a) $w(x) \in \{1/k_1, \ldots, 1/k_q\}$;
   (b) $|\{x \in U | w(x) = 1/k_i\}| \geq k_i$, *for any* $1 \leq i \leq q$;
3. $\Gamma = \{A \subseteq U | w(A) \geq 1\}$.

The terminology "distributive" is justified by the fact that a DWTAS can be viewed as a multilevel access structure [13], whose authorized sets are "distributed" over levels. Indeed, the set U of participants can be partitioned into *levels* $U_i = \{x \in U | w(x) = 1/k_i\}$, where $1 \leq i \leq q$. Each level U_i satisfies $1 \leq k_i \leq n_i$, where n_i is the cardinality of U_i. Moreover, all participants in U_i have the same weight $1/k_i$.

An authorized set $A \in \Gamma$ of participants may contain participants from any level provided that the sum of the weights of the participants in A exceeds 1. Thus, if $A \subseteq U$ contains at least k_i participants from the level U_i, for some i, then A is an authorized set (that is, k_i acts as a threshold for this level). This is the reason we have chosen the global threshold 1 for DWTAS.

Remark 2. *A* disjunctive multilevel access structure *(DMAS) [13]* [2] *over a set U of participants is a tuple $(\overline{k}, \overline{U}, \Gamma)$, where $\overline{k} = (k_1, \ldots, k_q)$ is a vector of positive integers satisfying $0 < k_1 < \cdots < k_q$, $\overline{U} = (U_1, \ldots, U_q)$ is a partition of U (that is, all U_i are non-empty and their union is U), and Γ is defined by:*

$$\Gamma = \{A \subseteq U | (\exists 1 \leq i \leq q)(|A \cap (\cup_{j=1}^{i} U_j)| \geq k_i)\}.$$

Given a DMAS $(\overline{k}, \overline{U}, \Gamma)$ one can construct a DWTAS $(\overline{k}, w, \Gamma')$ such that $\Gamma \subseteq \Gamma'$. Indeed, what we have to do is to define $w(x) = 1/k_i$, for any $x \in U_i$ and $1 \leq i \leq q$. From this point of view, DWTAS can be viewed as extensions of DMAS. Moreover, DWTAS are strict extensions of DMAS in the sense that there are DWTAS whose authorized sets cannot be defined by any DMAS. For instance, let $U = \{x_1, x_2, y_1, \ldots, y_4\}$ be a set of six participants, $k_1 = 2$, $k_2 = 4$, $w(x_1) = w(x_2) = 1/2$, and $w(y_1) = \cdots = w(y_4) = 1/4$. These elements define a DWTAS $(\overline{k}, w, \Gamma)$ for which Γ cannot be defined by any DMAS.

Remark 3. *A* conjunctive multilevel access structure *(CMAS) [14] over a set U of participants is a tuple $(\overline{k}, \overline{U}, \Gamma)$, where $\overline{k} = (k_1, \ldots, k_q)$ is a vector of positive integers satisfying $0 < k_1 < \cdots < k_q$, $\overline{U} = (U_1, \ldots, U_q)$ is a partition of U, and Γ is defined by:*

$$\Gamma = \{A \subseteq U | (\forall 1 \leq i \leq q)(|A \cap (\cup_{j=1}^{i} U_j)| \geq k_i)\}.$$

As one can see, CMAS are somewhat opposite to both DMAS and DWTAS: an authorized set of a CMAS should contain at least k_i participants from the levels U_1 up to U_i. From this point of view we may say that CMAS are incomparable with both DMAS and DWTAS.

Given $A \subseteq U$, the *characteristic vector of A w.r.t.* $(\overline{k}, w, \Gamma)$ is a vector $c_A = (c_1, \ldots, c_q)$ which satisfies $c_i = |\{a \in A | w(a) = 1/k_i\}|$, for all $1 \leq i \leq q$. That is, c_i is the number of participants with the same weight $1/k_i$. Then, $w(A) = \sum_{i=1}^{q} c_i/k_i$. Therefore, A is an authorized set if $\sum_{i=1}^{q} c_i/k_i \geq 1$, and A is a minimal authorized set if it is an authorized set and the following relationship

[2] Simmons [13] called them *multilevel access structures*. Later, Tassa [14] and Beimel et al. [8] called them *hierarchical threshold access structures* (HTAS), and Belenkiy [15] called them *disjunctive multilevel access structures* and used *conjunctive multilevel access structures* for the access structures introduced by Tassa.

holds for all j with $c_j > 0$:

$$\sum_{i=1,\, i\neq j}^{q} \frac{c_i}{k_i} + \frac{c_j - 1}{k_j} < 1.$$

The following lemma shows that if the participants in a minimal authorized set of a DWTAS are taken from the lth level up to the rth level, then the number of participants is at least k_l and at most k_r.

Lemma 4. *Let $(\overline{k}, w, \Gamma)$ be a DWTAS and A a minimal authorized set whose characteristic vector is $c_A = (c_1, \ldots, c_q)$. If there are l and r such that*

1. $1 \leq l \leq r \leq q$;
2. $c_i = 0$ *for all* $1 \leq i \leq l-1$ *and* $r+1 \leq i \leq q$;
3. $c_l > 0$ *and* $c_r > 0$,

then $k_l \leq \sum_{i=l}^{r} c_i \leq k_r$. Moreover, if $l < r$ then $k_l < \sum_{i=l}^{r} c_i \leq k_r$.

Proof. Let c_A, l, and r be as in the lemma. If $l = r$, then $c_l = k_l = k_r$ and the result in the lemma holds true.

Assume $l < r$ and let j such that $c_j > 0$. As A is minimal, it follows

$$\sum_{i=1}^{q} \frac{c_i}{k_i} \geq 1 \quad \text{and} \quad \sum_{i=1,\, i\neq j}^{q} \frac{c_i}{k_i} + \frac{c_j - 1}{k_j} < 1.$$

These lead to

$$k_j - \sum_{i=l,\, i\neq j}^{r} c_i \frac{k_j}{k_i} \leq c_j < k_j + 1 - \sum_{i=l,\, i\neq j}^{r} c_i \frac{k_j}{k_i}$$

Using these two inequalities and the fact that the thresholds are increasingly ordered, we obtain

$$\sum_{i=l}^{r} c_i = c_l + \sum_{i=l+1}^{r} c_i \geq k_l + \sum_{i=l+1}^{r} c_i(1 - \frac{k_l}{k_i}) > k_l$$

and

$$\sum_{i=l}^{r} c_i = c_r + \sum_{i=l}^{r-1} c_i < k_r + 1 + \sum_{i=l}^{r-1} c_i(1 - \frac{k_r}{k_i}).$$

As $\sum_{i=l}^{r} c_i$ is a positive integer, it follows $k_l < \sum_{i=l}^{r} c_i \leq k_r$. ■

3. DWTAS do not have ideal realizations

We show in this sections that DWTAS do not have ideal realizations. The main argument is based on a characterization theorem for ideal weighted threshold secret sharing schemes proposed in [7]. In order to understand it we recall first a few concepts.

A *tripartite access structure* (TPAS) over a set U of participants is a tuple $(A, B, C, m, d, t, \Gamma)$, where A, B and C are disjoint sets, A and C are nonempty, $U = A \cup B \cup C$, $m \geq t$, and Γ is either Δ_1 or Δ_2 as given below:

$$\Delta_1 = \{X \subseteq U | (|X| \geq m \ \wedge \ |X \cap (B \cup C)| \geq m - d) \ \vee \ |X \cap C| \geq t\}$$

$$\Delta_2 = \{X \subseteq U | (|X| \geq m \ \wedge \ |X \cap C| \geq m - d) \ \vee \ |X \cap (B \cup C)| \geq t\}$$

Given two disjoint sets U' and U'' of participants, two access structures Γ_1 and Γ_2 over U' and U'', respectively, and given $u \in U'$, define the *composition of* Γ_1 *and* Γ_2 *via* u as being the access structure

$$\Gamma = \{X \subseteq U' \cup U'' - \{u\} | X \in \Gamma_1 \ \vee \ (X \cap U'' \in \Gamma_2 \ \wedge \ (X \cap U') \cup \{u\} \in \Gamma_1)\}.$$

An access structure is called *ideal* if there are ideal realizations of it.

Theorem 5 ([7]). *A WTAS* Γ *over* U *is ideal if and only if one of the following three conditions holds:*

1. Γ *is an DMAS of at most three levels* [3]*;*
2. Γ *is a TPAS;*
3. Γ *is a composition of two ideal WTAS defined on sets of participants smaller than* U*.*

Based on this theorem we obtain the following result.

Theorem 6. *There are DWTAS that are not ideal.*

Proof. We show that there are DWTAS that do not satisfy any of the three conditions in Theorem 5.

It is not difficult to see that DWTAS with at least four levels cannot be defined by DMAS with at most three levels or by TPAS. We focus now on the more complex task of proving that no DWTAS with two or more levels can be decomposed into two WTAS. For the sake of simplicity we consider the case of a DWTAS $(\overline{k}, w, \Gamma)$ with two levels (that is, $\overline{k} = (k_1, k_2)$) over a set of participants U. Assume, by contradiction, that Γ can be written as a composition of two WTAS Γ_1 and Γ_2 via u, where Γ_1 is over U', Γ_2 is over U'', $U' \cap U'' = \emptyset$, $u \in U'$, and $|U| = |U'| + |U''| - 1$.

Without loss of generality we may assume that any authorized set $A \in \Gamma_1$ satisfies $A - \{u\} \neq \emptyset$ and Γ_2 has at least two minimal authorized sets. The assumption on Γ_2 leads to the fact that there exist $B_1, B_2 \in \Gamma_2$ such that $B_1 - B_2 \neq \emptyset$ and $B_2 - B_1 \neq \emptyset$.

Claim: All elements of any set $A \in \Gamma_1$ with $u \in A$ must be on the same level in Γ, and all the elements in U'' must be on the other level in Γ.

Proof of Claim: Assume there exists $A \in \Gamma_1$ with $u \in A$ such that $(A - \{u\}) \cap U_1 \neq \emptyset$ and $(A - \{u\}) \cap U_2 \neq \emptyset$ (that is, $A - \{u\}$ overlaps the two levels U_1 and U_2 in Γ). Given $b \in B_1 - B_2$ for some $B_1, B_2 \in \Gamma_2$, b is either on the first level or on the second one in Γ because $(A - \{u\}) \cup B_1 \in \Gamma$. If b is on the first level, then let $a \in (A - \{u\}) \cap U_1$. Then, $(A - \{a, u\}) \cup \{b\} \cup B_2$ must be in Γ because a and b have the same weight in Γ. However, $(A - \{a, u\}) \cup \{b\} \cup B_2$ cannot be obtained by composing Γ_1 and Γ_2 via u. Similarly, b cannot be on the second level.

Iterating the above argument for all sets $A \in \Gamma_1$ with $u \in A$ we obtain the statement in the Claim. □

[3] In [8], disjunctive multilevel access structures are called hierarchical threshold access structures (see also the discussion in Remark 2).

According to the above claim we assume that all the elements of the sets $A \in \Gamma_1$ with $u \in A$ are on the first level and all the elements in U'' are on the second level. Moreover, no element of a set $a \in A$ with $A \in \Gamma_1$ and $u \notin A$ can be on the second level. This follows from the fact that, otherwise, $(A - \{a\}) \cup \{b\}$ is authorized set, for any $b \in U''$ on the second level. However, this set cannot be obtained by the composition of Γ_1 and Γ_2 via u (remark that a and b must have the same weight in Γ).

As a conclusion, the second level must contain only elements of U''; this is a contradiction because any level in Γ should contain authorized sets, the second level of Γ contains only elements from U'', and the composition of Γ_1 and Γ_2 via u cannot yield authorized sets with elements only from U''. ■

4. CRT-based realization of DWTAS

We show in this section that there are CRT-based realizations of distributive weighted threshold access structures. Our approach is based on sequences of pairwise co-prime integers with some special properties. The main idea is as follows. A DWTAS $(\overline{k}, w, \Gamma)$ over a set U of participants partitions the set U into levels $U_i = \{x \in U | w(x) = 1/k_i\}$, $1 \leq i \leq q$. We associate to U_i a sequence L_i of pairwise co-prime integers and partition the secret among the participants on this level by using L_i in a manner similar to most CRT-based secret sharing schemes [4, 3, 5].

Definition 7. *Let $0 < \epsilon \leq 1$ be a real number and $\overline{k} = (k_1, \ldots, k_q)$ and $\overline{n} = (n_1 \ldots, n_q)$ be two vectors of positive integers with $0 < k_1 < \cdots < k_q$ and $k_i \leq n_i$ for all $1 \leq i \leq q$. An* $(\epsilon, \overline{k}, \overline{n})$-sequence *is a pair $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ consisting of a positive integer m_0 and q sets $L_1, \ldots, L_q$ of positive integers such that:*

1. *$|L_i| = n_i$, for all $1 \leq i \leq q$;*
2. *$(m_0, x) = 1$ and $(x, y) = 1$ for any $x, y \in \cup_{i=1}^{q} L_i$ with $x \neq y$;*
3. *$m_0 \cdot \alpha < \beta$, where $\alpha = \max\{x^{k_i - \epsilon} | 1 \leq i \leq q,\ x \in L_i\}$ and $\beta = \min\{x^{k_i} | 1 \leq i \leq q,\ x \in L_i\}$.*

The number m_0 in an $(\epsilon, \overline{k}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ is called the *security parameter* of $\mathcal{L}$ (the terminology is justified by the fact that, as we will see later, m_0 is used to define a secret space).

If we denote by $m_{i,1} < \cdots < m_{i,n_i}$ the elements of L_i together with their total ordering, then the third requirement in Definition 7 can be rewritten in the form

"$m_0 \cdot \alpha < \beta$, where $\alpha = \max_{i=1}^{q} m_{i,n_i}^{k_i - \epsilon}$ and $\beta = \min_{i=1}^{q} m_{i,1}^{k_i}$"

This notation will be used throughout the paper from now on.

Lemma 8. *For any $(\epsilon, \overline{k}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$, where ϵ, $\overline{k}$, and $\overline{n}$ are as in Definition 7, the following inequalities hold:*

1. *$m_0 < m_{q,1}^{\epsilon} \leq m_{q,1}$;*
2. *$m_{q,1} < \cdots < m_{q,n_q} < \cdots < m_{1,1} < \cdots < m_{1,n_1}$.*

Proof. (1) From Definition 7 it follows $m_0 m_{q,n_q}^{k_q-\epsilon} < m_{q,1}^{k_q}$ and, therefore, $m_0 < m_{q,1}^{\epsilon}$. As $0 < \epsilon \leq 1$, we also have $m_{q,1}^{\epsilon} \leq m_{q,1}$.

(2) We show that $m_{i,n_i} < m_{i-1,1}$, for all $2 \leq i \leq q$. Again, from Definition 7 it follows $m_{i,n_i}^{k_i-\epsilon} < m_{i-1,1}^{k_{i-1}}$. As $k_{i-1} \leq k_i - \epsilon$ for any $0 < \epsilon \leq 1$, we obtain $m_{i-1,1}^{k_{i-1}} \leq m_{i-1,1}^{k_i-\epsilon}$ and, therefore, $m_{i,n_i} < m_{i-1,1}$. ■

Theorem 9. *There are $(\epsilon, \overline{k}, \overline{n})$-sequences with arbitrarily large security parameters, for any ϵ, $\overline{k}$, and $\overline{n}$ as in Definition 7.*

Proof. Let ϵ, $\overline{k}$, and $\overline{n}$ be as in Definition 7, and let m_0 be a security parameter.

Recall first [18] that the infinite sequence of prime numbers $p_1, p_2, \ldots$ satisfies the following property

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

This shows that for any $\delta > 0$ there exists i_0 such that

$$p_{i+1} < (1+\delta)p_i, \tag{1}$$

for any $i \geq i_0$. Therefore, $p_{i+j} < (1+\delta)^j p_i$, for any $i \geq i_0$ and $j \geq 1$.

We discuss now the case $q = 1$. Given a real number $\delta > 0$, there exists i_0 such that $p_{i+j} < (1+\delta)^j p_i$ and $p_i > (m_0(1+\delta)^{(n_1-1)(k_1-\epsilon)})^{1/\epsilon}$, for any $i \geq i_0$ and $j \geq 1$. Therefore, for any $i \geq i_0$ we have

$$m_0 p_{i+n_1-1}^{k_1-\epsilon} < m_0(1+\delta)^{(n_1-1)(k_1-\epsilon)} p_i^{k_1-\epsilon} < p_i^{\epsilon} p_i^{k_1-\epsilon} = p_i^{k_1}.$$

Therefore, the sequence $p_i < \ldots < p_{i+n_1-1}$ of consecutive primes together with m_0 form an $(\epsilon, \overline{k}, \overline{n})$-sequence.

Consider now the case $q = 2$. We show that there are two sequences of consecutive primes

$$L_2: \quad p_i < \cdots < p_{i+n_2-1} \qquad\qquad L_1: \quad p_{i+j} < \cdots < p_{i+j+n_1-1}$$

where $j \geq n_2$, such that $(m_0, (L_1, L_2))$ is an $(\epsilon, \overline{k}, \overline{n})$-sequence. That is, L_1 and L_2 must fulfill the following inequalities:

$$m_0 p_{i+n_2-1}^{k_2-\epsilon} < p_i^{k_2} \tag{2}$$

$$m_0 p_{i+n_2-1}^{k_2-\epsilon} < p_{i+j}^{k_1} \tag{3}$$

$$m_0 p_{i+j+n_1-1}^{k_1-\epsilon} < p_i^{k_2} \tag{4}$$

$$m_0 p_{i+j+n_1-1}^{k_1-\epsilon} < p_{i+j}^{k_1} \tag{5}$$

Due to the fact that there are infinitely many prime numbers, for any real number $\delta > 0$ there exists i such that

$$p_i > \max\{(m_0(1+\delta)^{(n_2-1)(k_2-\epsilon)})^{1/\epsilon}, (m_0(1+\delta)^{n_1(k_1-\epsilon)})^{k_1/(\epsilon k_2)}\} \tag{6}$$

Claim 10. *Given a real number $\delta > 0$ and a positive integer i which satisfies the inequality (6), there exists j such that*

$$p_i^{k_2/k_1} < p_{i+j} < m_0^{-1/(k_1-\epsilon)}(1+\delta)^{-(n_1-1)} p_i^{k_2/(k_1-\epsilon)} \tag{7}$$

Proof. Let s be the largest positive integer with $p_s < p_i^{k_2/k_1}$. Then, $p_{s+1} > p_i^{k_2/k_1}$. We prove that $p_{s+1} < m_0^{-1/(k_1-\epsilon)}(1+\delta)^{-(n_1-1)}p_i^{k_2/(k_1-\epsilon)}$. We have:

$$p_{s+1} < (1+\delta)p_s < (1+\delta)p_i^{k_2/k_1} < m_0^{-1/(k_1-\epsilon)}(1+\delta)^{-(n_1-1)}p_i^{k_2/(k_1-\epsilon)}$$

(the first inequality follows from (1), the second one from the choice of s, and the third one from the fact that $p_i > (m_0(1+\delta)^{n_1(k_1-\epsilon)})^{k_1/(\epsilon k_2)})$.

As $k_2/k_1 > 1$, $s+1 = i+j$ for some $j \geq 1$. ■

We are now in a position to prove that, given $\delta > 0$, any positive integers i and j as in the Claim, satisfy the inequalities (2)-(5).

For the inequality (2) we use (1) and (6) and obtain:

$$m_0 p_{i+n_2-1}^{k_2-\epsilon} < m_0(1+\delta)^{(n_2-1)(k_2-\epsilon)}p_i^{k_2-\epsilon} < p_i^{\epsilon}p_i^{k_2-\epsilon} = p_i^{k_2}$$

To prove the inequality (3) we use (2) and (7):

$$m_0 p_{i+n_2-1}^{k_2-\epsilon} < p_i^{k_2} < p_{i+j}^{k_1}$$

Remark that the inequality (3) implies $j \geq n_2$ as $k_1 \leq k_2 - \epsilon$.

The inequality (4) can be obtained from (1) and (7):

$$m_0 p_{i+j+n_1-1}^{k_1-\epsilon} < m_0(1+\delta)^{(n_1-1)(k_1-\epsilon)}p_{i+j}^{k_1-\epsilon} < p_i^{k_2}$$

Finally, (4) and (7) lead to the inequality (5):

$$m_0 p_{i+j+n_1-1}^{k_1-\epsilon} < p_i^{k_2} < p_{i+j}^{k_1}$$

For the general case we show that there are q sequences of consecutive primes

$$\begin{array}{lccccc} L_q: & p_i & < & \cdots & < & p_{i+n_q-1} \\ L_{q-1}: & p_{i+j_1} & < & \cdots & < & p_{i+j_1+n_{q-1}-1} \\ \cdots & & & & & \\ L_1: & p_{i+j_{q-1}} & < & \cdots & < & p_{i+j_{q-1}+n_1-1} \end{array}$$

where $j_1 > n_q - 1,\ j_2 > j_1 + n_{q-1} - 1, \ldots, j_{q-1} > j_{q-2} + n_2 - 1$, such that

$$m_0 p_{i+j_l+n_{q-l}-1}^{k_{q-l}-\epsilon} < p_{i+j_r}^{k_{q-r}} \tag{8}$$

for all $0 \leq l \leq q-1$ and $0 \leq r \leq q-1$, where $j_0 = 0$.

Remark that (8) is a parameterized inequality, comprising q^2 inequalities, each of them being obtained by assigning values to l and r.

Following the same line as in the case $q = 2$, we can easily show that for any $\delta > 0$ there exists i such that

$$p_i > \max_{l=1}^{q-1}\{(m_0(1+\delta)^{(n_q-1)(k_q-\epsilon)})^{1/\epsilon}, (m_0(1+\delta)^{n_l(k_l-\epsilon)})^{k_l/(\epsilon k_q)}\} \tag{9}$$

Now, for each i which satisfies (9) and each $1 \leq l \leq q-1$, there exists j_l such that

$$p_i^{k_q/k_l} < p_{i+j_l} < m_0^{-1/(k_l-\epsilon)}(1+\delta)^{-(n_l-1)}p_i^{k_q/(k_l-\epsilon)} \tag{10}$$

(this is a generalization of the Claim).

In the same way as we did in the case $q = 2$, one can easily prove that, given $\delta > 0$, any positive integers $i, j_1, \ldots, j_{q-1}$ which satisfy the inequalities (9) and

Algorithm 1: Computing an $(\epsilon, \overline{k}, \overline{n})$-sequence

input : $0 < \epsilon \leq 1$, $\overline{k}$, $\overline{n}$;
output: an $(\epsilon, \overline{k}, \overline{n})$-sequence;
begin
choose a security parameter m_0;
choose a real number $\delta > 0$ (δ may be less than 1);
find i such that the inequalities (9) hold w.r.t. δ;
find $j_1, \ldots, j_{q-1}$ such that the inequalities (10) hold w.r.t. δ and i;
output the $(\epsilon, \overline{k}, \overline{n})$-sequence $(m_0, (L_i | 1 \leq i \leq q))$, where

$$(\forall 0 \leq l \leq q-1)(L_{q-l} : \ p_{i+j_l} < \cdots < p_{i+j_l+n_{q-l}-1})$$

(10) will also satisfy the inequalities (8). Moreover, $j_l > j_{l-1} + n_{q-l+1} - 1$, for all $1 \leq l \leq q-1$ (recall that $j_0 = 0$). ■

The proof of Theorem 9 suggests the Algorithm 1 below to generate $(\epsilon, \overline{k}, \overline{n})$-sequences. In Algorithm 1 remark that the smaller δ is, the smaller $i, j_1, \ldots, j_{q-1}$ are.

We show now that there are realizations of any DWTAS. A CRT-based *distributive weighted threshold secret sharing scheme* (DWTSSS) for a DWTAS $(\overline{k}, w, \Gamma)$ over a set U of participants works as follows:

1. choose $\epsilon > 0$ such that

   $$\epsilon < (1 - \max\{w(A) - 1/k_i | A \text{ minimal } \wedge \ (\exists a \in A)(w(a) = 1/k_i)\}) \cdot k_1$$

   Remark that the right hand side of the above inequality is less than or equal to 1 and the equality holds only when $q = 1$;
2. choose an $(\epsilon, \overline{k}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$, where $n_i = |U_i|$ for all $1 \leq i \leq q$ ($\mathcal{L}$ will be called an $(\epsilon, \overline{k}, \overline{n})$-*sequence associated to* $(\overline{k}, w, \Gamma)$);
3. the secret S is randomly chosen from $\mathbb{Z}_{m_0}$ and the number $S' = S + \gamma m_0 < \beta$ is computed (recall that $\beta = min_{i=1}^{q} m_{i,1}^{k_i}$);
4. (share distribution) – fixing a total ordering on the participants of each level, the jth participant from the ith level receives the share $S_{i,j} = S' \ mod \ m_{i,j}$, for all $1 \leq i \leq q$ and $1 \leq j \leq n_i$;
5. (share recovery) – if an authorized set A of participants pool together their shares, then they recover the secret S by solving the congruential system

   $$x \equiv S_{i,j} \ mod \ m_{i,j}, \quad (i,j) \in I_A$$

   and then reducing the result modulo m_0, where

   $$I_A = \{(i,j) | \exists a \in A : \ a \text{ is the } j\text{th participant on the } i\text{th level}\}.$$

The following lemma establishes the correctness of the secret sharing scheme described above. Namely, it shows that any authorized access structure can uniquely recover the secret. As with respect to unauthorized access structures, the next section provides full details regarding the security of the scheme.

Lemma 11. *With the notations above, if A is an minimal authorized set whose characteristic vector is $c_A = (c_1, \ldots, c_q)$ then, for any $1 \leq j \leq q$ with $c_j > 0$, there exists $0 < \theta_j < 1$ such that*

$$(\prod_{i \neq j} m_{i,n_i}^{c_i}) \cdot m_{j,n_j}^{c_j - 1} \leq \alpha^{\theta_j} < \alpha < \beta \leq \prod_{i=1}^{q} m_{i,1}^{c_i}.$$

Proof. Let A be a minimal authorized set, $c_A = (c_1, \ldots, c_q)$, and let j such that $c_j > 0$. Then, $w(A) \geq 1$ and $w(A) - 1/k_j < 1$. We prove that $\beta \leq \prod_{i=1}^{q} m_{i,1}^{c_i}$. Let $r \in \{1, \ldots, q\}$ such that $\beta = m_{r,1}^{k_r}$. Then, from $m_{r,1}^{k_r} < m_{i,1}^{k_i}$ it follows $m_{r,1}^{c_i \frac{k_r}{k_i}} \leq m_{i,1}^{c_i}$, for all $i \neq r$. Combining all these inequalities we obtain

$$m_{r,1}^{\sum_{i=1}^{q} c_i \frac{k_r}{k_i}} \leq \prod_{i=1}^{q} m_{i,1}^{c_i}.$$

But, $\sum_{i=1}^{q} \frac{c_i}{k_i} \geq 1$ which shows that $\beta \leq \prod_{i=1}^{q} m_{i,1}^{c_i}$.

In order to prove the other inequalities, let $s \in \{1 \ldots, q\}$ such that $\alpha = m_{s,n_s}^{k_s - \epsilon}$. From $m_{s,n_s}^{k_s - \epsilon} > m_{i,n_i}^{k_i - \epsilon}$ it follows $m_{s,n_s}^{c_i \frac{k_s - \epsilon}{k_i - \epsilon}} \geq m_{i,n_i}^{c_i}$, for all $i \neq s$. Combining all these inequalities we obtain:

$$(\prod_{i \neq j} m_{i,n_i}^{c_i}) \cdot m_{j,n_j}^{c_j - 1} \leq m_{s,n_s}^{\sum_{i \neq j} c_i \frac{k_s - \epsilon}{k_i - \epsilon} + (c_j - 1) \frac{k_s - \epsilon}{k_j - \epsilon}}.$$

As $\epsilon < (1 - (w(A) - 1/k_j))k_1$, we have $\frac{k_1}{k_1 - \epsilon}(w(A) - 1/k_j) < 1$. Combining this with $\frac{k_i}{k_i - \epsilon} < \frac{k_1}{k_1 - \epsilon}$ for all $i > 1$, we obtain

$$\begin{aligned} \sum_{i \neq j} c_i \frac{1}{k_i - \epsilon} + (c_j - 1) \frac{1}{k_j - \epsilon} &= \sum_{i \neq j} \frac{c_i}{k_i} \frac{k_i}{k_i - \epsilon} + \frac{c_j - 1}{k_j} \frac{k_j}{k_j - \epsilon} \\ &\leq \frac{k_1}{k_1 - \epsilon} (\sum_{i \neq j} \frac{c_i}{k_i} + \frac{c_j - 1}{k_j}) \\ &= \frac{k_1}{k_1 - \epsilon} (w(A) - 1/k_j) \\ &< 1. \end{aligned}$$

Taking $\theta_j = \sum_{i \neq j} c_i \frac{1}{k_i - \epsilon} + (c_j - 1) \frac{1}{k_j - \epsilon}$, we obtain $(\prod_{i \neq j} m_{i,n_i}^{c_i}) \cdot m_{j,n_j}^{c_j - 1} \leq \alpha^{\theta_j}$, which concludes the proof of the lemma. ■

5. Security issues

The security of CRT-based threshold secret sharing schemes can be studied in the most precise and elegant way by means of the concepts of *asymptotic perfectness*, *asymptotic idealness*, and *perfect zero-knowledge* as proposed in [12]. We recall below these concepts in terms of distributive weighted threshold secret sharing schemes.

5.1. Asymptotic perfectness

Let $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ be an $(\epsilon, \overline{k}, \overline{n})$-sequence and $I \subseteq \{(i,j) \mid 1 \leq i \leq q \text{ and } 1 \leq j \leq n_i\}$ be a non-empty set. We associate two random variables X and Y_I to $\mathcal{L}$ and I. The first one takes values in the secret space $\mathbb{Z}_{m_0}$, while

the second one into $\prod_{(i,j)\in I}\mathbb{Z}_{m_{i,j}}$. Given $y_I \in \prod_{(i,j)\in I}\mathbb{Z}_{m_{i,j}}$, define the *loss of entropy with respect to* y_I [12], denoted $\Delta(y_I)$, by

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

The following result was proposed in [12] for the case of the threshold secret sharing scheme in [5]. However, it can be easily adapted for $(\epsilon, \overline{k}, \overline{n})$-sequences as well.

Lemma 12 ([12]). *Let $\mathcal{L} = (m_0, (L_i|1 \le i \le q))$ be an $(\epsilon, \overline{k}, \overline{n})$-sequence and $I \subseteq \{(i,j)\ |1 \le i \le q \text{ and } 1 \le j \le n_i\}$ be a non-empty set. The loss of entropy of $\mathcal{L}$ with respect to $y_I \in \prod_{(i,j)\in I}\mathbb{Z}_{m_{i,j}}$ and a uniform distribution on the secret space satisfies the following relations:*

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

where

$$C(I) = \left\lfloor \frac{min_{i=1}^{q} m_{i,1}^{k_i}}{\prod_{(i,j)\in I} m_{i,j}} \right\rfloor$$

A distributive weighted threshold secret sharing scheme for a DWTAS $(\overline{k}, w, \Gamma)$ over a set U of participants is called *asymptotically perfect* if for any $\lambda > 0$ there exists $m \ge 0$ such that any $(\epsilon, \overline{k}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i|1 \le i \le q))$ associated to $(\overline{k}, w, \Gamma)$ with $m_0 \ge m$ satisfies the following properties:

- $H(X) \neq 0$;
- $|\Delta(y_{I_A})| < \lambda$, for any unauthorized set A and any $y_{I_A} \in \prod_{(i,j)\in I_A}\mathbb{Z}_{m_{i,j}}$ (recall that I_A is the set of all pairs (i,j) such that the jth participant on the ith level is in A).

Theorem 13. *The CRT-based distributive weighted threshold secret sharing scheme is asymptotically perfect if the secret is chosen uniformly from the secret space.*

Proof. Let $\mathcal{L} = (m_0, (L_i|1 \le i \le q))$ be an $(\epsilon, \overline{k}, \overline{n})$-sequence associated to a DWTAS $(\overline{k}, w, \Gamma)$ over a set U of participants. Let $\alpha = \max_{i=1}^{q} m_{i,n_i}^{k_i-\epsilon}$ and $\beta = \min_{i=1}^{q} m_{i,1}^{k_i}$ as in Definition 7.

If A is an unauthorized set, then $C(I_A) \neq 0$. Using that $x - 1 < \lfloor x \rfloor \le x$ and $C(I_A) = \left\lfloor \dfrac{\beta}{M_{I_A}} \right\rfloor$, where $M_{I_A} = \prod_{(i,j)\in I_A} m_{i,j}$, we have:

$$\begin{aligned}
\log \frac{m_0\left(\left\lfloor \frac{C(I_A)+1}{m_0}\right\rfloor + 1\right)}{C(I_A)} &< \log \frac{C(I_A) + m_0 + 1}{C(I_A)} \\
&< \log \frac{\beta + m_0 M_{I_A} + M_{I_A}}{\beta - M_{I_A}} \\
&= \log \frac{1 + \frac{m_0 M_{I_A}}{\beta} + \frac{M_{I_A}}{\beta}}{1 - \frac{M_{I_A}}{\beta}}
\end{aligned}$$

As $m_0\alpha < \beta$ and $M_{I_A} \leq \alpha^\theta$ for some $\theta < 1$ (by Lemma 11), we obtain:

$$\frac{m_0 M_{I_A}}{\beta} \leq \frac{m_0 \alpha^\theta}{\beta} < \frac{m_0^{1-\theta}}{\beta^{1-\theta}} = \left(\frac{m_0}{\beta}\right)^{1-\theta} < \left(\frac{1}{\alpha}\right)^{1-\theta}$$

The last term of this sequence of inequalities goes to 0 as m_0 goes to infinity (remark that $1-\theta$ is a fixed quantity). Therefore, $\dfrac{m_0 M_{I_A}}{\beta}$ goes to 0 as m_0 goes to infinity. This proves that $\dfrac{M_{I_A}}{\beta}$ goes to 0 too as m_0 goes to infinity. Putting all together, Lemma 12 shows that $\Delta(y_{I_A})$ goes to 0 as m_0 goes to infinity. ■

5.2. Asymptotic idealness

Following [12], the distributive weighted threshold secret sharing scheme for a DWTAS $(\overline{k}, w, \Gamma)$ over a set U of participants is called *asymptotically ideal* if it is asymptotic perfect and for any $\lambda > 0$ there exists $m \geq 0$ such that any $(\epsilon, \overline{k}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ associated to $(\overline{k}, w, \Gamma)$ with $m_0 \geq m$ satisfies

$$\frac{|\mathbb{Z}_{m_{i,j}}|}{|\mathbb{Z}_{m_0}|} < 1 + \lambda,$$

for any $1 \leq i \leq q$ and $1 \leq j \leq n_i$ ($|\mathbb{Z}_{m_{i,j}}|/|\mathbb{Z}_{m_0}|$ is the *information rate* of the jth participant on the ith level).

As $m_{i,j}$ can be arbitrarily large in comparison with m_0 (one can see that in the proof of Theorem 9 the prime p_i can be arbitrarily large which shows that the distance between m_0 and the integers $m_{i,j}$ can be arbitrarily large), we conclude that the distributive weighted threshold secret sharing scheme cannot be asymptotically ideal. Moreover, the information rate is not upper-bounded. If we make use of Lemma 8 we can establish a lower bound for the information rate. Namely, from Lemma 8(1) it follows that $m_0 < m_{i,j}^\epsilon$, for any $1 \leq i \leq q$ and $1 \leq j \leq n_i$. Therefore,

$$\frac{|\mathbb{Z}_{m_{i,j}}|}{|\mathbb{Z}_{m_0}|} > m_0^{1/\epsilon - 1},$$

for any i and j (recall that $\epsilon < 1$ in the definition of the distributive weighted threshold secret sharing scheme).

5.3. Perfect zero-knowledge

Let $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ be an $(\epsilon, \overline{k}, \overline{n})$-sequence and $I \subseteq \{(i,j) \mid 1 \leq i \leq q \text{ and } 1 \leq j \leq n_i\}$ be a non-empty set. Given a secret $S \in \mathbb{Z}_{m_0}$ consider the random variable $Y_{S,I}$ which takes values $y_I \in \prod_{(i,j)\in I} \mathbb{Z}_{m_{i,j}}$ as possible shares for all $(i,j) \in I$ in the same process of sharing S.

The distributive weighted threshold secret sharing scheme for a DWTAS $(\overline{k}, w, \Gamma)$ over a set U of participants is called *perfect zero-knowledge* [12] if for any polynomial *poly* there exists $m \geq 0$ such that for any $(\epsilon, \overline{k}, \overline{n})$-sequence $\mathcal{L} = (m_0, (L_i | 1 \leq i \leq q))$ associated to $(\overline{k}, \overline{n}, \Gamma)$ with $m_0 \geq m$, any secrets $S, S' \in \mathbb{Z}_{m_0}$, and any unauthorized set A, the following holds:

$$\sum_{y_{I_A} \in \prod_{(i,j)\in I_A} \mathbb{Z}_{m_{i,j}}} \left| P(Y_{S,I_A} = y_{I_A}) - P(Y_{S',I_A} = y_{I_A}) \right| \leq \frac{1}{poly(m_0)} \qquad (11)$$

That is, it is indistinguishable whether the shares $y_{I_A} = (y_{i,j}|(i,j) \in I_A)$ come from S or from S'.

Theorem 14. *The CRT-based distributive weighted threshold secret sharing scheme is perfect zero-knowledge if the secret is chosen uniformly from the secret space.*

Proof. Let $\mathcal{L} = (m_0, (L_i|1 \leq i \leq q))$ be an $(\epsilon, \overline{k}, \overline{n})$-sequence associated to $(\overline{k}, w, \Gamma)$, and let $\alpha = \max_{i=1}^{q} m_{i,n_i}^{k_i - \epsilon}$ and $\beta = \min_{i=1}^{q} m_{i,1}^{k_i}$. Consider further an unauthorized set A, and S and S' two secrets from $\mathbb{Z}_{m_0}$.

If U_{I_A} is an uniform random variable on $\prod_{(i,j)\in I_A} \mathbb{Z}_{m_{i,j}}$, then:

$$\left|P(Y_{S,I_A} = y_{I_A}) - P(Y_{S',I_A} = y_{I_A})\right| \leq$$

$$|P(Y_{S,I_A} = y_{I_A}) - P(U_{I_A} = y_{I_A})| + \left|P(Y_{S',I_A} = y_{I_A}) - P(U_{I_A} = y_{I_A})\right|$$

In order to prove the theorem, it is sufficient to look for a suitable upper bound for the term

$$\sum_{y_{I_A} \in \prod_{(i,j)\in I_A} \mathbb{Z}_{m_{i,j}}} |P(Y_{S,I_A} = y_{I_A}) - P(U_{I_A} = y_{I_A})| .$$

For simplicity, let $M_{I_A} = \prod_{(i,j)\in I_A} m_{i,j}$. There exists an isomorphism h from $\prod_{(i,j)\in I_A} \mathbb{Z}_{m_{i,j}}$ to $\mathbb{Z}_{M_{I_A}}$, so let Z_{I_A} denote a new variable such that U_{I_A} takes the value y_{I_A} with probability p if and only if Z_{I_A} takes the value $h(y_{I_A})$ with probability p. Given the property that for any $y_{I_A} \in \prod_{(i,j)\in I_A} \mathbb{Z}_{m_{i,j}}$ there exists a unique $r \in \mathbb{Z}_{M_{I_A}}$ such that $y_{i,j} = (S + r \cdot m_0) \ mod \ m_{i,j}$ for all $(i,j) \in I_A$, let R_S denote a random variable with values in $\mathbb{Z}_\beta$ such that

$$\sum_{y_{I_A} \in \prod_{(i,j)\in I_A} \mathbb{Z}_{m_{i,j}}} |P(Y_{S,I_A} = y_{I_A}) - P(U_{I_A} = y_{I_A})| =$$

$$\sum_{r \in \mathbb{Z}_{M_{I_A}}} |P(R_S \ mod M_{I_A} = r) - P(Z_{I_A} = r)|$$

If $0 \leq r < (\beta \ mod \ M_{I_A})$, then

$$P(R_S \ mod \ M_{I_A} = r) = \frac{\frac{\beta - (\beta \ mod \ M_{I_A})}{M_{I_A}} + 1}{\beta}$$

and if $(\beta \ mod \ M_{I_A}) \leq r < M_{I_A}$ then

$$P(R_S \ mod \ M_{I_A} = r) = \frac{\beta - (\beta \ mod \ M_{I_A})}{\beta M_{I_A}}$$

Combining these with $P(Z_{I_A} = r) = 1/M_{I_A}$, we obtain

$$\sum_{r \in \mathbb{Z}_{M_{I_A}}} |P(R_S \ mod \ M_{I_A} = r) - P(Z_{I_A} = r)| = 2\left(\frac{\beta \ mod \ M_{I_A}}{\beta} - \frac{(\beta \ mod \ M_{I_A})^2}{\beta M_{I_A}}\right)$$

As $w(A) < 1$, we have $M_{I_A} < \alpha$. Combining with $m_0\alpha < \beta$ the result of the theorem easily follows. ■

6. Conclusions

In this paper we have introduced *distributive weighted threshold access structures* as a subclass of weighted threshold access structures. The authorized sets of a distributive weighted threshold access structure are either the authorized sets of the component threshold access structures or sets of participants on different levels whose sum of weights exceeds 1. From this point of view, distributive weighted threshold access structures can be viewed as a method of combining disjoint threshold access structures, yielding "extensions" of disjunctive multilevel access structures (in the sense in Remark 2).

We have proposed an asymptotically perfect (Theorem 13) and perfect zero-knowledge (Theorem 14) CRT-based realization of them. As with respect to idealness, we have proved that distributive weighted threshold access structures do not generally have ideal realizations (Theorem 6). From this point of view, our scheme is all that can be achieved using CRT.

One can easily see that if we restrict distributive threshold access structures to just one level, then the distributive weighted threshold secret sharing scheme proposed in this paper is a variation of the Asmuth-Bloom threshold scheme [3]. Moreover, this variation is both asymptotically perfect and perfect zero-knowledge, while the original Asmuth-Bloom threshold scheme does not meet these properties.

We leave open the problem of finding perfect (and not only asymptotically perfect) realizations of distributive weighted threshold access structures, and we emphasize once more that distributive weighted threshold access structures do not generally have ideal realizations (Theorem 6).

We end the paper by a parallel between our work and, probably, the closest work to ours [19] (see also [11]). In [19], CRT-based realizations of weighted threshold access structures were proposed. The main idea in [19] is the next one. Given a set $U = \{1, \ldots, n\}$ of $n \geq 2$ participants, a weight function $w : U \to \mathbf{N} - \{0\}$, and a threshold t satisfying $2 \leq t \leq \sum_{i \in U} w(i)$, define a sequence of integers $m_1, \ldots, m_n$ as follows:

1. consider first a sequence of positive integers

$$m'_1, \ldots, m'_N$$

   satisfying a Mignotte- or Asmuth-Bloom-like constraint [19, 11], where $N = \sum_{i \in U} w(i)$ (this sequence is regarded as corresponding to N participants each of which having weight one);
2. group the elements of the above sequence into n groups $U_1, \ldots, U_n$ such that $|U_i| = w(i)$, for all $1 \leq i \leq n$ (that is, $w(i)$ participants each with weight one are regarded as one participant with weight $w(i)$);
3. for each group U_i compute the least common multiple m_i of its elements, $1 \leq i \leq n$.

The resulting sequence $m_1, \ldots, m_n$ satisfies a similar constraint to the initial sequence $m'_1, \ldots, m'_N$ [19], and it can be used for secret sharing in the Mignote or Asmuth-Bloom style, depending on the imposed constraint. It is to be mentioned that [19, 11] do not provide any security analysis of the schemes proposed.

Although the construction above [19] is interesting, it suffers from several drawbacks:

1. each integer m_i is composed of $w(i)$ proper factors (being the least common multiple of the set U_i of cardinality $w(i)$). Therefore, except for the case $w(i) = 1$, none of the integers m_i is a prime;
2. as the sequence $m_1, \ldots, m_n$ mainly consists of composite integers, the security results in [12] cannot be applied in this case (the security results in [12] make use of sequences of consecutive primes);
3. good security results can be obtained even for sequences of pair-wise co-primes [20, 21], but in this case the sequence should fulfill some compactness properties: all its elements should be in a compact interval (an interval is compact if it is of the form $(a - a^\theta, a + a^\theta)$ for some integer a and real number $\theta \in (0, 1)$). It is not clear how the sequences proposed in [19] and described above can be chosen from a compact interval and composed of pair-wise co-prime integers;
4. the sequences proposed in [19] are direct generalizations of the Mignotte [4] and Asmuth-Bloom [3] sequences of co-primes. Unfortunately, the Mignotte threshold secret sharing is far from being asymptotically perfect [20]; the Asmuth-Bloom threshold scheme provides better security than the Mignotte scheme, but it is still not asymptotically perfect if it is based on arbitrary sequences of co-primes [20]. Direct generalizations of the Mignotte and Asmuth-Bloom sequences of co-primes by renouncing to co-primality certainly do not lead to better security properties.

The $(\epsilon, \overline{k}, \overline{n})$-sequences used in our paper fulfill a kind of compactness due to the real number $\epsilon \in (0, 1]$, which is crucial when establishing the security of the proposed scheme.

[1] G. Blakley, "Safeguarding cryptographic keys," in *1979 AFIPS National Computer Conference*. AFIPS Press, 1979, pp. 313–317.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[3] 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.

[4] 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.

[5] 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.

[6] P. Morillo, C. Padr, G. Sez, and J. Villar, "Weighted threshold secret sharing schemes," *Information Processing Letters*, vol. 70, no. 5, pp. 211–216, 1999.

[7] A. Beimal, T. Tassa, and E. Weinreb, "Characterizing ideal weighted threshold secret sharing," in *2nd International Conference on the Theory of Cryptography*, ser. Lecture Notes in Computer Science, vol. 3378, 2005, pp. 600–619.

[8] ——, "Characterizing ideal weighted threshold secret sharing," *SIAM Journal of Discrete Mathematics*, vol. 22, no. 1, pp. 360–397, 2008.

[9] M. Wang, Z. J. Liu, and Y. S. Zhang, "Secret sharing among weighted participants," *Journal of Beijing Electronic Science and Technology Institute*, vol. 13, no. 2, pp. 1–9, 2005.

[10] C.-W. Chan and C.-C. Chang, "A scheme for threshold multi-secret sharing," *Applied Mathematics and Computation*, vol. 166, no. 1, pp. 1–14, 2005.

[11] S. Iftene, "Secret sharing schemes with applications in security protocols," Ph.D. dissertation, "AL.I.Cuza" University of Iasi, Romania, 2007.

[12] 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.

[13] G. J. Simmons, "How to (really) share a secret," in *8th Annual International Cryptology Conference on Advances in Cryptology (CRYPT '88)*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed., vol. 403. Springer, 1988, pp. 390–448.

[14] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptology*, vol. 20, no. 2, pp. 237–264, 2007.

[15] M. Belenkiy, "Disjunctive multi-level secret sharing," Brown University, Tech. Rep., 2008.

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

[17] D. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Chapman and Hall/CRC, 2005.

[18] P. Ribenboim, *The New Book of Prime Number Record*, 3rd ed. Springer Verlag, 1996.

[19] S. Iftene, "General secret sharing based on the chinese remainder theorem with applications in e-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, no. 0, pp. 67 – 84, 2007, proceedings of the First Workshop in Information and Computer Security (ICS 2006).

[20] M. Barzu, F. L. iplea, and C. C. Drgan, "Compact sequences of co-primes and their applications to the security of crt-based threshold schemes," *Information Sciences*, vol. 240, no. 0, pp. 161 – 172, 2013.

[21] F. L. iplea and C. C. Drgan, "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.