Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem

Sorin Iftene and Ioana Boureanu

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

{siftene,iboureanu}@infoiasi.ro

Abstract

A secret sharing scheme derives from a given secret certain shares (or shadows) which are distributed to users. The secret can be recovered only by certain predetermined groups. 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. In the weighted threshold secret sharing schemes, the users do not have the same status. More exactly, 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. In this paper we extend the threshold secret sharing schemes based on the Chinese remainder theorem in order to realize weighted threshold secret sharing.

AMS Subject Classification: 94A60, 94A62, 11A07
Keywords and phrases: cryptography, secret sharing, weighted threshold access structure, Chinese remainder theorem

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 predetermined groups. Secret sharing has applications to safeguarding cryptographic keys and providing shared access to strategical resources, threshold cryptography (see, for example, [7]) and some e-voting schemes (see, for example, [6]).

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. We mention Shamir's threshold secret sharing scheme [19] based on polynomial interpolation, Blakley's geometric threshold secret sharing scheme [5], Mignotte's threshold secret sharing scheme [13] and Asmuth-Bloom threshold secret sharing scheme [1], the last two ones based on the Chinese remainder

theorem. There are situations which require more complex access structures than the threshold ones. Shamir [19] 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. In these situations, the users do not have the same status. In the *weighted threshold* secret sharing schemes, 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. Weighted threshold secret sharing was studied in [2], [3], and [14].

In this paper, we extend the threshold secret sharing schemes based on the Chinese remainder theorem in order to realize weighted threshold secret sharing.

The paper is organized as follows. The rest of this section is dedicated to the Chinese remainder theorem. In Section 2, after a brief introduction to secret sharing, we present threshold secret sharing schemes based on the Chinese remainder theorem. In Section 3, we extend the threshold secret sharing schemes based on the Chinese remainder theorem in order to realize weighted threshold secret sharing. The last section concludes the paper.

We further present some basic facts on the Chinese remainder theorem.

The Chinese remainder theorem has many applications in computer science (see, for example, [8]). We only mention its applications to the RSA decryption algorithm as proposed by Quisquater and Couvreur [17], to the discrete logarithm algorithm as proposed by Pohlig and Hellman [16], and to the algorithm for recovering the secret in the Mignotte's threshold secret sharing scheme [13] and in its generalization [12], 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 [15]:

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

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

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 $\mathbf{Z}_{[m_1,\ldots,m_k]}$ ($[m_1, \ldots, m_k]$ denotes the least common multiple of $m_1, \ldots, m_k$).

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 [10] found an efficient algorithm for this case and Fraenkel [9] 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. Let n be an integer, $n \geq 2$ and $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. 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.*

A natural condition is that an access structure $\mathcal{A}$ is *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 access sets, i.e., the set

$$\mathcal{A}_{min} = \{A \in \mathcal{A} | (\forall B \in \mathcal{A} \setminus \{A\})(\neg B \subseteq A)\}.$$

In the same way, 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

$$\overline{\mathcal{A}}_{max} = \{A \in \overline{\mathcal{A}} | (\forall B \in \overline{\mathcal{A}} \setminus \{A\})(\neg A \subseteq B)\}.$$

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, $2 \leq k \leq n$, 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.*

We briefly present 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 [13] uses special sequences of integers, referred to as *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 a randomly chosen 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 $I_i = S \bmod m_i$, 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

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

A generalization of Mignotte's scheme by allowing modules that are not necessarily pairwise coprime was proposed in [12], 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

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

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, except for the fact $\alpha = min_{1 \leq i_1 < \cdots < i_k \leq n}([m_{i_1}, \ldots, m_{i_k}])$ and $\beta = max_{1 \leq i_1 < \cdots < i_{k-1} \leq n}([m_{i_1}, \ldots, m_{i_{k-1}}])$. 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], also 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

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

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

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

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 to threshold secret sharing has also been discussed in [11] and an unitary point of view on the security of the threshold secret sharing schemes based on the Chinese remainder theorem was presented in [18].

3 Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem

We first introduce the weighted threshold access structures.

Definition 3 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*.

The parameters $\omega_1, \ldots, \omega_n$ will be referred to as the *weights* and w as the *threshold*. If $\mathcal{A}$ is a (ω, w, n)-weighted threshold access structure, then any $\mathcal{A}$-secret sharing scheme will be referred to as a (ω, w, n)-*weighted threshold secret sharing scheme*. Intuitively, in the weighted threshold secret sharing schemes, 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.

We have to remark that exist access structures that are not weighted threshold. We present a simple example that proves this statement.

Example 1 (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 and, respectively, 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, further, $2 \cdot max(\omega_1, \omega_2) + 2 \cdot max(\omega_3, \omega_4) \geq 2w$ 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 set!

We indicate now how to extend the threshold secret schemes based on the Chinese remainder theorem to weighted threshold 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 the Asmuth-Bloom scheme. We first extend the (generalized) threshold Mignotte sequences in a natural manner.

Definition 4 Let $n \geq 2$, $\omega = (\omega_1, \ldots, \omega_n)$ a sequence of weights, and the threshold w such that $2 \leq w \leq \sum_{i=1}^{n} \omega_i$. A (ω, w, n)-Mignotte sequence is a sequence $m_1, \ldots, m_n$ of positive integers such that

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

Remark 1 In case $\omega_1 = \cdots = \omega_n = 1$ and $w = k$, a sequence $m_1, \ldots, m_n$ is a (ω, w, n)-Mignotte sequence if and only if $m_1, \ldots, m_n$ is a generalized (k, n)-Mignotte sequence in sense of Definition 2.

In the same case, an ordered sequence $m_1, \ldots, m_n$ with pairwise coprime elements is a (ω, w, n)-Mignotte sequence if and only if $m_1, \ldots, m_n$ is a (k, n)-Mignotte sequence in sense of Definition 1.

For arbitrary weights and thresholds, a (ω, w, n)-Mignotte sequence can be constructed as follows. Let $m'_1, \ldots, m'_N$ be a generalized (w, N)-Mignotte sequence, where $N = \sum_{i=1}^{n} \omega_i$ and define $m_i = [\{m'_j | j \in P_i\}]$, 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 $1 \leq i \leq n$. We obtain that

$$\begin{aligned} max_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \leq w-1}}([\{m_i | i \in A\}]) &= max_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \leq w-1}}([\{[\{m'_j | j \in P_i\}] | i \in A\}]) \\ &= max_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \leq w-1}}([\{m'_j | j \in \cup_{i \in A} P_i\}]). \end{aligned}$$

Moreover, for any set $A \in \mathcal{P}(\{1, 2, \ldots, n\})$ with $\sum_{i \in A} \omega_i \leq w - 1$ we also have $|\{m'_j | j \in \cup_{i \in A} P_i\}| = \sum_{i \in A} |P_i| = \sum_{i \in A} \omega_i \leq w - 1$ and, thus,

$$max_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \leq w-1}}([\{m_i | i \in A\}]) \leq max_{1 \leq i_1 < \cdots < i_{w-1} \leq N}([m'_{i_1}, \ldots, m'_{i_{w-1}}]) \tag{2}$$

By the same reason, we obtain that

$$min_{1 \leq i_1 < \cdots < i_w \leq N}([m'_{i_1}, \ldots, m'_{i_w}]) \leq min_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \geq w}}([\{m_i | i \in A\}]). \tag{3}$$

Using relations (2), (3), and the fact that $m'_1, \ldots, m'_N$ is a generalized (w, N)-Mignotte sequence, we obtain that the relation (1) holds, which implies that the sequence $m_1, \ldots, m_n$ is indeed a (ω, w, n)-Mignotte sequence.

Example 2 illustrates this construction.

Example 2 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 $7, 11, 13, 17, 19, 23$ is a generalized $(3, 6)$-Mignotte 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 23, 19, $[7, 17]$, $[11, 13]$ is a $((1, 1, 2, 2), 3, 4)$-Mignotte sequence.

These sequences can be used for constructing weighted threshold secret sharing schemes in an obvious way. More exactly, having a (ω, w, n)-Mignotte sequence $m_1, \ldots, m_n$, we may construct a (ω, w, n)-weighted threshold secret sharing scheme as follows:

- the secret S is an arbitrary integer in the interval $[\beta + 1, \alpha - 1]$, where $\alpha = min_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \geq w}}([\{m_i | i \in A\}])$ and $\beta = max_{\substack{A \in \mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i \in A} \omega_i \leq w-1}}([\{m_i | i \in A\}])$;
- the shares $I_1, \ldots, I_n$ are chosen as follows: $I_i = S \bmod m_i$, for all $1 \leq i \leq n$.

Having a set of shares $\{I_i \mid i \in A\}$, where A satisfies $\sum_{i\in A}\omega_i \geq w$, the secret S can be obtained as the unique solution modulo $[\{m_i|i \in A\}]$ of the system of equations

$$\left\{ \begin{array}{rcl} x & \equiv & I_i \ mod \ m_i, \quad i \in A \end{array} \right.$$

Indeed, the secret S is the unique solution modulo $[\{m_i|i \in A\}]$ 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, $S \in \mathbf{Z}_{[\{m_i|i\in A\}]}$, by the choice of the secret S ($S < \alpha$ and $\alpha = min_{\substack{A\in\mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i\in A}\omega_i \geq w}}([\{m_i|i \in A\}])$).

Having a set of shares $\{I_i \mid i \in A\}$, where A satisfies $\sum_{i\in A}\omega_i \leq w-1$, the only information we can obtain by finding the unique solution x_0 in $\mathbf{Z}_{[\{m_i|i\in A\}]}$ of the system of equations

$$\left\{ \begin{array}{rcl} x & \equiv & I_i \ mod \ m_i, \quad i \in A \end{array} \right.$$

is that $S \equiv x_0 \ mod \ [\{m_i|i \in A\}]$. Indeed, the secret S is not the unique solution modulo $[\{m_i|i \in A\}]$ of the above system of equations because $S \notin \mathbf{Z}_{[\{m_i|i\in A\}]}$, by the choice of the secret S ($S > \beta$ and $\beta = max_{\substack{A\in\mathcal{P}(\{1,2,\ldots,n\}) \\ \sum_{i\in A}\omega_i \leq w-1}}([\{m_i|i \in A\}])$). By choosing (ω, w, n)-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 $S \equiv x_0 \ mod \ [\{m_i|i \in A\}]$, for some unauthorized access set A, is intractable.

Example 3 (with artificial small parameters)
Consider $n = 4$, the weights $\omega_1 = \omega_2 = 1$, $\omega_3 = \omega_4 = 2$, and the threshold $w = 3$. The corresponding weighted threshold access structure is given by $\mathcal{A}_{min} = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$ and $\overline{\mathcal{A}}_{max} = \{\{1, 2\}, \{3\}, \{4\}\}$. According to Example 2, the sequence 23, 19, 119, 143 is a $((1, 1, 2, 2), 3, 4)$-Mignotte sequence. We obtain that

$$\alpha = min([23, 119], [23, 143], [19, 119], [19, 143], [119, 143]) = 2261,$$
$$\beta = max([23, 19], 119, 143) = 437.$$

A $((1, 1, 2, 2), 3, 4)$-weighted threshold secret sharing scheme is described next:

- the secret S is chosen in the interval $[438, 2260]$, for example, $S = 601$;
- the shares are $I_1 = 601 \ \texttt{mod} \ 23 = 3$, $I_2 = 601 \ \texttt{mod} \ 19 = 12$, $I_3 = 601 \ \texttt{mod} \ 119 = 6$, and $I_4 = 601 \ \texttt{mod} \ 143 = 29$.

Having the shares $I_1 = 3$ and $I_3 = 6$, the secret S can be obtained as the unique solution in $\mathbf{Z}_{2737}$ of the system of equations

$$\left\{ \begin{array}{rcl} x & \equiv & 3 \ mod \ 23 \\ x & \equiv & 6 \ mod \ 119 \end{array} \right.$$

that is indeed 601.

But having the shares $I_1 = 3$ and $I_2 = 12$, the secret S can not be obtained as the unique solution in $\mathbf{Z}_{437}$ of the system of equations

$$\left\{ \begin{array}{rcl} x & \equiv & 3 \ mod \ 23 \\ x & \equiv & 12 \ mod \ 19 \end{array} \right.$$

because this is 164.

4 Conclusions

We have extended the threshold secret schemes based on the Chinese remainder theorem in order to address to the weighted threshold access structures by introducing the weighted threshold Mignotte sequences. We have proposed a method for generating such sequences using generalized Mignotte threshold sequences. We leave open the problem of finding weighted threshold Mignotte sequences without using threshold Mignotte sequences. Another interesting problem is to efficiently generate weighted threshold 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] A. Beimel, T. Tassa, and E. Weinreb. Characterizing ideal weighted threshold secret sharing. In J. Kilian, editor, *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 600–619. Springer-Verlag, 2005.

[3] Amos Beimel and Enav Weinreb. Monotone circuits for weighted threshold functions. In *20th Annual IEEE Conference on Computational Complexity (CCC 2005), 11-15 June 2005, San Jose, CA, USA*, pages 67–75. IEEE Computer Society, 2005.

[4] 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.

[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] 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.

[7] 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.

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

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

[10] H. Garner. The residue number system. *IRE Transactions on Electronic Computers*, EC-8:140–147, 1959.

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

[12] 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. Mirton Publishing House, 2004.

[13] 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.

[14] P. Morillo, C. Padró, G. Sáez, and J. L. Villar. Weighted threshold secret sharing schemes. *Information Processing Letters*, 70(5):211–216, 1999.

[15] O. Ore. The general Chinese remainder theorem. *American Mathematical Monthly*, 59:365–370, 1952.

[16] 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.

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

[18] 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.

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