Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Electronic Notes in Theoretical Computer Science 186 (2007) 67–84
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting

Sorin Iftene[1]

Faculty of Computer Science
"Al.I.Cuza" University
Iaşi, Romania

Abstract

Threshold secret sharing based on the Chinese remainder theorem has been considered by Mignotte [23] and Asmuth and Bloom [1]. In this paper we demonstrate that the Chinese remainder theorem can be used for realizing more general access structures, as the compartmented or the weighted threshold ones. We also prove that there exist some non-weighted threshold access structures whose realizations require the general variant of the Chinese remainder theorem, i.e., the variant in which the modules are not necessarily pairwise coprime.
As an application of the proposed secret sharing schemes, we present a multi-authority e-voting schemes in which, as a novelty, the tallying authorities may have non-equal weights.

Keywords: secret sharing, Chinese remainder theorem, e-voting

1 Introduction and Preliminaries

A secret sharing scheme starts with a *secret* and then derives from it certain *shares* (or *shadows*) which are distributed to users. The secret may be recovered only by certain groups which belong to a predetermined *access structure*. In the first secret sharing schemes only the number of shares was important for recovering the secret. Such schemes have been referred to as *threshold* secret sharing schemes. We mention here Shamir's scheme [29] based on polynomial interpolation, Blakley's geometric scheme [5], Mignotte's scheme [23] and Asmuth-Bloom scheme [1], both based on the Chinese remainder theorem. Ito, Saito, and Nishizeki [19], Benaloh and Leichter [4] have proposed constructions for more general secret sharing schemes.

In this paper we prove that the Chinese remainder theorem can be used for realizing more general access structures. We consider first the *compartmented* secret

[1] Email: siftene@infoiasi.ro

doi:10.1016/j.entcs.2007.01.065

sharing schemes, in which the set of users is partitioned into compartments and the secret can be recovered if and only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold and the total number of participants is greater than or equal to a global threshold. We extend Brickell's construction [6] to the case that the global threshold is strictly greater than the sum of the compartment thresholds and we indicate how to use the threshold secret sharing schemes based on the Chinese remainder theorem in order to decrease the size of shares.

We also extend the threshold Mignotte and Asmuth-Bloom schemes in order to address more general access structures. We present how to realize any *weighted threshold* access structure (in which some positive weight is associated to each user and the secret can be reconstructed if and only if the sum of the weights of the participants is greater than or equal to a fixed threshold) but we prove that our extensions are also suitable for some non-weighted threshold access structures.

The paper is organized as follows. The rest of this section is dedicated to some preliminaries on number theory, focusing on the Chinese remainder theorem. After a short introduction to secret sharing, we survey the threshold secret sharing schemes based on the Chinese remainder theorem in Section 2. In Section 3 we extend the Brickell's construction for compartmented secret sharing to the case that the global threshold is strictly greater than the sum of the compartment thresholds and we indicate how to use the threshold secret sharing schemes based on the Chinese remainder theorem in order to decrease the size of shares. In Section 4 we extend the threshold secret sharing schemes based on the Chinese remainder theorem to more general access structures and discuss the homomorphic properties of the resulted schemes. In Section 5 we describe a multi-authority e-voting scheme based on the proposed secret sharing schemes. Our conclusions and some interesting future research directions are presented in the last section.

In the rest of this section we present some basic facts and notations from number theory. For more details, the reader is referred to [8].

Let $a, m \in \mathbb{Z}$, $m \neq 0$. The *quotient* of the integer division of a by m will be denoted by $a \texttt{ div } m$ and the *remainder* will be denoted by $a \texttt{ mod } m$. Let $a, b, m \in \mathbb{Z}$. We say that a and b are *congruent modulo* m, and we use the notation $a \equiv b \ mod \ m$, if $m|(a-b)$. In case $m \neq 0$, $a \equiv b \ mod \ m$ is equivalent with $a \texttt{ mod } m = b \texttt{ mod } m$. The set $\{0, 1, \ldots, m-1\}$ will be denoted by $\mathbb{Z}_m$, for any integer $m \geq 1$.

Let $a_1, \ldots, a_n \in \mathbb{Z}$, $a_1^2 + \cdots + a_n^2 \neq 0$. The *greatest common divisor* (*gcd*) of $a_1, \ldots, a_n$ will be denoted by $(a_1, \ldots, a_n)$. It is well-known that there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ that satisfy $\alpha_1 a_1 + \cdots + \alpha_n a_n = (a_1, \ldots, a_n)$ (the linear form of the *gcd*).

Let $a_1, \ldots, a_n \in \mathbb{Z}$ such that $a_1 \cdots a_n \neq 0$. The *least common multiple* (*lcm*) of $a_1, \ldots, a_n$ will be denoted by $[a_1, \ldots, a_n]$.

The Chinese remainder theorem has many applications in computer science (see [10] for a survey on this topic). We only mention its applications to the *RSA* decryption algorithm as proposed by Quisquater and Couvreur [27], the discrete logarithm algorithm as proposed by Pohlig and Hellman [26], and the algorithm

for recovering the secret in Mignotte's threshold secret sharing scheme [23] or in Asmuth-Bloom threshold secret sharing scheme [1].

Several versions of the Chinese remainder theorem have been proposed. The next one is called the *general* Chinese remainder theorem ([24]):

Theorem 1.1 *Let $k \geq 2$, $p_1, \ldots, p_k \geq 2$, and $b_1, \ldots, b_k \in \mathbb{Z}$. The system of equations*

$$\begin{cases} x \equiv b_1 \ mod \ p_1 \\ \quad \vdots \\ x \equiv b_k \ mod \ p_k \end{cases}$$

has solutions in $\mathbb{Z}$ if and only if $b_i \equiv b_j \ mod \ (p_i, p_j)$, for all $1 \leq i, j \leq k$. Moreover, if the above system of equations has solutions in $\mathbb{Z}$, then it has a unique solution in $\mathbb{Z}_{[p_1,\ldots,p_k]}$.

Ore has proven that this solution can be obtained as

$$\sum_{i=1}^{k} \gamma_i \delta_i b_i \ \texttt{mod} \ [p_1, \ldots, p_k],$$

where $\delta_i = \frac{[p_1,\ldots,p_k]}{p_i}$, for all $1 \leq i \leq k$, and $\gamma_1, \ldots, \gamma_k$ are arbitrary integers such that $\gamma_1\delta_1 + \cdots + \gamma_k\delta_k = 1$ (remark that $(\delta_1, \ldots, \delta_k) = 1$).

When $(p_i, p_j) = 1$, for all $1 \leq i < j \leq k$, one gets the *standard* version of the Chinese remainder theorem. Garner [13] has found an efficient algorithm for this case and Fraenkel [12] has extended it to the general case.

2 Threshold Secret Sharing Schemes Based on the Chinese Remainder Theorem

We present first some basic facts about secret sharing schemes. The reader is referred to [31] for a survey on this topic. Suppose we have n users labeled with the numbers $1, \ldots, n$ and consider a set of groups[2] $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. Informally, an *$\mathcal{A}$-secret sharing scheme* is a method of generating $(S, (I_1, \ldots, I_n))$ such that

- (*correctness*) for any $A \in \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$, is "easy";
- (*security*) for any $A \in \mathcal{P}(\{1, 2, \ldots, n\}) \setminus \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$, is intractable.

The set $\mathcal{A}$ will be referred to as the *authorized access structure* or simply as the *access structure*, S will be referred to as the *secret* and $I_1, \ldots, I_n$ will be referred to as the *shares* (or the *shadows*) of S. The elements of the set $\mathcal{A}$ will be referred to as the *authorized groups*.

[2] $\mathcal{P}(\{1, 2, \ldots, n\})$ denotes the set of all subsets of the set $\{1, 2, \ldots, n\}$.

In a *perfect* secret sharing scheme, the shares of any unauthorized group give no information (in information-theoretic sense) about the secret. Karnin, Greene, and Hellman [20] have proven, using the concept of entropy, that in any perfect threshold secret sharing scheme, the shares must be at least as long as the secret and, later on, Capocelli, De Santis, Gargano, and Vaccaro [7] have extended this result to the case of any perfect secret sharing scheme. In an *ideal* secret sharing scheme, the shares are as long as the secret.

A natural condition is that an access structure $\mathcal{A}$ be *monotone* ([4]), i.e.,

$$(\forall B \in \mathcal{P}(\{1,2,\ldots,n\}))((\exists A \in \mathcal{A})(A \subseteq B) \Rightarrow B \in \mathcal{A}).$$

Any monotone access structure $\mathcal{A}$ is well specified by the set of the minimal authorized groups, i.e., the set $\mathcal{A}_{min} = \{A \in \mathcal{A} | (\forall B \in \mathcal{A} \setminus \{A\})(\neg B \subseteq A)\}$. Also, the unauthorized access structure $\overline{\mathcal{A}}$, $\overline{\mathcal{A}} = \mathcal{P}(\{1,2,\ldots,n\}) \setminus \mathcal{A}$, is well specified by the set of the maximal unauthorized groups, i.e., the set $\overline{\mathcal{A}}_{max} = \{A \in \overline{\mathcal{A}} | (\forall B \in \overline{\mathcal{A}} \setminus \{A\})(\neg A \subseteq B)\}$.

In the first secret sharing schemes only the number of the participants in the reconstruction phase was important for recovering the secret. Such schemes have been referred to as *threshold* secret sharing schemes.

Definition 2.1 Let $n \geq 2$, $2 \leq k \leq n$. The access structure

$$\mathcal{A} = \{A \in \mathcal{P}(\{1,2,\ldots,n\}) \mid |A| \geq k\}$$

will be referred to as the (k,n)-*threshold* access structure.

In this case we also obtain that $\mathcal{A}_{min} = \{A \in \mathcal{P}(\{1,2,\ldots,n\}) \mid |A| = k\}$, $\overline{\mathcal{A}} = \{A \in \mathcal{P}(\{1,2,\ldots,n\}) \mid |A| \leq k-1\}$, and $\overline{\mathcal{A}}_{max} = \{A \in \mathcal{P}(\{1,2,\ldots,n\}) \mid |A| = k-1\}$. Any $\mathcal{A}$-secret sharing scheme will be referred to as an (k,n)-*threshold secret sharing scheme*.

We briefly discuss next the most important threshold secret sharing schemes based on the Chinese remainder theorem.

2.1 Mignotte's Threshold Secret Sharing Scheme

Mignotte's threshold secret sharing scheme [23] uses some special sequences of integers, referred to as the *Mignotte sequences*.

Definition 2.2 Let n be a positive integer, $n \geq 2$, and $2 \leq k \leq n$. An (k,n)-*Mignotte sequence* is a sequence of pairwise coprime positive integers $p_1 < p_2 < \cdots < p_n$ such that

$$\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

The above inequality is equivalent with

$$max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}(p_{i_1} \cdots p_{i_{k-1}}) < min_{1 \leq i_1 < \cdots < i_k \leq n}(p_{i_1} \cdots p_{i_k}).$$

Given a publicly known (k, n)-Mignotte sequence, the scheme works as follows:

- The secret S is chosen as a random integer such that $\beta < S < \alpha$, where $\alpha = \prod_{i=1}^{k} p_i$ and $\beta = \prod_{i=0}^{k-2} p_{n-i}$;
- The shares I_i are chosen as $I_i = S \bmod p_i$, for all $1 \leq i \leq n$;
- Given k distinct shares $I_{i_1}, \ldots, I_{i_k}$, the secret S is recovered, using the standard variant of the Chinese remainder theorem, as the unique solution modulo $p_{i_1} \cdots p_{i_k}$ of the system

$$\begin{cases} x \equiv I_{i_1} \ mod \ p_{i_1} \\ \quad \vdots \\ x \equiv I_{i_k} \ mod \ p_{i_k} \end{cases}.$$

Indeed, the secret S is an integer solution of the above system by the choice of the shadows and, moreover, S lies in $\mathbb{Z}_{p_{i_1} \cdots p_{i_k}}$ because $S < \alpha$. On the other hand, having only $k-1$ distinct shares $I_{i_1}, \ldots, I_{i_{k-1}}$, we obtain only that $S \equiv x_0 \mod p_{i_1} \cdots p_{i_{k-1}}$, where x_0 is the unique solution modulo $p_{i_1} \cdots p_{i_{k-1}}$ of the resulted system (in this case, $S > \beta \geq p_{i_1} \cdots p_{i_{k-1}} > x_0$). Therefore, in order to assure a reasonable level of security, (k, n)-Mignotte sequences with a large factor $\frac{\alpha - \beta}{\beta}$ must be chosen (a method of generating such sequences is presented in [21, page 9]).

Obviously, Mignotte's scheme is not perfect, but it can lead to small shares and, thus, can be used in applications in which the compactness of the shares is the deciding factor.

We have extended Mignotte's scheme in [17], by introducing the generalized threshold Mignotte sequences whose elements are not necessarily pairwise coprime.

Definition 2.3 Let n be an integer, $n \geq 2$, and $2 \leq k \leq n$. A *generalized* (k, n)-*Mignotte sequence* is a sequence $p_1, \ldots, p_n$ of positive integers such that

$$max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}([p_{i_1}, \ldots, p_{i_{k-1}}]) < min_{1 \leq i_1 < \cdots < i_k \leq n}([p_{i_1}, \ldots, p_{i_k}]).$$

It is easy to see that every (k, n)-Mignotte sequence is a generalized (k, n)-Mignotte sequence. Moreover, if we multiply every element of a (generalized) (k, n)-Mignotte sequence $p_1, \ldots, p_n$ by a fixed element $\delta \in \mathbb{Z}$, $(\delta, p_1 \cdots p_n) = 1$, we also obtain a generalized (k, n)-Mignotte sequence.

The extended Mignotte scheme works like Mignotte's scheme, where $\alpha = min_{1 \leq i_1 < \cdots < i_k \leq n}([p_{i_1}, \ldots, p_{i_k}])$ and $\beta = max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}([p_{i_1}, \ldots, p_{i_{k-1}}])$. In this case, the general variant of the Chinese remainder theorem must be used for recovering the secret.

2.2 Asmuth-Bloom Threshold Secret Sharing Scheme

This scheme, proposed by Asmuth and Bloom in [1], also uses some special sequences of integers. More exactly, a sequence of pairwise coprime positive integers $p_0, p_1 <$

$\cdots < p_n$ is chosen such that

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

Given a publicly known Asmuth-Bloom sequence, the scheme works as follows:

- The secret S is chosen as a random element of the set $\mathbb{Z}_{p_0}$;
- The shares I_i are chosen as $I_i = (S + \gamma \cdot p_0) \bmod p_i$, for all $1 \leq i \leq n$, where γ is an arbitrary integer such that $S + \gamma \cdot p_0 \in \mathbb{Z}_{p_1 \cdots p_k}$;
- Given k distinct shares $I_{i_1}, \ldots, I_{i_k}$, the secret S can be reconstructed as $S = x_0 \bmod p_0$, where x_0 is obtained, using the standard variant of the Chinese remainder theorem, as the unique solution modulo $p_{i_1} \cdots p_{i_k}$ of the system

$$\begin{cases} x \equiv I_{i_1} \ mod \ p_{i_1} \\ \quad \vdots \\ x \equiv I_{i_k} \ mod \ p_{i_k} \end{cases}.$$

Goldreich, Ron, and Sudan [15] have proposed choosing $p_0, p_1, \ldots, p_n$ as prime numbers of the same size. Quisquater, Preneel, and Vandewalle [28] have proven that, by choosing $p_0, p_1, \ldots, p_n$ as consecutive primes, the resulted schemes are asymptotically perfect and asymptotically ideal (for technical details, the reader is referred to [28]).

The sequences used in Asmuth-Bloom scheme can be also generalized by allowing modules that are not necessarily pairwise coprime in an obvious manner. We can use any sequence $p_0, p_1, \cdots, p_n$ such that

$$p_0 \cdot max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}([p_{i_1}, \ldots, p_{i_{k-1}}]) < min_{1 \leq i_1 < \cdots < i_k \leq n}([p_{i_1}, \ldots, p_{i_k}]).$$

It is easy to see that if we multiply the elements, excepting the first one, of a (generalized) Asmuth-Bloom sequence $p_0, p_1, \cdots, p_n$ with a fixed element $\delta \in \mathbb{Z}$, $(\delta, p_0 \cdots p_n) = 1$, we also obtain a generalized Asmuth-Bloom sequence.

3 Compartmented Secret Sharing Based on the Chinese Remainder Theorem

In case of compartmented secret sharing, the set of users is partitioned into compartments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold, and the total number of participants is greater than or equal to a global threshold. The compartmented secret sharing has been discussed for the first time by Simmons in [30]. Simmons has presented the example of an official action that requires that at least two U.S. members and at least two U.S.S.R. members be simultaneously present for its initiation.

The compartmented access structures can be introduced as follows.

Definition 3.1 Let $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ be a partition of $C_0 = \{1, 2, \ldots, n\}$ and consider a sequence $\mathcal{K} = (k_0, k_1, k_2, \ldots, k_m)$, where $k_j \leq |C_j|$, for all $0 \leq j \leq m$, and $\sum_{j=1}^{m} k_j \leq k_0$. The $(\mathcal{C}, \mathcal{K})$-*compartmented access structure* is given by

$$\mathcal{A} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid (\forall j = \overline{0, m})(|A \cap C_j| \geq k_j)\}.$$

In this case, any $\mathcal{A}$-secret sharing scheme will be referred to as a $(\mathcal{C}, \mathcal{K})$-*compartmented secret sharing scheme*. The sets $C_1, C_2, \ldots, C_m$ will be referred to as the *compartments* of the scheme, the values $k_1, k_2, \ldots, k_m$ as the *compartment thresholds* and k_0 as the *global threshold* of the scheme.

An (k, n)-threshold secret sharing scheme is nothing else than a $(\mathcal{C}, \mathcal{K})$-compartmented secret sharing scheme with $\mathcal{C} = \{\{1, 2, \ldots, n\}\}$ $(m = 1)$ and $\mathcal{K} = (k, k)$.

Brickell [6] has proposed an elegant solution for the case $k_0 = \sum_{j=1}^{m} k_j$ by expressing the secret S as a combination of some compartment secrets $s_1, \ldots, s_m$ and using an $(k_j, |C_j|)$-threshold secret sharing scheme for obtaining the shares $\{I_i | i \in C_j\}$ corresponding to the compartment secret s_j, for all $1 \leq j \leq m$. In the reconstruction phase, if the number of participants from the j^{th} compartment is greater than or equal to k_j, for all $1 \leq j \leq m$, then all compartment secrets can be recovered and, thus, the secret S can be obtained (remark that in this case the compartmented access structure can be simplified to $\{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid (\forall j = \overline{1, m})(|A \cap C_j| \geq k_j)\}$).

Ghodosi, Pieprzyk, and Safavi-Naini proposed an efficient scheme for the general case in [14].

We extend Brickell's construction to the case $\sum_{j=1}^{m} k_j < k_0$ as follows.

- The secret is chosen as $S = s_0 + s_1 + \cdots + s_m$, where $s_0, s_1, \ldots, s_m$ are positive integers;
- The shares are chosen as $I_i = (g_i, c_i)$, for any $1 \leq i \leq n$, where
  - $g_1, \ldots, g_n$ are the shares corresponding to the secret s_0 with respect to an arbitrary (k_0, n)-threshold secret sharing scheme - these elements will be referred to as the *global* components of the shares;
  - for every $1 \leq j \leq m$, $\{c_i | i \in C_j\}$ are the shares corresponding to the secret s_j with respect to an arbitrary $(k_j, |C_j|)$-threshold secret sharing scheme - these elements will be referred to as the *compartment* components of the shares.

Remark 3.2 (Correctness)
Let A be an authorized access group. Thus, $|A| \geq k_0$ and, for all $j = \overline{1, m}$, $|A \cap C_j| \geq k_j$. Having at least k_0 of the shares $g_1, \ldots, g_n$, the value s_0 can be obtained. Then, for any $j = \overline{1, m}$, having at least k_j of the shares $\{c_i | i \in C_j\}$, the value s_j can be obtained, and finally, the secret S can be reconstructed as $S = s_0 + s_1 + \cdots + s_m$.

Remark 3.3 (Security)
Let A be an unauthorized access group. There are two possibilities:

- $|A| < k_0$ - in this case, the value s_0 can not be determined;
- There is an compartment j such that $|A \cap C_j| < k_j$ - in this case the value s_j can not be determined.

In both cases, the secret S can not be reconstructed.

Using perfect threshold secret sharing schemes as building blocks can lead to large shares. We propose using the threshold secret sharing schemes based on the Chinese remainder theorem in order to decrease the size of shares, maintaining, at the same time, a reasonable level of security. For simplicity, we shall use only Mignotte's scheme, but we have to mention that this technique can be also applied using Asmuth-Bloom scheme.

For any $0 \leq j \leq m$, we will generate and broadcast a generalized $(k_j, |C_j|)$-Mignotte sequence $(p_{j,i} | i \in C_j)$. Let $\beta_j = max_{i_1,\ldots,i_{k_j-1} \in C_j}([p_{j,i_1}, \ldots, p_{j,i_{k_j-1}}])$ and $\alpha_j = min_{i_1,\ldots,i_{k_j} \in C_j}([p_{j,i_1}, \ldots, p_{j,i_{k_j}}])$, for $0 \leq j \leq m$. We may use a generalized Mignotte sequence twice in case that $k_j = k_l$ and $|C_j| = |C_l|$, for some $1 \leq j < l \leq m$. The secret S is chosen as $S = \sum_{j=0}^{m} s_j$, where $\beta_j < s_j < \alpha_j$. The components of the shares will be chosen as

$$g_i = s_0 \bmod p_{0,i},$$

$$c_i = s_{c(i)} \bmod p_{c(i),i},$$

where $c(i)$ is the unique element j, $1 \leq j \leq m$, such that $i \in C_j$, for all $1 \leq i \leq n$. Example 3.4 illustrates this scheme.

Example 3.4 (with artificially small parameters)
Let us consider $n = 6$, $\mathcal{C} = \{\{1, 2, 3\}, \{4, 5, 6\}\}$, the compartment thresholds $k_1 = 2$, $k_2 = 2$ and the global threshold $k_0 = 5$. The sequence 5, 7, 11, 13, 17, 19 is a $(5, 6)$-Mignotte sequence, with $\alpha_0 = 85085$ and $\beta_0 = 46189$, and the sequence 7, 11, 13 is a $(2, 3)$-Mignotte sequence with $\alpha_1 = \alpha_2 = 77$ and $\beta_1 = \beta_2 = 13$. We choose $s_0 = 50000$, $s_1 = 30$, and $s_2 = 40$. The secret is $S = 50070$ and the corresponding shares are $I_1 = (0, 2)$, $I_2 = (6, 8)$, $I_3 = (5, 4)$, $I_4 = (2, 5)$, $I_5 = (3, 7)$, and $I_6 = (11, 1)$.

Having the shares $I_1 = (0, 2)$, $I_2 = (6, 8)$, $I_4 = (2, 5)$, $I_5 = (3, 7)$, and $I_6 = (11, 1)$, we solve the systems

$$\begin{cases} x \equiv 0 \ mod \ 5 \\ x \equiv 6 \ mod \ 7 \\ x \equiv 2 \ mod \ 13 \\ x \equiv 3 \ mod \ 17 \\ x \equiv 11 \ mod \ 19 \end{cases},$$

$$\begin{cases} x \equiv 2 \ mod \ 7 \\ x \equiv 8 \ mod \ 11 \end{cases},$$

$$\begin{cases} x \equiv 7 \ mod \ 11 \\ x \equiv 1 \ mod \ 13 \end{cases},$$

and obtain, respectively, $s_0 = 50000$, $s_1 = 30$, $s_2 = 40$, and finally $S = 50070$.

Let us analyze the security of the scheme. Let B be an unauthorized group and consider $\Delta_B = \{j \in \{0, 1, \ldots, m\} | \ |A \cap C_j| < k_j\}$. The informations obtained from the shares corresponding to B lead to a set of possible vectors $(s_0, s_1, \ldots, s_m)$ of cardinality at least $\prod_{j \in \Delta_B} \frac{\alpha_j - \beta_j}{\beta_j}$. The generalized Mignotte sequences can be thus generated accordingly to the unauthorized access structure in order to obtain a suitable security level.

Although the shares of our scheme have two components, by using Mignotte's scheme as a building block, the sizes of shares can be smaller than the size of the secret. Further improvements can be obtained by choosing the Mignotte sequences and the values $s_0, s_1, \ldots, s_m$ such that the global components of some shares coincide with the corresponding compartment ones, i.e., $g_i = c_i$, for some $i \in \{1, 2, \ldots, n\}$. In this case we can define the share I_i as $I_i = g_i = c_i$. For this, we can generate first $s_1, \ldots, s_m$ and $c_1, \ldots, c_n$ and determining s_0 by solving the system of equations

$$\begin{cases} x \equiv c_1 \ mod \ p_{0,1} \\ \quad \vdots \\ x \equiv c_{k_0} \ mod \ p_{0,k_0} \end{cases}.$$

We will choose $I_i = g_i = c_i$, for all $1 \leq i \leq k_0$, $g_i = s_0 \ \texttt{mod} \ p_{0,i}$ and $I_i = (g_i, c_i)$, for all $k_0 + 1 \leq i \leq n$. Further improvements can be obtained in case that $s_0 \ \texttt{mod} \ p_{0,i} = s_{c(i)} \ \texttt{mod} \ p_{c(i),i}$, for some $k_0 + 1 \leq i \leq n$.

Example 3.5 illustrates the reduction of the shares.

Example 3.5 (with artificially small parameters)
Let us reconsider Example 3.4. We choose $s_1 = 30$ and $s_2 = 40$. We obtain $c_1 = 2$, $c_2 = 8$, $c_3 = 4$, $c_4 = 5$, $c_5 = 7$, and $c_6 = 1$. The system

$$\begin{cases} x \equiv 2 \ mod \ 5 \\ x \equiv 8 \ mod \ 7 \\ x \equiv 4 \ mod \ 11 \\ x \equiv 5 \ mod \ 13 \\ x \equiv 7 \ mod \ 17 \end{cases}$$

has the solution $s_0 = 32817$. The secret will be $S = 32887$ and the shares $I_1 = 2$, $I_2 = 8$, $I_3 = 4$, $I_4 = 5$, $I_5 = 7$, and $I_6 = (4, 1)$.

Thus, in case that k_0 is close to n, real improvements related to the size of shares can be made. However, every compression of a share, i.e., any equalization of form $g_i = c_i$, can affect the security with a factor of $\frac{\alpha_{c(i)} - \beta_{c(i)}}{\beta_{c(i)}}$. Thus, depending of the intended application, a compromise between the size of the shares and the level of security must be made.

4 More General Secret Sharing Based on the Chinese Remainder Theorem

In this section we extend the threshold secret sharing schemes based on the Chinese remainder theorem in order to deal with more general access structures. For this, we will generalize the threshold Mignotte and Asmuth-Bloom sequences in a natural manner, the rest of these secret sharing schemes remaining unaffected.

We begin with extending Mignotte sequences.

Definition 4.1 Let n be a positive integer, $n \geq 2$ and $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. An *$\mathcal{A}$-Mignotte sequence* is a sequence of positive integers $p_1, \ldots, p_n$ such that

$$\beta = max_{B \in \overline{\mathcal{A}}}([\{p_i | i \in B\}]) < min_{A \in \mathcal{A}}([\{p_i | i \in A\}]) = \alpha.$$

The above property is equivalent with

$$max_{B \in \overline{\mathcal{A}}_{max}}([\{p_i | i \in B\}]) < min_{A \in \mathcal{A}_{min}}([\{p_i | i \in A\}]).$$

If $\mathcal{A}$ is specified by $\mathcal{A}_{min} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid |A| = k\}$ then any $\mathcal{A}$-Mignotte sequence is a generalized threshold (k, n)-Mignotte sequence in sense of Definition 2.3. It is easy to see that if we multiply the elements of an $\mathcal{A}$-Mignotte sequence $p_1, \cdots, p_n$ with a fixed element $\delta \in \mathbb{Z}$, $(\delta, p_1 \cdots p_n) = 1$, we also obtain an $\mathcal{A}$-Mignotte sequence.

We will describe next how to construct Mignotte sequences in case of the weighted threshold access structures.

In a *weighted threshold* secret sharing scheme, a positive weight is associated to each user and the secret can be reconstructed if and only if the sum of the weights of all participants is greater than or equal to a fixed threshold. Such schemes have been considered for the first time by Shamir [29]. Shamir has discussed the case of sharing a secret between the executives of a company such that the secret can be recovered by any three executives, or by any executive and any vice-president, or by the president alone. The Shamir's solution for this case is based on a threshold secret sharing scheme with the threshold 3. Thus, the president receives three shares, each vice-president receives two shares and, finally, every simple executive receives a single share.

The weighted threshold access structures can be introduced as follows.

Definition 4.2 Let $n \geq 2$, $\omega = (\omega_1, \ldots, \omega_n)$ a sequence of positive integers, and w

a positive integer such that $2 \leq w \leq \sum_{i=1}^{n} \omega_i$. The access structure

$$\mathcal{A} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid \sum_{i \in A} \omega_i \geq w\}$$

will be referred to as the (ω, w, n)-*weighted threshold access structure.*

In this case, any $\mathcal{A}$-secret sharing scheme will be referred to as an (ω, w, n)-*weighted threshold secret sharing scheme.* The parameters $\omega_1, \ldots, \omega_n$ will be referred to as the *weights* and w will be referred to as the *threshold* of the scheme.

An (k, n)-threshold secret sharing scheme is nothing else than an (ω, w, n)-weighted threshold secret sharing scheme with $\omega_1 = \cdots = \omega_n = 1$ and $w = k$.

In case that $\mathcal{A}$ is the (ω, w, n)-weighted threshold access structure, an $\mathcal{A}$-Mignotte sequence will be referred to as an (ω, w, n)-Mignotte sequence. More exactly, an (ω, w, n)-Mignotte sequence is a sequence of positive integers $p_1, \ldots, p_n$ such that

$$max_{\substack{B \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in B} \omega_i \leq w-1}} ([\{p_i | i \in B\}]) < min_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \geq w}} ([\{p_i | i \in A\}]).$$

An (ω, w, n)-Mignotte sequence can be constructed as follows (see also [18]). Let $p'_1, \ldots, p'_N$ be a generalized threshold (w, N)-Mignotte sequence, where $N = \sum_{i=1}^{n} \omega_i$ and define $p_i = [\{p'_j \mid j \in P_i\}]$, for all $1 \leq i \leq n$, where $\{P_1, \ldots, P_n\}$ is an arbitrary partition of the set $\{1, 2, \ldots, N\}$ such that $|P_i| = \omega_i$, for all $1 \leq i \leq n$. It is easy to prove that the sequence $p_1, \ldots, p_n$ is indeed an (ω, w, n)-Mignotte sequence.

Benaloh and Leichter have proven in [4] that there exist access structures that are not weighted threshold. We present next their example that proves this statement.

Example 4.3 (Benaloh and Leichter [4])
Let $n = 4$ and $\mathcal{A}_{min} = \{\{1, 2\}, \{3, 4\}\}$. Suppose that this access structure is a weighted threshold access structure with the weights ω_1, ω_2, ω_3, ω_4, and the threshold w. So, $\omega_1 + \omega_2 \geq w$ and $\omega_3 + \omega_4 \geq w$. If we sum these inequalities we obtain $\omega_1 + \omega_2 + \omega_3 + \omega_4 \geq 2w$, and, thus, we obtain that $2 \cdot max(\omega_1, \omega_2) + 2 \cdot max(\omega_3, \omega_4) \geq 2w$ which leads to $max(\omega_1, \omega_2) + max(\omega_3, \omega_4) \geq w$. Thus, one of the sets $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$ or $\{2, 4\}$ is an authorized access group!

We will present how to realize this access structure using the proposed extension of Mignotte scheme. In fact, the main problem is to find an $\mathcal{A}$-Mignotte sequence. More exactly, we are interested in finding a sequence of positive integers p_1, p_2, p_3, p_4 such that

$$max([p_1, p_3], [p_1, p_4], [p_2, p_3], [p_2, p_4]) < min([p_1, p_2], [p_3, p_4]).$$

It is interesting to remark that this access structure can not be realized using sequences of pairwise coprime numbers. Indeed, there is no $\mathcal{A}$-Mignotte sequence with pairwise coprime elements, because, otherwise, the above inequality will lead to $p_1 p_3 < p_1 p_2$ and $p_2 p_4 < p_3 p_4$ and, thus, to $p_3 < p_2$ and $p_2 < p_3$!

If q_1, q_2, q_3, q_4 are pairwise coprime, then the sequence $p_1 = q_1q_2, p_2 = q_3q_4, p_3 = q_1q_3, p_4 = q_2q_4$ is an $\mathcal{A}$-Mignotte sequence. In this case, the general variant of the Chinese remainder theorem must be used for recovering the secret.

Asmuth-Bloom sequences can be extended as follows.

Definition 4.4 Let n be a positive integer, $n \geq 2$ and $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. An *$\mathcal{A}$-Asmuth-Bloom sequence* is a sequence of positive integers $p_0, p_1, \ldots, p_n$ such that

$$p_0 \cdot max_{B \in \overline{\mathcal{A}}}([\{p_i | i \in B\}]) < min_{A \in \mathcal{A}}([\{p_i | i \in A\}]).$$

The above property is equivalent with

$$p_0 \cdot max_{B \in \overline{\mathcal{A}}_{max}}([\{p_i | i \in B\}]) < min_{A \in \mathcal{A}_{min}}([\{p_i | i \in A\}]).$$

If $\mathcal{A}$ is specified by $\mathcal{A}_{min} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid |A| = k\}$ then any $\mathcal{A}$-Asmuth-Bloom sequence is a generalized threshold (k, n)-Asmuth-Bloom sequence. It is easy to see that if we multiply the elements, excepting the first one, of an $\mathcal{A}$-Asmuth-Bloom sequence $p_0, p_1, \cdots, p_n$ with a fixed element $\delta \in \mathbb{Z}$, $(\delta, p_0 \cdots p_n) = 1$, we also obtain an $\mathcal{A}$-Asmuth-Bloom sequence.

We will describe next how to construct Asmuth-Bloom sequences in case of the weighted threshold access structures. Let $n \geq 2$, $\omega = (\omega_1, \ldots, \omega_n)$ a sequence of weights, and w a threshold. An *(ω, w, n)-Asmuth-Bloom sequence* is a sequence of positive integers $p_0, p_1, \ldots, p_n$ such that

$$p_0 \cdot max_{\substack{B \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in B} \omega_i \leq w-1}}([\{p_i | i \in B\}]) < min_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \geq w}}([\{p_i | i \in A\}]).$$

An (ω, w, n)-Asmuth-Bloom sequence can be constructed as follows. Let $p'_0, p'_1, \ldots, p'_N$ be a generalized threshold (w, N)-Asmuth-Bloom sequence, where $N = \sum_{i=1}^{n} \omega_i$ and define $p_0 = p'_0$ and $p_i = [\{p'_j \mid j \in P_i\}]$, for all $1 \leq i \leq n$, where $\{P_1, \ldots, P_n\}$ is an arbitrary partition of the set $\{1, 2, \ldots, N\}$ such that $|P_i| = \omega_i$, for all $1 \leq i \leq n$. It is easy to prove that the sequence $p_0, p_1, \ldots, p_n$ is indeed an (ω, w, n)-Asmuth-Bloom sequence.

Example 4.5 illustrates this construction.

Example 4.5 (with artificially small parameters)

Consider $n = 4$, the weights $\omega_1 = \omega_2 = 1$, $\omega_3 = \omega_4 = 2$, and the threshold $w = 3$. We obtain $N = 6$. The sequence 5, 17, 19, 23, 29, 31, 37 is a $(3, 6)$-Asmuth-Bloom sequence and, if we consider the partition $\{\{6\}, \{5\}, \{1, 4\}, \{2, 3\}\}$ of the set $\{1, 2, 3, 4, 5, 6\}$, we obtain that the sequence 5, 37, 31, $17 \cdot 29$, $19 \cdot 23$ is an $((1, 1, 2, 2), 3, 4)$-Asmuth-Bloom sequence.

The access structure given by $\mathcal{A}_{min} = \{\{1, 2\}, \{3, 4\}\}$ can not be realized using Asmuth-Bloom sequences of pairwise coprime numbers. Indeed, there is no $\mathcal{A}$-Asmuth-Bloom sequence with pairwise coprime elements, because, otherwise, the condition $p_0 \cdot max([p_1, p_3], [p_1, p_4], [p_2, p_3], [p_2, p_4]) < min([p_1, p_2], [p_3, p_4])$ will lead

to $p_0p_1p_3 < p_1p_2$ and $p_0p_2p_4 < p_3p_4$ and, thus, to $p_0p_3 < p_2$ (which implies $p_0^2p_3 < p_0p_2$), and $p_0p_2 < p_3$, which will finally lead to $p_0^2 < 1$!

If q_1, q_2, q_3, q_4 are pairwise coprime, then the sequence $p_0, p_1 = q_1q_2, p_2 = q_3q_4, p_3 = q_1q_3, p_4 = q_2q_4$ is an $\mathcal{A}$-Asmuth-Bloom sequence, for any $p_0 < min(q_1, q_2, q_3, q_4)$. Indeed, in this case, $min([p_1, p_2], [p_3, p_4]) = q_1q_2q_3q_4$ and $max([p_1, p_3], [p_1, p_4], [p_2, p_3], [p_2, p_4]) = \frac{q_1q_2q_3q_4}{q_i}$, for some $i \in \{1, 2, 3, 4\}$. In this case, the general variant of the Chinese remainder theorem must be used for recovering the secret.

4.1 Secret Sharing Homomorphisms

Benaloh has introduced the notion of secret sharing homomorphisms in [2]. We present here a slightly different version of his definition.

Definition 4.6 Let $\mathcal{S}$ and $\mathcal{S}_1, \ldots, \mathcal{S}_n$ be the set of possible secrets and, respectively, the set of possible shares corresponding to each user. Consider the binary operations $\oplus$ and $\otimes_1, \ldots, \otimes_n$ over these sets. We say that an $\mathcal{A}$-secret sharing scheme is $(\oplus, \otimes_1, \ldots, \otimes_n) - homomorphic$ if for any $S_1, S_2 \in \mathcal{S}$ with the corresponding shares $(I_1^1, \ldots, I_n^1)$, and respectively, $(I_1^2, \ldots, I_n^2)$, the shares of the secret $S_1 \oplus S_2$ are $(I_1^1 \otimes_1 I_1^2, \ldots, I_n^1 \otimes_n I_n^2)$.

Intuitively, this means that the compositions of the shares are shares of the composition of the secrets.

The extended Mignotte scheme has such properties. Let $\otimes$ be a binary operation over $\mathbb{Z}$, $\otimes \in \{+, -, \cdot\}$, and let $\otimes_m$ denote the corresponding operation modulo m, i.e., $\otimes_m$ is the binary operation over $\mathbb{Z}_m$ given by $a \otimes_m b = (a \otimes b)$ `mod` m, for any $a, b \in \mathbb{Z}_m$. If $p_1, \ldots, p_n$ is an extended Mignotte sequence and $\otimes \in \{+, -, \cdot\}$, then the corresponding secret sharing scheme is $(\otimes, \otimes_{p_1}, \ldots, \otimes_{p_n})$-partial homomorphic, in sense that, if S_1 and S_2 are some secrets such that $\beta < S_1 \otimes S_2 < \alpha$, with the corresponding shares $(I_1^1, \ldots, I_n^1)$, and respectively, $(I_1^2, \ldots, I_n^2)$, then $(I_1^1 \otimes_{p_1} I_1^2, \ldots, I_n^1 \otimes_{p_n} I_n^2)$ are the shares corresponding[3] to the secret $S_1 \otimes S_2$.

The extended Asmuth-Bloom scheme has homomorphic properties in case that the extended Asmuth-Bloom sequence has the property $p_0|p_i$, for all $1 \leq i \leq n$. In this case, the secret can be expressed as

$$\begin{aligned} S &= (\textstyle\sum_{i \in A} \gamma_i \delta_i I_i \ \texttt{mod}\ [\{p_i | i \in A\}]) \ \texttt{mod}\ p_0 \\ &= \textstyle\sum_{i \in A} \gamma_i \delta_i I_i \ \texttt{mod}\ p_0, \end{aligned}$$

for some authorized group A, where $\delta_i = \frac{[\{p_i | i \in A\}]}{p_i}$, for all $i \in A$, and γ_i, for $i \in A$, are arbitrary integers such that $\sum_{i \in A} \gamma_i \delta_i = 1$. Thus, any extended Asmuth-Bloom scheme based on a sequence with such properties is $(\otimes_{p_0}, \otimes_{p_0}, \ldots, \otimes_{p_0})$ - homomorphic, where $\otimes \in \{+, -\}$. Unfortunately, the property $p_0|p_i$ also implies

[3] This property follows directly from the properties of the congruences. More exactly, if $S_1 \equiv I_i^1 \ mod\ p_i$ and $S_2 \equiv I_i^2 \ mod\ p_i$ then $S_1 \otimes S_2 \equiv I_i^1 \otimes_{p_i} I_i^2 \ mod\ p_i$.

that

$$\begin{aligned} I_i \bmod p_0 &= ((S + \gamma \cdot p_0) \bmod p_i) \bmod p_0 \\ &= (S + \gamma \cdot p_0) \bmod p_0 \\ &= S, \end{aligned}$$

and, thus, the security of the scheme is entirely compromised. It will be interesting to find Asmuth-Bloom sequences which lead to homomorphic properties, without affecting the security of the scheme. One solution would be to find $\mathcal{A}$-Asmuth-Bloom sequences $p_0, p_1, \ldots, p_n$ such that $p_0 | [\{p_i | i \in A\}]$, for all $A \in \mathcal{A}_{min}$, but $p_0 \not| p_i$, for all $1 \leq i \leq n$.

5 An E-voting Scheme

According to [32], "an *electronic voting* (*e-voting*) system is a voting system in which the election data is recorded, stored and processed primarily as digital information". We present next the most important requirements for an e-voting scheme (the reader is referred to [16] for more details):

- *Correctness* - according to this requirement, the announced tally is identical with the real outcome of the election;
- *Privacy* - this requirement guarantees that no reasonable sized coalitions of voters or authorities may link a voter's identity to his vote;
- *Robustness* - according to this requirement, no reasonable sized coalitions of voters or authorities may affect the election;
- *Verifiability* - this requirement assures the existence of some mechanisms for auditing the election in order to verify if it has taken place properly.

We have to remark that these properties may contradict or interrelate one with another. For example, verifiability implies the existence of some proofs for the consistency of the votes but these may affect privacy. On the other hand, verifiability is a strong supporter both for the correctness and for the robustness of the scheme.

We focus only on the case of *yes/no* e-voting. We follow the approach of Benaloh [2], [3] for designing a multi-authority e-voting scheme. The novelty of our scheme is that the tallying authorities may have non-equal weights. The parties involved are the voters $V_1, \ldots, V_m$, the tallying authorities $A_1, \ldots, A_n$ and the central authority `A`. We present next the steps of our e-voting scheme.

- **Setup**
  - The central authority `A` decides on an authorized access structure $\mathcal{A}$ for the tallying authorities and generates and broadcasts an $\mathcal{A}$-Mignotte sequence $p_1, \ldots, p_n$ with a large factor $\frac{\alpha-\beta}{\beta}$;
  - The central authority `A` broadcasts the values v_{yes} and v_{no}, where $v_{yes}, v_{no} \in \{\beta + 1, \ldots, \alpha - 1\}$ are assigned to the *yes* vote and to the *no* vote;
- **Ballot Construction**

- For $1 \leq j \leq m$, the voter V_j chooses a vote mask[4] b_j, $0 < b_j < \alpha - v_j$, for his vote $v_j \in \{v_{yes}, v_{no}\}$ and forms the ballot $B_j = v_j + b_j$;
- The voter V_j securely sends the sub-ballot $B_{j,i} = B_j \texttt{ mod } p_i$ to the tallying authority A_i, for all $1 \leq j \leq m$ and for all $1 \leq i \leq n$;

• **Ballot Tallying**
- At the end of ballot construction period, the tallying authority A_i computes the partial "masked" tally $T_i = \sum_{j=1}^{m} B_{j,i} \texttt{ mod } p_i$ and securely sends it to the central authority A, for all $1 \leq i \leq n$;
- The central authority A obtains the final "masked" tally $T = \sum_{j=1}^{m} B_j$ by solving, using the general variant of the Chinese remainder theorem, the system of equations

$$\begin{cases} x \equiv T_i \ mod \ p_i, \ i \in A \end{cases}$$

for some $A \in \mathcal{A}$; for the correctness of this reasoning, any possible final "masked" tally T must satisfy $T < \alpha$ (the relation $\beta < T$ holds by the choice of the values v_{yes}, v_{no} and of the mask values). Indeed, in this case, by the fact that the extended Mignotte secret sharing scheme is $(+, +_{p_1}, \ldots, +_{p_n})$-partial homomorphic, the values $T_1, \ldots, T_n$ are the shares of the element T. In order to assure $T < \alpha$, the central authority A may impose, for example, the condition

$$m \cdot (max(v_{yes}, v_{no}) + max(b_1, \ldots, b_m)) < \alpha;$$

- At the previous step, the central authority A can also verify the consistency of the values $T_i, i \in A$, by testing if $T_i \equiv T_{i'} \ mod \ (p_i, p_{i'})$, for any $i, i' \in A$;

• **Vote Casting**
- At the end of ballot tallying period, the voter V_j securely sends b_j to the central authority A, for all $1 \leq j \leq m$;

• **Vote Counting**
- At the end of vote casting period, the central authority A computes the sum of votes $S = \sum_{j=1}^{m} v_j$ as $S = T - \sum_{j=1}^{m} b_j$;
- The numbers of *yes* and *no* votes can be obtained as the solution of the equation $v_{yes} \cdot x + v_{no} \cdot y = S$; if the values v_{yes} and v_{no} are chosen such that $m \cdot v_{yes} < v_{no}$, then this solution can be determined as

$$number\_votes\_no \ = S \texttt{ div } v_{no},$$
$$number\_votes\_yes = (S \texttt{ mod } v_{no}) \texttt{ div } v_{yes}.$$

- The central authority broadcasts $number\_votes\_yes$, $number\_votes\_no$.

Our e-voting scheme has the following properties:

- *Privacy* - in order to link a voter's identity (V_j) to his vote (v_j), at least an authorized group of tallying authorities and the central authority must collaborate.

[4] The purpose of the masks is to hide any information about the voters' choices. Moreover, the ballot construction and ballot tallying can be performed in advance.

Indeed, the ballot B_j may be reconstructed only by an authorized group of tallying authorities and the mask b_j is known only by the central authority. Thus, our scheme assures privacy against any coalition formed by a group $B \in \overline{\mathcal{A}}$ of tallying authorities and the central authority A;

- *Verifiability* - some verifications are made in the ballot tallying phase but some proofs have to be added at the voters' level. This includes the proof that a voter really chooses a vote in $\{v_{yes}, v_{no}\}$ and the proof that the sub-ballots are properly derived. For the second part, verifiable secret sharing (see [11], [25]) may be used. A non-interactive modular verifiable secret sharing scheme was proposed in [22] and we may use it for our case;
- *Robustness* - assuming that the voters' actions are performed honestly (or using verifiable secret sharing for detecting frauds), the election carries on correctly if at least a group $A \in \mathcal{A}$ of tallying authorities and the central authority A act honestly.

6 Conclusions and Future Work

We have demonstrated that the Chinese remainder theorem can be used for realizing more general access structures than the threshold ones.

We have first extended Brickell's construction for compartmented secret sharing to the case that the global threshold is strictly greater than the sum of the compartment thresholds and we have proposed using threshold secret sharing schemes based on the Chinese remainder theorem as building blocks in order to decrease the size of shares, maintaining, in the same time, a reasonable level of security.

We have then extended the threshold secret sharing schemes based on the Chinese remainder theorem in order to deal with more general access structures. We have presented how to realize any weighted threshold access structure but we have also proven that our extensions are suitable for realizing some non-weighted threshold access structures. In our future work, we will investigate what other classes of access structures can be realized using our schemes and we will also study the related problem of generating Mignotte or Asmuth-Bloom sequences. It is interesting to remark that some access structures can not be realized using sequences of pairwise coprime numbers and, thus, the general variant of the Chinese remainder theorem must be used for recovering the secret. The access structure given by $\mathcal{A}_{min} = \{\{1,2\},\{3,4\}\}$ is such an example (see Section 4). It will be interesting to find other access structures with the same property or even find a general criterion for deciding if a certain access structure may be realized using the standard variant of the Chinese remainder theorem.

We have presented a multi-authority e-voting scheme based on the proposed secret sharing schemes, in which, as a novelty, the tallying authorities may have non-equal weights. The resulted e-voting scheme has some important properties as privacy and robustness. Some verifiability mechanisms are present in the ballot tallying phase but in our future work we will try to add proofs of consistency at voters' level and at the central authority level (following, for example, the approach

described in [9]).

Threshold cryptography in which the implicated parties may have non-equal weights is another promising future research direction and we think that our secret sharing schemes can be used in this sense.

Acknowledgement

Research reported here was partially supported by the National University Research Council of Romania under the grant CNCSIS 632/2006.

References

[1] Asmuth, C. A. and J. Bloom, *A modular approach to key safeguarding*, IEEE Transactions on Information Theory **IT-29** (1983), pp. 208–210.

[2] Benaloh, J., *Secret sharing homomorphisms: Keeping shares of a secret secret*, in: A. M. Odlyzko, editor, *Advanced in Cryptology-CRYPTO' 86*, Lecture Notes in Computer Science **263** (1987), pp. 251–260.

[3] Benaloh, J., "Verifiable Secret-Ballot Elections," Ph.D. thesis, Yale University (1988).

[4] Benaloh, J. and J. Leichter, *Generalized secret sharing and monotone functions*, in: S. Goldwasser, editor, *Advanced in Cryptology-CRYPTO' 88*, Lecture Notes in Computer Science **403** (1989), pp. 27–35.

[5] Blakley, G. R., *Safeguarding cryptographic keys*, in: *National Computer Conference, 1979*, American Federation of Information Processing Societies Proceedings **48**, 1979, pp. 313–317.

[6] Brickell, E. F., *Some ideal secret sharing schemes.*, in: J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89*, Lecture Notes in Computer Science **434** (1990), pp. 468–475.

[7] Capocelli, R. M., A. D. Santis, L. Gargano and U. Vaccaro, *On the size of shares for secret sharing schemes*, Journal of Cryptology **6** (1993), pp. 157–167, (a preliminary version of this paper appeared in Advances in Cryptology - CRYPTO '91).

[8] Cohen, H., "A Course in Computational Algebraic Number Theory," Graduate Texts in Mathematics, Springer-Verlag, 2000, 4th edition.

[9] Cramer, R., M. K. Franklin, B. Schoenmakers and M. Yung, *Multi-authority secret-ballot elections with linear work*, in: U. Maurer, editor, *Advances in Cryptology - EuroCrypt '96*, Lecture Notes in Computer Science **1070** (1996), pp. 72–83.

[10] Ding, C., D. Pei and A. Salomaa, "Chinese remainder theorem: applications in computing, coding, cryptography," World Scientific Publishing Co., Inc., 1996.

[11] Feldman, P., *A practical scheme for non-interactive verifiable secret sharing*, in: *Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science, 1987* (1987), pp. 427–437.

[12] Fraenkel, A. S., *New proof of the generalized Chinese remainder theorem*, Proceedings of American Mathematical Society **14** (1963), pp. 790–791.

[13] Garner, H., *The residue number system*, IRE Transactions on Electronic Computers **EC-8** (1959), pp. 140–147.

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

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

[16] Gritzalis, D., editor, "Secure Electronic Voting," Advances in Information Security **7**, Kluwer Academic Publishers, 2003.

[17] Iftene, S., *A generalization of Mignotte's secret sharing scheme*, in: T. Jebelean, V. Negru, D. Petcu and D. Zaharie, editors, *Proceedings of the 6th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September, 2004* (2004), pp. 196–201.

[18] Iftene, S. and I. Boureanu, *Weighted threshold secret sharing based on the Chinese remainder theorem*, Scientific Annals of the "Al. I. Cuza" University of Iasi, Computer Science Section **XVI** (2005), pp. 161–172.

[19] Ito, M., A. Saito and T. Nishizeki, *Secret sharing scheme realizing general access structure*, in: *Proceedings of the IEEE Global Telecommunications Conference, Globecom '87* (1987), pp. 99–102.

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

[21] Kranakis, E., "Primality and Cryptography," Wiley-Teubner Series in Computer Science, 1986.

[22] Li, Q., Z. Wang, X. Niu and S. Sun, *A non-interactive modular verifiable secret sharing scheme*, in: *ICCCAS'05, International Conference on Communications, Circuits and Systems, 2005*, 2005, pp. 84–87.

[23] Mignotte, M., *How to share a secret*, in: T. Beth, editor, *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982*, Lecture Notes in Computer Science **149** (1983), pp. 371–375.

[24] Ore, O., *The general Chinese remainder theorem*, American Mathematical Monthly **59** (1952), pp. 365–370.

[25] Pedersen, T. P., *Non-interactive and information-theoretic secure verifiable secret sharing*, in: J. Feigenbaum, editor, *Advances in Cryptology - Crypto '91*, Lecture Notes in Computer Science **576** (1992), pp. 129–140.

[26] Pohlig, S. C. and M. E. Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Transactions on Information Theory **24** (1978), pp. 106–110.

[27] Quisquater, J.-J. and C. Couvreur, *Fast decipherment algorithm for the RSA public-key cryptosystem*, IEE Electronics Letters **18 (21)** (1982), pp. 905–907.

[28] Quisquater, M., B. Preneel and J. Vandewalle, *On the security of the threshold scheme based on the Chinese remainder theorem*, in: D. Naccache and P. Paillier, editors, *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002*, Lecture Notes in Computer Science **2274** (2002), pp. 199–210.

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

[30] Simmons, G. J., *How to (really) share a secret.*, in: S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88*, Lecture Notes in Computer Science **403** (1990), pp. 390–448.

[31] Stinson, D. R., *An explication of secret sharing schemes*, Designs, Codes and Cryptography **2** (1992), pp. 357–390.

[32] VoteHere, *Network voting system standards* (April 2002).