General Secret Sharing Based on the Chinese Remainder Theorem

Sorin Iftene

Faculty of Computer Science
"Al. I. Cuza" University
Iaşi, Romania
siftene@infoiasi.ro

Abstract. In this paper we extend the threshold secret sharing schemes based on the Chinese remainder theorem in order to deal with more general access structures. Aspects like verifiability, secret sharing homomorphisms and multiplicative properties are also discussed.

AMS Subject Classification: 94A62, 11A07
Keywords and phrases: secret sharing, general access structure, Chinese remainder theorem

1 Introduction and Preliminaries

A secret sharing scheme starts with a *secret* and then derives from it certain *shares* (*shadows*). The secret may be recovered only in the case of possessing a certain predetermined set of shares. The initial applications of secret sharing were safeguarding cryptographic keys and providing shared access to strategical resources. Threshold cryptography (see, for example, [10]) and some e-voting schemes (see, for example, [9]) are more recent applications of the secret sharing schemes.

In the first secret sharing schemes only the cardinality of the sets of shares was important for recovering the secret. Such schemes have been referred to as *threshold* secret sharing schemes. We mention Shamir's threshold secret sharing scheme [30] based on polynomial interpolation, Blakley's geometric threshold secret sharing scheme [5], Mignotte's threshold secret sharing scheme [22] and Asmuth-Bloom threshold secret sharing scheme [1], both based on the Chinese remainder theorem. Ito, Saito, and Nishizeki [21], Benaloh and Leichter [3] give constructions for more general secret sharing schemes.

This paper extends the threshold schemes based on the Chinese remainder theorem in order to address more general access structures and presents some interesting capabilities of these schemes like verifiability, secret sharing homomorphisms and multiplicative properties.

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, and secret sharing schemes. We survey the threshold secret sharing schemes based on the Chinese remainder theorem in Section 2 and the general secret sharing techniques in

Section 3. In Section 4 we extend the threshold secret schemes based on the Chinese remainder theorem to more general access structures. In the next section we discuss aspects like verifiability, secret sharing homomorphisms, and multiplicative properties of our schemes. Our conclusions are presented in the last section.

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

Let $a, b \in \mathbf{Z}$, $b \neq 0$. The *quotient* of integer division of a by b will be denoted by $a \texttt{ div } b$ and the *remainder* will be denoted by $a \texttt{ mod } b$. In the case $a \texttt{ mod } b = 0$ we will say that b is a *divisor* of a and denote this by $b|a$.

Let $a_1, \ldots, a_n \in \mathbf{Z}$, $a_1^2 + \cdots + a_n^2 \neq 0$. 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 $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ that satisfy $\alpha_1 a_1 + \cdots + \alpha_n a_n = (a_1, \ldots, a_n)$ (the linear form of the *gcd*).

Let $a_1, \ldots, a_n \in \mathbf{Z}$ such that $a_1 \cdots a_n \neq 0$. The *least common multiple* (*lcm*) of $a_1, \ldots, a_n$ will be denoted by $[a_1, \ldots, a_n]$. For a given sequence of integers $m_1, \ldots, m_n$ and for a set $A \in \mathcal{P}(\{1, \ldots, n\})$[1], the least common multiple of the elements m_i, for $i \in A$, will be also denoted by $[A]$.

$\mathbf{Z}_m$ is the set $\{0, 1, \ldots, m-1\}$, $\mathbf{Z}_m^*$ stands for the set $\{a \in \mathbf{Z}_m | (a, m) = 1\}$ and $\phi(m)$ denotes the cardinality of the set $\mathbf{Z}_m^*$, for all $m \geq 2$.

Let $a, b, m \in \mathbf{Z}$. We say that *a and b are congruent modulo m*, and we use the notation $a \equiv b \ mod \ m$, if $m|(a - b)$. It is easy to see that $a \texttt{ mod } b \equiv a \ mod \ m$, for any $a, b, m \in \mathbf{Z}$ such that $m|b$.

For an element $a \in \mathbf{Z}_m^*$, the *order of a modulo m*, i.e., the least non-zero positive integer k such that $a^k \equiv 1 \ mod \ m$ will be denoted by $ord_m(a)$. It is well-known that the relation $a^i \equiv a^j \ mod \ m$ is equivalent with $i \equiv j \ mod \ ord_m(a)$, for any integers i and j. A *primitive root* modulo m is an element $a \in \mathbf{Z}_m^*$ such that $ord_m(a) = \phi(m)$.

The Chinese remainder theorem has many applications in computer science (see, for example, [13]). 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 the Mignotte's threshold secret sharing scheme [22] or in its generalization [19], or in the 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. *Let $k \geq 2$, $m_1, \ldots, m_k \geq 2$, and $b_1, \ldots, b_k \in \mathbf{Z}$. The system of equations*

$$\begin{cases} x \equiv b_1 \ mod \ m_1 \\ \quad \vdots \\ x \equiv b_k \ mod \ m_k \end{cases}$$

has solutions in $\mathbf{Z}$ if and only if $b_i \equiv b_j \ mod \ (m_i, m_j)$ for all $1 \leq i, j \leq k$. Moreover, if the above system of equations has solutions in $\mathbf{Z}$, then it has an unique solution in $\mathbf{Z}_{[m_1, \ldots, m_k]}$.

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

When $(m_i, m_j) = 1$, for all $1 \leq i < j \leq k$, one gets the *standard* version of the Chinese remainder theorem. Garner [17] found an efficient algorithm for this case and Fraenkel [16] extended it to the general case.

We present next some basic facts about secret sharing schemes. Let n be an integer, $n \geq 2$ and $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. Informally, an $\mathcal{A}$-*secret sharing scheme* is a method of generating $(S, (I_1, \ldots, I_n))$ such that

- for any $A \in \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$ is "easy";
- 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 access sets* of the scheme.
A natural[2] condition is that an access structure $\mathcal{A}$ is *monotone*, 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 access sets, 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 access sets, 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 our paper we consider only monotone access structures $\mathcal{A}$ that also satisfy the condition $(\forall i \in \{1, 2, \ldots, n\})(\exists A \in \mathcal{A}_{min} : i \in A)$ because, in case there is an i such that the mentioned property does not hold, we may consider the set $\{1, 2, \ldots, n\} \setminus \{i\}$. In this case, n will be referred to as the *size* of the access structure.

An important particular class of secret sharing schemes is that of the *threshold* secret sharing schemes. In these schemes, only the cardinality of the sets of shares is important for recovering the secret. More exactly, if the required threshold is k, $1 \leq k \leq n$, the minimal access structure is $\mathcal{A}_{min} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid |A| = k\}$. In this case, an $\mathcal{A}$-secret sharing scheme will be referred to as a (k, n)-*threshold secret sharing scheme*.

2 Threshold Secret Sharing Schemes Based on the Chinese Remainder Theorem

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

[2] There are papers (see, for example, [4] or [6]) that consider non-monotone access structures. More exactly, in these schemes, there are positive and negative shares which lead to veto capabilities. As Obana and Kurosawa have remarked in [23], the simplest solution for the veto feature is that the opposing participants give a special "veto" share in the secret reconstruction phase, leading to an incorrect secret.

2.1 Mignotte's Threshold Secret Sharing scheme

Mignotte's threshold secret sharing scheme [22] uses special sequences of integers, referred to as the *Mignotte sequences.*

Definition 1. Let n be an integer, $n \geq 2$, and $2 \leq k \leq n$. An (k,n)-*Mignotte sequence* is a sequence of positive integers $m_1 < \cdots < m_n$ such that $(m_i, m_j) = 1$, for all $1 \leq i < j \leq n$, and $m_{n-k+2} \cdots m_n < m_1 \cdots m_k$.

Given an (k,n)-Mignotte sequence, the scheme works as follows:

- The secret S is chosen as a random integer such that $\beta < S < \alpha$, where $\alpha = m_1 \cdots m_k$ and $\beta = m_{n-k+2} \cdots m_n$;
- The shares I_i are chosen by $I_i = S \texttt{ mod } m_i$, 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 Chinese remainder theorem, as the unique solution modulo $m_{i_1} \cdots m_{i_k}$ of the system

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

A generalization of Mignotte's scheme by allowing modules that are not necessarily pairwise coprime was proposed in [19], by introducing *generalized Mignotte sequences.*

Definition 2. Let n be an integer, $n \geq 2$, and $2 \leq k \leq n$. A *generalized* (k,n)-*Mignotte sequence* is a sequence $m_1, \ldots, m_n$ of positive integers such that

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

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 an (k,n)-Mignotte sequence by a fixed element $\delta \in \mathbf{Z}$, $(\delta, m_1 \cdots m_n) = 1$, we obtain a generalized (k,n)-Mignotte sequence. Generalized Mignotte's scheme works like Mignotte's scheme, with $\alpha = min_{1 \leq i_1 < \cdots < i_k \leq n}([\{i_1, \ldots, i_k\}])$ and $\beta = max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}([\{i_1, \ldots, i_{k-1}\}])$. Moreover, in this case, the general 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], uses special sequences of integers. More exactly, a sequence of pairwise coprime positive integers $r, m_1 < \cdots < m_n$ is chosen such that $r \cdot m_{n-k+2} \cdots m_n < m_1 \cdots m_k$.

Given such a sequence, the scheme works as follows:

- The secret S is chosen as a random element of the set $\mathbf{Z}_r$;
- The shares I_i are chosen by $I_i = (S + \gamma \cdot r) \texttt{ mod } m_i$, for all $1 \leq i \leq n$, where γ is an arbitrary integer such that $S + \gamma \cdot r \in \mathbf{Z}_{m_1 \cdots m_k}$;
- Given k distinct shares $I_{i_1}, \ldots, I_{i_k}$, the secret S can be obtained as $S = x_0 \texttt{ mod } r$, where x_0 is obtained, using the standard Chinese remainder theorem, as the unique solution modulo $m_{i_1} \cdots m_{i_k}$ of the system

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

The sequences used in the Asmuth-Bloom scheme can be generalized by allowing modules that are not necessarily pairwise coprime in an obvious manner. We can use any sequence $r, m_1, \cdots, m_n$ such that

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

It is easy to see that if we multiply every element of an ordinary Asmuth-Bloom sequence excepting r with a fixed element $\delta \in \mathbf{Z}$, $(\delta, m_1 \cdots m_n) = 1$, we obtain a generalized Asmuth-Bloom sequence.

The application of the Chinese remainder theorem in threshold secret sharing has been also discussed in [18] and a unitary point of view on the security of the threshold secret sharing schemes based on the Chinese remainder theorem was presented in [28]. Although the threshold secret sharing schemes based on the Chinese remainder theorem are not perfect[3], by choosing carefully the parameters, these schemes can lead to a reasonable factor $\frac{\text{security}}{\text{size of shares}}$.

3 General Secret Sharing Schemes

There are situations which require more complex access structures than the threshold ones. Shamir [30] 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. This is an example of the so-called *hierarchical* secret sharing schemes. The Shamir's solution for this case is based on an ordinary $(3, m)$-threshold secret sharing scheme. Thus, the president receives three shares, each vice-president receives two shares and, finally, every simple executive receives a single share.

The above idea leads to the so-called *weighted* (or *multiple shares based*) threshold secret sharing schemes. In these schemes, the shares are pairwise disjoint[4] sets of

[3] In a *perfect* secret sharing scheme, the shares of any unauthorized group give no information (in information-theoretical sense) about the secret.

[4] In the sense that, if the shadows of the used threshold secret sharing scheme are $s_1, \ldots, s_m$ and the shadows of the weighted threshold secret sharing scheme are $I_i = \{s_j | j \in M_i\}$, for some $M_i \subseteq \{1, 2, \ldots, m\}$, $1 \leq i \leq n$, then $M_j \cap M_l = \emptyset$ for all $1 \leq j \neq l \leq n$.

shares provided by an ordinary threshold secret sharing scheme. Benaloh and Leichter have proven in [3] that there are access structures that can not be realized using such schemes. We present next their example that proves this.

Example 1. Let $n = 4$ and $\mathcal{A}_{min} = \{\{1,2\},\{3,4\}\}$. Suppose that this access structure can be realized using a weighted threshold secret sharing scheme based on an ordinary threshold secret sharing scheme with threshold k, and let a, b, c and, respectively, d be the numbers of shares used. So, $a+b \geq k$ and $c+d \geq k$. If we sum these inequalities we obtain $a+b+c+d \geq 2k$, and, further, $2 \cdot max(a,b) + 2 \cdot max(c,d) \geq 2k$ which leads to $max(a,b)+max(c,d) \geq k$. Thus, one of the sets $\{1,3\}$, $\{1,4\}$, $\{2,3\}$ or $\{2,4\}$ is an authorized access set!

We present next the most important general secret sharing techniques.

3.1 Ito-Saito-Nishizeki Scheme

Ito, Saito, and Nishizeki [21] have introduced the so-called *cumulative array* technique for monotone access structures.

Definition 3. Let $\mathcal{A}$ be a monotone authorized access structure of size n and let $B_1, \ldots, B_m$ be the corresponding maximal unauthorized access sets. The *cumulative array* for the access structure $\mathcal{A}$, denoted by $\mathcal{C}^{\mathcal{A}}$, is the $n \times m$ matrix, $\mathcal{C}^{\mathcal{A}} = (\mathcal{C}^{\mathcal{A}}_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ where

$$\mathcal{C}^{\mathcal{A}}_{i,j} = \begin{cases} 0, & \text{if } i \in B_j \\ 1, & \text{if } i \notin B_j \end{cases}$$

for all $1 \leq i \leq n$ and $1 \leq j \leq m$.

Let consider now an arbitrary (m,m)-threshold secret sharing scheme with the secret S and the corresponding shadows $s_1, \ldots, s_m$. In the $\mathcal{A}$-secret sharing scheme, the shadows $I_1, \ldots, I_n$ corresponding to the secret S will be defined as

$$I_i = \{s_j | \mathcal{C}^{\mathcal{A}}_{i,j} = 1\},$$

for all $1 \leq i \leq n$.

Example 2. Let $n = 4$ and $\mathcal{A}_{min} = \{\{1,2\},\{3,4\}\}$. In this case, we obtain that $\overline{\mathcal{A}}_{max} = \{\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$ and $m = 4$. The cumulative array for the access structure $\mathcal{A}$ is $\mathcal{C}^{\mathcal{A}} = \left(\begin{smallmatrix} 0&0&1&1 \\ 1&1&0&0 \\ 0&1&0&1 \\ 1&0&1&0 \end{smallmatrix}\right)$. In this case, $I_1 = \{s_3, s_4\}$, $I_2 = \{s_1, s_2\}$, $I_3 = \{s_2, s_4\}$ and $I_4 = \{s_1, s_3\}$, where s_1, s_2, s_3, s_4 are the shadows of a $(4,4)$-threshold secret sharing scheme with the secret S.

3.2 Benaloh-Leichter Scheme

Benaloh and Leichter [3] have represented the access structures using formulae. More exactly, for a monotone authorized access structure $\mathcal{A}$ of size n, they defined the set $\mathcal{F}_{\mathcal{A}}$ as the set of formulae on a set of variables $\{v_1, v_2, \ldots, v_n\}$ such that for every $F \in \mathcal{F}_{\mathcal{A}}$, the interpretation of F with respect to an assignation of the variables is *true* if and only if the true variables correspond to a set $A \in \mathcal{A}$. They have remarked that such formulae can be used as templates for describing how a secret can be shared with respect to the given access structure. Because the formulae can be expressed using only $\wedge$ operators and $\vee$ operators, it is sufficient to indicate how to "split" the secret across these operators.

Thus, we can inductively define the shares of a secret S with respect to a formulae F as follows

$$Shares(S,F) = \begin{cases} (S,i), & \text{if } F = v_i,\ 1 \leq i \leq n; \\ \cup_{i=1}^{k} Shares(S,F_i), & \text{if } F = F_1 \vee F_2 \vee \cdots \vee F_k; \\ \cup_{i=1}^{k} Shares(s_i,F_i), & \text{if } F = F_1 \wedge F_2 \wedge \cdots \wedge F_k, \end{cases}$$

where, for the case $F = F_1 \wedge F_2 \wedge \cdots \wedge F_k$, we can use any (k,k)-threshold secret sharing scheme for deriving some shares $s_1, \ldots, s_k$ corresponding to the secret S and, finally, the shares as $I_i = \{s | (s,i) \in Shares(S,F)\}$, for all $1 \leq i \leq n$, where F is an arbitrary formula in the set $\mathcal{F}_{\mathcal{A}}$.

Example 3. Let $n = 3$ and an authorized access structure $\mathcal{A}$ given by $\mathcal{A}_{min} = \{\{1,2\},\{2,3\}\}$. For example, the formula

$$F = (v_1 \wedge v_2) \vee (v_2 \wedge v_3)$$

is in the set $\mathcal{F}_{\mathcal{A}}$. In this case $Shares(S,F)$, for some secret S, can be obtained as

$$\begin{aligned} Shares(S,F) &= Shares(S, v_1 \wedge v_2) \cup Shares(S, v_2 \wedge v_3) \\ &= Shares(s_1, v_1) \cup Shares(s_{2,1}, v_2) \cup Shares(s_{2,2}, v_2) \cup Shares(s_3, v_3) \\ &= \{(s_1,1),(s_{2,1},2),(s_{2,2},2),(s_3,3)\}, \end{aligned}$$

where $s_1, s_{2,1}$ and, respectively, $s_{2,2}, s_3$ are shadows of the secret S with respect to two arbitrary $(2,2)$-threshold secret schemes. Thus, the shares corresponding to the secret S with respect to the access structure $\mathcal{A}$ are $I_1 = \{s_1\}$, $I_2 = \{s_{2,1}, s_{2,2}\}$ and $I_2 = \{s_3\}$.

Remark 1. A shadow I_i may contain many sub-shadows, one sub-shadow for every minimal access set to which i belongs. Thus, an ordering of these sub-shadows is required in order to select the correct sub-shadow corresponding to a certain access set in the reconstruction phase.

Remark 2. Benaloh and Leichter also proposed using general $\texttt{threshold}_{\texttt{k,m}}$ operators[5] in order to construct smaller formulae, reducing in this way the size of the shadows. In this case, the definition of $Shares(S, F)$ can be extended for these operators as follows:

$$Shares(S, F) = \cup_{i=1}^{m} Shares(s_i, F_i),$$

if $F = \texttt{threshold}_{k,m}(F_1, \ldots, F_m)$, where $s_1, \ldots, s_m$ are the shadows corresponding to the secret S with respect to an arbitrary (k, m)-threshold secret sharing scheme.

Example 4. Let $n = 4$ and a monotone authorized access structure $\mathcal{A}$ given by $\mathcal{A}_{min} = \{\{2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}\}$. For example, the formula

$$F = (v_2 \wedge v_3) \vee (v_1 \wedge v_2 \wedge v_4) \vee (v_1 \wedge v_3 \wedge v_4)$$

is in the set $\mathcal{F}_{\mathcal{A}}$. Using the $\texttt{threshold}$ operator, we can obtain a shorter formula, namely, $(v_2 \wedge v_3) \vee \texttt{threshold}_{3,4}(v_1, v_2, v_3, v_4)$.

4 General Secret Sharing Based on the Chinese Remainder Theorem

We indicate how we can extend the threshold secret schemes based on the Chinese remainder theorem to more general access structures. For simplicity, we only deal with the Mignotte's scheme, but we must mention that this extension technique can be also applied to Asmuth-Bloom scheme. We first extend the (generalized) threshold Mignotte sequences in a natural manner.

Definition 4. Let n be a positive integer, $n \geq 2$ and $\mathcal{A}$ an authorized access structure. An *$\mathcal{A}$-Mignotte sequence* is a sequence $m_1, \ldots, m_n$ of positive integers such that

$$max_{A \in \overline{\mathcal{A}}}([A]) < min_{A \in \mathcal{A}}([A])$$

Remark 3. The above property is equivalent with

$$max_{A \in \overline{\mathcal{A}}_{max}}([A]) < min_{A \in \mathcal{A}_{min}}([A])$$

Remark 4. 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 (k, n)-Mignotte sequence in sense of Definition 2. Moreover, for the same access structure, any ordered $\mathcal{A}$-Mignotte sequence with pairwise coprime elements is a (k, n)-Mignotte sequence in sense of Definition 1.

[5] For $m \geq 1$, $1 \leq k \leq m$, $\texttt{threshold}_{k,m}(F_1, \ldots, F_m)$ denotes the formula

$$\bigvee_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} (\bigwedge_{j=1}^{k} F_{i_j})$$

Thus, $F_1 \vee F_2 \vee \cdots \vee F_m = \texttt{threshold}_{1,m}(F_1, \ldots, F_m)$ and $F_1 \wedge F_2 \wedge \cdots \wedge F_m = \texttt{threshold}_{m,m}(F_1, \ldots, F_m)$.

Example 5. Let $\mathcal{A} = \{\{1\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. In this case we have that $\mathcal{A}_{min} = \{\{1\}, \{2,3\}\}$, $\overline{\mathcal{A}} = \{\emptyset, \{2\}, \{3\}\}$ and $\overline{\mathcal{A}}_{max} = \{\{2\}, \{3\}\}$. The sequence $18, 3, 5$ is an $\mathcal{A}$-Mignotte sequence because $5 = max(\{m_2, m_3\}) < min(\{m_1, [m_2, m_3]\}) = 15$.

These sequences can be used for constructing secret sharing schemes for more general access structures in an obvious way. More exactly, having an $\mathcal{A}$-Mignotte sequence, we may construct an *$\mathcal{A}$-Mignotte secret sharing scheme* as follows:

- the secret S is an arbitrary integer in the interval $[\beta+1, \alpha-1]$, where $\alpha = min_{A\in\mathcal{A}_{min}}([A])$, $\beta = max_{A\in\overline{\mathcal{A}}_{max}}([A])$;
- the shares $I_1, \ldots, I_n$ are chosen as follows: $I_i = S \ \mathtt{mod}\ m_i$, for all $1 \leq i \leq n$.

Having a set of shares $\{I_i \mid i \in A\}$ with $A \in \mathcal{A}$, the secret S can be obtained as the unique solution modulo $[A]$ of the system of equations

$$\Big\{ x \equiv I_i \ mod\ m_i, \, i \in A$$

Indeed, the secret S is the unique solution modulo $[A]$ of the above system of equations because S is an integer solution of the system by the choice of the shares $I_1, \ldots, I_n$ and, moreover, $S \in \mathbf{Z}_{[A]}$, by the choice of the secret S ($S < \alpha$ and $\alpha = min_{A\in\mathcal{A}}([A])$).

Having a set of shares $\{I_i \mid i \in A\}$ with $A \in \overline{\mathcal{A}}$ the only information we can obtain by finding the unique solution x_0 in $\mathbf{Z}_{[A]}$ of the system of equations

$$\Big\{ x \equiv I_i \ mod\ m_i, \, i \in A$$

is that $S \equiv x_0 \ mod\ [A]$. Indeed, the secret S is not the unique solution modulo $[A]$ of the above system of equations because $S \notin \mathbf{Z}_{[A]}$, by the choice of the secret S ($S > \beta$ and $\beta = max_{A\in\overline{\mathcal{A}}}([A])$). Choosing $\mathcal{A}$-Mignotte sequences with a large factor $\frac{\alpha-\beta}{\beta}$, the problem of finding the secret S, knowing that S is in the interval $[\beta+1, \alpha-1]$ and $S \equiv x_0 \ mod\ [A]$, for some unauthorized access set A, is intractable.

Example 6. (with artificial small parameters) Let $\mathcal{A}_{min} = \{\{1\}, \{2,3\}\}$. We use the sequence from Example 5. Thus, the secret S will be generated in the interval $[5, 15]$. For example, we consider $S = 13$. The shares will be $I_1 = S \ \mathtt{mod}\ m_1 = 13$, $I_2 = S \ \mathtt{mod}\ m_2 = 1$ and $I_3 = S \ \mathtt{mod}\ m_3 = 3$. The sets $\{I_1\}$ or $\{I_2, I_3\}$ will lead to the secret S, but the set $\{I_2\}$ will lead only to $S \equiv 1 \ mod\ 3$.

Remark 5. It is interesting to see that some access structures can not be realized using sequences of pairwise coprime numbers and, thus, the general Chinese remainder theorem must be used. For example, for the access structure $\mathcal{A}$ given by $\mathcal{A}_{min} = \{\{1,2\}, \{3,4\}\}$, there is no $\mathcal{A}$-Mignotte sequence with pairwise coprime elements, because, otherwise, the condition

$$max([m_1, m_3], [m_1, m_4], [m_2, m_3], [m_2, m_4]) < min([m_1, m_2], [m_3, m_4])$$

will lead to $m_1 m_3 < m_1 m_2$ and $m_2 m_4 < m_3 m_4$ and, thus, to $m_3 < m_2$ and $m_2 < m_3$!

The sequence $6, 35, 10, 21$ is an $\mathcal{A}$-Mignotte sequence. In general, if $a, b, c, d \geq 2$ are pairwise coprime, the sequence ab, cd, ac, bd is an $\mathcal{A}$-Mignotte sequence.

5 Capabilities of the Presented Scheme

In this section we discuss some interesting aspects of the proposed scheme like verifiability, secret sharing homomorphisms and multiplicative properties. These notions have been introduced for the threshold secret sharing schemes, but they can be extended to the general case in a natural manner. Moreover, we shall also show how to use these properties in electronic voting or in threshold cryptography.

5.1 Verifiability

In practice, the secret and the shares are generated by an *administrator* (or *dealer*) which must be a mutually trusted party. Afterwards, the administrator securely distributes the shares to the users. The *verifiable secret sharing schemes* (see, for example, [7], [15], [25]) can detect, with some probability, a dishonest behavior of the administrator or of some users in the reconstructing phase. This feature is very important, for example, in e-voting protocols based on secret sharing schemes.

In our case, we shall use that, if $I_1, \ldots, I_n$ represent correct shares of a secret S, then $S \equiv I_i \ mod \ m_i$, for all $1 \leq i \leq n$. Such a congruence is equivalent with $\alpha_i^S \equiv \alpha_i^{I_i} \ mod \ p_i$, for any positive integer p_i and any element $\alpha_i \in \mathbf{Z}_{p_i}^*$ of order m_i (m_i must be a divisor of $\phi(p_i)$).

The administrator makes public the values $(p_i, \alpha_i, \alpha_{S,i})$, where $\alpha_{S,i} = \alpha_i^S \ \mathtt{mod} \ p_i$, for all $1 \leq i \leq n$, and sends securely $I_1, \ldots, I_n$ to users.

The i^{th} user, after receiving I_i, can verify that his share is correct by computing $\alpha_i^{I_i} \ \mathtt{mod} \ p_i$ and comparing the result with $\alpha_{S,i}$. Moreover, the integrity of the shares is also assured. The security of this new feature of our secret sharing scheme is based on the intractability of the discrete logarithm problem.

5.2 Secret Sharing Homomorphisms

Benaloh introduced the notion of secret sharing homomorphisms in [2].

Definition 5. Let D_{secret} and D_{shares} be the set of possible secrets and, respectively, the set of possible shares. Consider two binary operations $\oplus$ and $\otimes$ over D_{secret} and, respectively, D_{shares}. We say that an $\mathcal{A}$-secret sharing scheme is $(\oplus, \otimes)-$*homomorphic* if for any $S_1, S_2 \in D_{secret}$ with the corresponding shares $(I_1^1, \ldots, I_n^1)$, and respectively, $(I_1^2, \ldots, I_n^2)$, the shares $(I_1^1 \otimes I_1^2, \ldots, I_n^1 \otimes I_n^2)$ correspond to the secret $S_1 \oplus S_2$.

Our secret sharing scheme provides some partial secret sharing homomorphisms in the following sense. Consider $D_{secret} = \{\beta+1, \ldots, \alpha-1\}$, $D_{shares} = \mathbf{Z}$ and a binary operation $\odot \in \{+, -, \cdot\}$ over $\mathbf{Z}$. The extended Mignotte secret sharing scheme is *partially* $(\odot, \odot) -$ *homomorphic*, in the sense that, for any $S_1, S_2 \in D_{secret}$ with the corresponding shares $(I_1^1, \ldots, I_n^1)$, respectively, $(I_1^2, \ldots, I_n^2)$, the shares[6] $(I_1^1 \ \odot$

[6] In the extended Mignotte scheme, the shares are chosen as $I_i = S \ \mathtt{mod} \ m_i$, for $1 \leq i \leq n$, but any integers I_i with $I_i \equiv (S \ \mathtt{mod} \ m_i) \ mod \ m_i$, for $1 \leq i \leq n$, will work.

$I_1^2, \ldots, I_n^1 \odot I_n^2)$ correspond to the secret $S_1 \odot S_2$, providing that $S_1 \odot S_2 \in D_{secret}$. Moreover, if S is a secret with the corresponding shares $(I_1, \ldots, I_n)$ and f is a polynomial function with integer coefficients such that $f(S) \in D_{secret}$ then the shares $(f(I_1), \ldots, f(I_n))$ correspond to the secret $f(S)$. All these properties result from the corresponding properties of the congruences.

An E-voting Scheme

We propose an e-voting scheme based on these properties, following an idea from [2]. More exactly, we address to the case of *yes/no* e-voting. Any voting server deals with a group of at most m voters and each server is divided in n subservers, for some $n \geq 2$. The central voting server decides on an authorized access structure $\mathcal{A}$ of size n and generates an $\mathcal{A}$-Mignotte sequence with a large factor $\frac{\alpha-\beta}{\beta}$. A secret value $value_{yes} \in \{\beta+1, \ldots, \alpha-1\}$ is assigned to a *yes* vote and a secret value $value_{no} \in \{\beta+1, \ldots, \alpha-1\}$ is assigned to a *no* vote.

Each voter securely obtains the secret $value_{yes}$ or $value_{no}$ corresponding to his *yes* or *no* vote using any oblivious transfer technique and distributes the corresponding shares to the n subservers. Each subserver can verify the consistency of the received share using the technique described in Section 5.1. Each subserver computes the sum of the incoming shares and, at the end of voting, sends the result to the central voting server. By the partial $(+,+)$-homomorphism property of the extended Mignotte secret sharing scheme, the sums of shares are shares of the sum of the secrets. The values $value_{yes}$ and $value_{no}$ must satisfy $m \cdot max(value_{yes}, value_{no}) < \alpha$. Thus, the central voting server can obtain the final sum by using the sums of shares from any trusted authorized subservers.

Moreover, if the values $value_{yes}$ and $value_{no}$ satisfy $m \cdot value_{yes} < value_{no}$, then the correct numbers of *yes* and *no* votes can be obtained as the unique solutions of the equation $value_{yes} \cdot x + value_{no} \cdot y = final\_sum$, or, more exactly, as follows:
$number\_votes\_no = final\_sum \ \texttt{div} \ value_{no}$,
$number\_votes\_yes = (final\_sum \ \texttt{mod} \ value_{no}) \ \texttt{div} \ value_{yes}$.

5.3 Multiplicative Aspects

The *multiplicative* threshold secret sharing schemes were introduced in [11]. We present here a slight modification of the definition given in the mentioned paper.

Definition 6. Let D_{secret} be the set of possible secrets, D_{shares} be the set of possible shares and consider an associative and commutative binary operation $\odot$ over D_{secret}. We say that an $\mathcal{A}$-secret sharing scheme is *multiplicative with respect to* $\odot$ if for any set $A \in \mathcal{A}$ there is a family of public functions $(f_{(i,A)} | i \in A)$ from D_{shares} to D_{secret} such that

$$S = \odot_{i \in A} f_{(i,A)}(I_i)$$

This property of secret sharing schemes can be used in designing threshold cryptographic primitives. We show that the extended Mignotte secret sharing scheme can be used for this purpose. More exactly, we indicate how our secret sharing scheme can be combined with ElGamal decryption in order to obtain threshold decryption. Our proposal follows an idea from [12].

We shall first present the ElGamal public-key cryptosystem [14]. The public key is (p, α, β) where p is a large prime, α is a primitive root modulo p, $\beta = \alpha^a \texttt{ mod } p$ and $a \in \mathbf{Z}_{p-1}$ is the private key. A message $x \in \mathbf{Z}_p$ is encrypted by a pair (γ, δ) where $\gamma = \alpha^l \texttt{ mod } p$, $\delta = x \cdot \beta^l \texttt{ mod } p$ and $l \in \mathbf{Z}_{p-1}$ is a parameter chosen by the sender. The legal receiver can obtain the message x by computing $\gamma^{-a} \cdot \delta \texttt{ mod } p$.

The administrator decides on an authorized access structure $\mathcal{A}$ of size n, for some $n \geq 2$, and generates an $\mathcal{A}$-Mignotte sequence with a large factor $\frac{\alpha-\beta}{\beta}$ such that $\beta < a < \alpha$. The private key a will be the secret and the shares $I_1, \ldots, I_n$ will be securely distributed to the users $U_1, \ldots, U_n$. Consider now an authorized access set A. Using the Ore's construction [24] for obtaining the solution of the corresponding system of modular equations (see also [19]), the secret a can be expressed as

$$a = \sum_{i \in A} f_{(i,A)}(I_i) \texttt{ mod } [A],$$

where the function $f_{(i,A)} : \mathbf{Z} \to \mathbf{Z}$ is given by $f_{(i,A)}(x) = \lambda_{(i,A)}\mu_{(i,A)}x$ with

- $\lambda_{(i,A)} = \frac{[A]}{m_i}$ (remark that these numbers are coprime);
- the numbers $\mu_{(i,A)}$ are arbitrary integers that satisfy

$$\sum_{i \in A} \lambda_{(i,A)}\mu_{(i,A)} = 1,$$

for all $i \in A$.

We return to the decryption operation for ElGamal cryptosystem. Suppose that a group of users $\{U_i \mid i \in A\}$, for some authorized access set A, want to decrypt a message (γ, δ). If they individually compute the elements

$$\gamma_i = \gamma^{f_{(i,A)}(I_i)} \texttt{ mod } p,$$

then

$$\prod_{i \in A} \gamma_i \texttt{ mod } p = \gamma^{\sum_{i \in A} f_{(i,A)}(I_i)} \texttt{ mod } p$$

On the other hand,

$$\gamma^a \texttt{ mod } p = \gamma^{\sum_{i \in A} f_{(i,A)}(I_i) \texttt{ mod } [A]} \texttt{ mod } p$$

Thus, if the access set A additionally satisfies the condition

$$\sum_{i \in A} f_{(i,A)}(I_i) \equiv (\sum_{i \in A} f_{(i,A)}(I_i) \texttt{ mod } [A]) \ mod \ ord_p(\gamma)$$

(for example, we may have $(p-1)|[A]$ which leads, using $ord_p(\gamma)|(p-1)$, to $ord_p(\gamma)|[A]$) then $\gamma^a \texttt{ mod } p$ can be obtained as $\prod_{i \in A} \gamma_i \texttt{ mod } p$, and the message x can be finally obtained as $(\gamma^a \texttt{ mod } p)^{-1} \cdot \delta \texttt{ mod } p$. If p and $\mathcal{A}$ are chosen such that $(p-1)|[A]$, for all $A \in \mathcal{A}$, then the decryption can be carried on by any authorized group of users.

In [20] we have combined the threshold secret sharing schemes based on the general Chinese remainder theorem with the *RSA* cryptosystem [29] in order to get threshold decryption or signature generation. This technique can be extended to more general access structures in an obvious manner.

6 Conclusions

We have extended the threshold secret schemes based on the Chinese remainder theorem in order to address more general access structures. We have also shown that some access structures can not be realized using only sequences of pairwise coprime numbers and, thus, the general Chinese remainder theorem must be used. We have further presented some interesting aspects of these schemes like verifiability, secret sharing homomorphisms and multiplicative properties and we have also showed how to exploit these properties in e-voting or in threshold cryptography.

An interesting open problem is to characterize the access structures that can be realized using the proposed schemes. Another interesting problem is the problem to efficiently generate extended Mignotte sequences with a large factor $\frac{\alpha-\beta}{\beta}$. We shall consider these problems in our future work.

Acknowledgements Research reported here was partially supported by the National University Research Council of Romania under the grant CNCSIS632/2005.

References

1. C. A. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, IT-29(2):208–210, 1983.
2. J. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret secret. In A. M. Odlyzko, editor, *Advanced in Cryptology-CRYPTO' 86*, volume 263 of *Lecture Notes in Computer Science*, pages 251–260. Springer-Verlag, 1987.
3. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advanced in Cryptology-CRYPTO' 88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1989.
4. A. Beutelspacher. How to say "no". In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - EuroCrypt '89*, volume 434 of *Lecture Notes in Computer Science*, pages 491–496, 1990.
5. G. R. Blakley. Safeguarding cryptographic keys. In *National Computer Conference, 1979*, volume 48 of *American Federation of Information Processing Societies Proceedings*, pages 313–317, 1979.
6. C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. Secret sharing schemes with veto capabilities. In G. Cohen, S. Litsyn, A. Lobstein, and G. Zemor, editors, *Algebraic Coding*, volume 781 of *Lecture Notes in Computer Science*, pages 82–89, 1993.
7. B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science*, pages 383–395. IEEE Press, 1985.

8. H. Cohen. *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. Springer-Verlag, 4th edition, 2000.
9. R. Cramer, 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*, volume 1070 of *Lecture Notes in Computer Science*, pages 72–83. Springer-Verlag, 1996.
10. Y. Desmedt. Some recent research aspects of threshold cryptography. In E. Okamoto, G. I. Davida, and M. Mambo, editors, *ISW '97: Proceedings of the First International Workshop on Information Security*, volume 1396 of *Lecture Notes in Computer Science*, pages 158–173. Springer-Verlag, 1998.
11. Y. Desmedt, G. Di Crescenzo, and M. Burmester. Multiplicative non-abelian sharing schemes and their applications to threshold cryptography. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology - Asiacrypt'94*, volume 917 of *Lecture Notes in Computer Science Volume*, pages 21–32. Springer-Verlag, 1995.
12. Y. Desmedt and Y. Frankel. Threshold cryptosystems. In G. Brassard, editor, *Advances in Cryptology - Crypto '89*, volume 435 of *Lecture Notes in Computer Science*, pages 307–315. Springer-Verlag, 1990.
13. C. Ding, D. Pei, and A. Salomaa. *Chinese remainder theorem: applications in computing, coding, cryptography.* World Scientific Publishing Co., Inc., 1996.
14. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology: Proceedings of Crypto '84*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer-Verlag, 1985.
15. P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science, 1987*, pages 427–437. IEEE Press, 1987.
16. A. S. Fraenkel. New proof of the generalized Chinese remainder theorem. *Proceedings of American Mathematical Society*, 14:790–791, 1963.
17. H. Garner. The residue number system. *IRE Transactions on Electronic Computers*, EC-8:140–147, 1959.
18. O. Goldreich, D. Ron, and M. Sudan. Chinese remaindering with errors. *IEEE Transactions on Information Theory*, IT-46(4):1330–1338, 2000.
19. S. Iftene. 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*, pages 196–201, 2004.
20. S. Iftene. Threshold RSA based on the general Chinese remainder theorem. Technical Report TR 05-05, "Al.I.Cuza" University of Iaşi, Faculty of Computer Science, 2005. URL:http://www.infoiasi.ro/˜tr/tr.pl.cgi.
21. M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *Proceedings of the IEEE Global Telecommunications Conference, Globecom '87*, pages 99–102. IEEE Press, 1987.
22. M. Mignotte. How to share a secret. In T. Beth, editor, *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982*, volume 149 of *Lecture Notes in Computer Science*, pages 371–375. Springer-Verlag, 1983.
23. S. Obana and K. Kurosawa. Veto is impossible in secret sharing schemes. *Information Processing Letters*, 58(6):293–295, 1996.
24. O. Ore. The general Chinese remainder theorem. *American Mathematical Monthly*, 59:365–370, 1952.
25. T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology - Crypto '91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140. Springer-Verlag, 1992.
26. S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24:106–110, 1978.
27. J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for the RSA public-key cryptosystem. *IEE Electronics Letters*, 18 (21):905–907, 1982.

28. M. Quisquater, 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*, volume 2274 of *Lecture Notes in Computer Science*, pages 199–210. Springer-Verlag, 2002.
29. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
30. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.