Compartmented Secret Sharing Based on the Chinese Remainder Theorem

Sorin Iftene

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

Abstract

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. 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 a fixed compartment threshold and the total number of participants is greater than a global threshold.

In this paper we present a new compartmented secret sharing scheme by extending the Brickell's construction [4] 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.

AMS Subject Classification: 94A62, 11A07

Keywords and phrases: secret sharing, compartmented 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*) which are distributed to users. The secret may be recovered only by certain predetermined groups. The initial applications of secret sharing were 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]) are more recent applications of the secret sharing schemes.

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 [20] based on polynomial interpolation, Blakley's geometric threshold secret sharing scheme [3], Mignotte's threshold secret sharing scheme [15] and Asmuth-Bloom threshold secret sharing scheme [1], both based on the Chinese remainder theorem. Ito, Saito,

and Nishizeki [14], Benaloh and Leichter [2] give constructions for more general secret sharing schemes.

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 a fixed compartment threshold, and the total number of participants is greater than a global threshold.

In this paper we present a new compartmented secret sharing scheme by extending the Brickell's construction [4] 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.

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. In Section 2, after a brief introduction to secret sharing, we present the threshold secret sharing schemes based on the Chinese remainder theorem. In Section 3 we indicate how to use the threshold secret sharing schemes based on the Chinese remainder theorem in order to realize compartmented secret sharing. The last section concludes the paper.

In the rest of this section we present some basic facts on number theory. For more details, the reader is referred to [5].

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 $a \texttt{ mod } b$.

Let $a_1, \ldots, a_n \in \mathbf{Z}$ such that $a_1^2 + \cdots + a_n^2 \neq 0$. The *greatest common divisor* (*gcd*) of $a_1, \ldots, a_n$ will be denoted by $(a_1, \ldots, a_n)$.

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 $[a_1, \ldots, a_n]$.

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 $m|(a-b)$. $\mathbf{Z}_m$ denotes the set $\{0, 1, \ldots, m-1\}$

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 [18], the discrete logarithm algorithm as proposed by Pohlig and Hellman [17], and the algorithm for recovering the secret in the Mignotte's threshold secret sharing scheme [15] 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 [16]:

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 $\mathbf{Z}_{[m_1,\ldots,m_k]}$.

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. Suppose we have n users labeled with the numbers $1, \ldots, n$ and consider a set of groups $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. 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 groups*.

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

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 [15] 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 $I_i = S \bmod m_i$, 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 [13], 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 $I_i = (S + \gamma \cdot r) \bmod m_i$, 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 $S = x_0 \bmod r$, 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 in threshold secret sharing has been also discussed in [12] and an unitary point of view on the security of the threshold secret sharing schemes based on the Chinese Remainder Theorem was presented in [19]. Although the threshold secret sharing schemes based on the Chinese Remainder Theorem are not perfect[1], by choosing carefully the parameters, these schemes can lead to a reasonable factor $\frac{\text{security}}{\text{size of shares}}$.

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 a fixed compartment threshold, and the total number of participants is greater than the global threshold.

The compartmented access structures can be introduced as follows.

Definition 3 Let $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ be a partition of $\{1, 2, \ldots, n\}$ and consider a sequence of *compartment thresholds* $\mathcal{K} = \{k_1, k_2, \ldots, k_m\}$, where $1 \leq k_j \leq |C_j|$, for all $1 \leq j \leq m$, and a *global threshold* k, $\sum_{j=1}^{m} k_j \leq k \leq n$. The $(\mathcal{C}, \mathcal{K}, k)$-*compartmented access structure* is given by

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

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

In this case, an $\mathcal{A}$-secret sharing scheme will be referred to as a $(\mathcal{C}, \mathcal{K}, k)$-*compartmented secret sharing scheme*.

The compartmented secret sharing has been discussed for the first time by Simmons in [21]. Brickell [4] proposed an elegant solution for the case $k = \sum_{j=1}^{m} k_j$ by choosing the secret S as a combination of m compartment secrets and using a threshold secret sharing scheme for each compartment. Ghodosi, Pieprzyk, and Safavi-Naini proposed an efficient scheme for the general case in [11].

We extend Brickell's construction to the general case as follows.

- The secret is chosen as $S = s + s_1 + \cdots + s_m$, where $s, s_1, \ldots, s_m$ 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 with respect to an arbitrary (k, n)-threshold secret sharing scheme;
  - 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.

Remark 1 *(Correctness)*
Let A be an authorized access group. Thus, $|A| \geq k$ and, for all $j = \overline{1, m}$, $|A \cap C_j| \geq k_j$. Having at least k of the shares $g_1, \ldots, g_n$, the value s 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 obtained as $S = s + s_1 + \cdots + s_m$.

Remark 2 *(Security)*
Let A be an unauthorized access group. There are two possibilities:

- $|A| < k$ - in this case, the value s 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.

Remark 3
In case $k = \sum_{j=1}^{m} k_j$, if all compartment threshold conditions hold then the global threshold condition holds too. Thus, the component s of the secret can be removed and the shares can be chosen only as $I_i = c_i$, for any $1 \leq i \leq n$, thus obtaining Brickell's construction.

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, in the same time, a reasonable level of security. For simplicity, we shall only deal with the Mignotte's scheme, but we must mention that the technique can be also applied to Asmuth-Bloom scheme.

Example 1 *(with artificial small parameters)*
Consider $n = 6$, $\mathcal{C} = \{\{1, 2, 3\}, \{4, 5, 6\}\}$, the compartment thresholds $k_1 = 2$, $k_2 = 2$ and the global threshold $k = 5$. The sequence 5, 7, 11, 13, 17, 19 is a $(5, 6)$-Mignotte sequence, with $\alpha = 85085$ and $\beta = 46189$ and the sequence 7, 11, 13 is a $(2, 3)$-Mignotte sequence with $\alpha = 77$ and $\beta = 13$. We choose $s = 50000$, $s_1 = 30$, and $s_2 = 40$. The secret will be $S = 50070$ and the shares $I_1 = (0, 2)$, $I_2 = (6, 8)$, $I_3 = (5, 4)$, $I_4 = (2, 5)$, $I_5 = (3, 7)$, 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 resolve 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, $s = 50000$, $s_1 = 30$, $s_2 = 40$, and finally $S = 50070$.

Further improvements can be obtained by choosing s, $s_1, \ldots, s_m$ such that $g_i = c_i$ for some $i \in \{1, 2, \ldots, n\}$. For these cases we can define $I_i = g_i = c_i$. For this, we can generate first $s_1, \ldots, s_m$ and $c_1, \ldots, c_n$ and determining s by solving the system of equations

$$\begin{cases} x \equiv c_1 \ mod\ m_1 \\ \vdots \qquad \vdots \\ x \equiv c_k \ mod\ m_k \end{cases}$$

In this case we can choose $g_i = c_i$ for all $1 \leq i \leq k$ and $g_i = s \bmod m_i$, for all $k+1 \leq i \leq n$. A compromise between the size of the shares and the level of security must be made.

Example 2 illustrates the reduction of the shares.

Example 2 *(with artificial small parameters)*
Let reconsider Example 1. 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 $s = 32817$. 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 $I_6 = (4, 1)$.

4 Conclusions

In this paper we have presented a new compartmented secret sharing scheme. More exactly, we have extended Brickell's construction to case that the global threshold is strictly greater than the sum of the compartment thresholds and we have proposed using computational-secure threshold secret sharing schemes as building blocks in order to decrease the size of shares, maintaining, in the same time, a reasonable level of security. Moreover, using threshold secret sharing schemes based on the Chinese remainder theorem can lead to further improvements. A compromise between the size of the shares and the level of security must be made. We shall investigate this subject 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 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.

[3] 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.

[4] E. F. Brickell. Some ideal secret sharing schemes. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 468–475. Springer-Verlag, 1990.

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

[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] H. Ghodosi, 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*, volume 1438 of *Lecture Notes in Computer Science*, pages 367–378. Springer-Verlag, 1998.

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

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

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

[19] 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.

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

[21] G. J. Simmons. How to (really) share a secret. In S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer-Verlag, 1990.