Compartmented Threshold *RSA* Based on the Chinese Remainder Theorem

Sorin Iftene
Department of Computer Science,
"Al. I. Cuza" University,
700483 Iasi, Romania
siftene@info.uaic.ro

Ştefan Ciobâcă
LSV, ENS Cachan & CNRS,
94235 Cachan, France
ciobaca@lsv.ens-cachan.fr

Manuela Grindei
LSV, ENS Cachan & CNRS,
94235 Cachan, France
grindei@lsv.ens-cachan.fr

Abstract

In this paper we combine the compartmented secret sharing schemes based on the Chinese remainder theorem with the RSA scheme in order to obtain, as a novelty, a dedicated solution for compartmented threshold decryption or compartmented threshold digital signature generation.

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

1. Introduction

In *threshold* (or *group-oriented*) cryptography, the capacity of performing cryptographic operations such as decryption or digital signature generation is shared among the members of a certain organization. In this paper we will consider realizing threshold variants of the well-known RSA scheme [18].

A *secret sharing scheme* is used for splitting the secret key in some partial keys, which are then distributed to the members of a certain organization, such that only some predetermined groups (which belong to the *access structure*) can perform the desired operation. The majority of the existing threshold cryptographic schemes rely on Shamir's secret sharing scheme [19]. Some interesting approaches relying on the secret sharing schemes based on the Chinese remainder theorem have been considered in [11] and [14]. All these threshold cryptographic schemes consider that all members of the organization have the same weight (belong to the so-called *threshold* access structure). The problem of threshold RSA over general access structures has been considered in [9]. However, this construction is too general, and the efficiency of this scheme strongly depends on the particularities of the underlying access structure. Thus, better solutions are required for specific classes of access structures. For example, an interesting solution for the case of the weighted threshold *RSA* has been recently proposed in [13].

In this paper we propose a solution for realizing threshold variants of RSA with respect to the *compartmented* access structures. In this case, the set of users is partitioned into compartments and the threshold operation can be performed if and only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold, and the total number of participants is greater than or equal to a global threshold.

The paper is organized as follows. In Section 2 we present the general variant of the Chinese remainder theorem. We review the secret sharing schemes based on the Chinese remainder theorem in Section 3. In Section 4 we present the compartmented threshold variants of the *RSA* cryptosystem and digital signature scheme. The last section concludes the paper.

2 The General Chinese Remainder Theorem

We recall a few basic facts on number theory (for more details, the reader is referred to [4]).

Let $a, b \in \mathbf{Z}$, $b \neq 0$. The *quotient* of the 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 case that $a \texttt{ mod } b = 0$ we will say that b is a *divisor* of a and we will denote this by $b|a$. An integer $p \geq 2$ that has only two positive divisors (1 and p) is called *prime*.

Let $a_1, \ldots, a_n \in \mathbf{Z}$, $a_1^2 + \cdots + a_n^2 \neq 0$. The *greatest common divisor* 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 greatest common divisor). In case that $(a_1, \ldots, a_n) = 1$, the numbers $a_1, \ldots, a_n$ are called *coprime*.

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

$\mathbf{Z}_m$ 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 will use the notation $a \equiv b \ mod \ m$, if $m|(a-b)$.

We will present next the *general* variant of the Chinese remainder theorem, variant that has been used in our previous schemes ([10, 11, 12, 13]):

Theorem 1 (Ore [17]) *The system of equations*

$$\begin{cases} x & \equiv & b_1 \ mod \ m_1 \\ & \vdots & \\ x & \equiv & b_k \ mod \ m_k \end{cases} \tag{1}$$

has solutions in $\mathbf{Z}$ *if and only if*

$$(\forall 1 \leq i, j \leq k)(b_i \equiv b_j \ mod \ (m_i, m_j)). \tag{2}$$

Moreover, if the above system of equations has solutions in $\mathbf{Z}$*, then it has a unique solution in* $\mathbf{Z}_{[m_1, \ldots, m_k]}$.

In case $(m_i, m_j) = 1$, for all $1 \leq i < j \leq k$, we obtain the *standard* variant of the Chinese remainder theorem. In this case there is always a solution modulo $m_1 \ldots m_k$.

Ore's proof ([17]) leads to the following algorithm:

CRT_Ore$(\mathbf{b_1}, \ldots, \mathbf{b_k}, \mathbf{m_1}, \ldots, \mathbf{m_k})$
`input:` $b_1, \ldots, b_k, m_1, \ldots, m_k \in \mathbf{Z}$ such that relation (2) holds true;
`output:` x, the unique solution modulo $[m_1, \ldots, m_k]$ of the system (1);
`begin`
1. `for` i:=1 `to` k `do` $c_i := \frac{[m_1, \ldots, m_k]}{m_i}$; (remark that $(c_1, \ldots, c_k) = 1$)
2. `find` $\alpha_1, \ldots, \alpha_k \in \mathbf{Z}$ that satisfy $\alpha_1 c_1 + \cdots + \alpha_k c_k = 1$;
3. $x := (\alpha_1 c_1 b_1 + \cdots + \alpha_k c_k b_k)$ `mod` $[m_1, \ldots, m_k]$;

`end`.

The Chinese remainder theorem has many applications in computer science (see [8] for an interesting survey on this topic).

3. Secret Sharing Based on the Chinese Remainder Theorem

A secret sharing scheme starts with a *secret* and then derives from it certain *shares* (or *shadows*) which are distributed to some users. The secret may be recovered only by certain predetermined authorized groups which belong to the *access structure*. Secret sharing schemes have been independently introduced by Blakley [2] and Shamir [19] as a solution for safeguarding cryptographic keys. Secret sharing schemes can be used for any situation in which the access to an important resource has to be restricted. We mention here the case of opening a bank vault or launching a nuclear missile.

Suppose we have n users labeled with the numbers $1, \ldots, n$ and let us consider an access structure[1] $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. Informally, an $\mathcal{A}$-*secret sharing scheme* is a method of generating $(S, (I_1, \ldots, I_n))$ such that

- (*correctness*) - for any $A \in \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$, is "easy";
- (*security*) - for any $A \notin \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$, is "hard".

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

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

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

will be referred to as the (k, n)-*threshold* access structure and an $\mathcal{A}$-secret sharing scheme will be referred to as an (k, n)-*threshold secret sharing scheme*.

In this paper we consider the compartmented access structures in which the set of users is partitioned into compartments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold, and the total number of participants is greater than or equal to a global threshold.

The compartmented access structures can be introduced as follows.

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

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

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

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

The sets $C_1, C_2, \ldots, C_m$ will be referred to as the *compartments* of the scheme, the values $k_1, k_2, \ldots, k_m$ as the *compartment thresholds* and k_0 as the *global threshold* of the scheme.

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

3.1 Threshold Secret Sharing Scheme based on the Chinese Remainder Theorem

Mignotte's threshold secret sharing scheme [16] uses special sequences of integers, referred to as *Mignotte sequences*.

Definition 2 Let n be an integer, $n \geq 2$, and $2 \leq k \leq n$. An (k, n)-*Mignotte sequence* is a sequence of pairwise coprime positive integers $p_1 < p_2 < \cdots < p_n$ such that $\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i$.

The above relation is equivalent with

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

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

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

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

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

  Indeed, the secret S is an integer solution of the above system by the choice of the shadows. Moreover, S lies in $\mathbf{Z}_{p_{i_1} \cdots p_{i_k}}$ because $S < \alpha$. On the other hand, having only $k-1$ distinct shares $I_{i_1}, \ldots, I_{i_{k-1}}$, we obtain only that $S \equiv x_0 \bmod p_{i_1} \cdots p_{i_{k-1}}$, where x_0 is the unique solution modulo $p_{i_1} \cdots p_{i_{k-1}}$ of the resulted system ($S > \beta \geq p_{i_1} \cdots p_{i_{k-1}} > x_0$). Therefore, in order to assure a reasonable level of security, (k, n)-Mignotte sequences with a large factor $\frac{\alpha - \beta}{\beta}$ must be chosen (a method of generating such sequences is presented in [15, page 9], these sequences being formed by consecutive primes).

An extension of the Mignotte's threshold secret sharing scheme has been proposed in [10] by introducing the generalized Mignotte sequences whose elements are not necessarily pairwise coprime.

Definition 3 Let n be an integer, $n \geq 2$, and $2 \leq k \leq n$. A *generalized* (k, n)-*Mignotte sequence* is a sequence $p_1, \ldots, p_n$ of positive integers such that

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

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

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

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

Asmuth and Bloom have proposed a slightly different scheme in [1], by choosing the shares as $I_i = (S + \gamma \cdot p_0) \bmod p_i$, for all $1 \leq i \leq n$. In their scheme, p_0 is a prime number smaller than $\frac{\alpha}{\beta}$ and the secret S is chosen as a positive integer smaller than p_0. γ is an arbitrary integer such that $S + \gamma \cdot p_0 \in \mathbf{Z}_{p_1 \cdots p_k}$. The secret is then reconstructed as $S = x_0 \bmod p_0$, where x_0 is the solution of the system of k modular equations.

3.2. Compartmented Secret Sharing Based on the Chinese Remainder Theorem

We present the compartmented secret sharing scheme from [12].

- The secret is chosen as $S = \sum_{j=0}^{m} s_j$, where $s_0, s_1, \ldots, s_m$ are positive integers;
- The shares are chosen as $I_i = (g_i, c_i)$, for any $1 \leq i \leq n$, where
  - $g_1, \ldots, g_n$ are the shares corresponding to the secret s_0 with respect to an arbitrary (k_0, n)-threshold secret sharing scheme - these elements will be referred to as the *global* components of the shares;
  - for every $1 \leq j \leq m$, $\{c_i | i \in C_j\}$ are the shares corresponding to the secret s_j with respect to an arbitrary $(k_j, |C_j|)$-threshold secret sharing scheme - these elements will be referred to as the *compartment* components of the shares.

The correctness and the security of this scheme can be easily proven (see [12]). The threshold secret sharing schemes based on the Chinese remainder theorem can be used in order to decrease the size of shares, maintaining, at the same time, a reasonable level of security. For simplicity, we presently use only the construction based on Mignotte's scheme, but we have to mention that this technique can be also applied using Asmuth-Bloom scheme.

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

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

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

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

4. Compartmented Threshold *RSA* Based on the Chinese Remainder Theorem

In [18], Rivest, Shamir, and Adleman have proposed the following public-key cryptosystem, known as the *RSA* cryptosystem:

- `public key`: (N, e), where $N = p \cdot q$, p and q are distinct primes, and $e \in \mathbf{Z}^*_{\phi(N)}$;
- `private key`: (p, q, d), where d is a positive integer such that[2]
$$e \cdot d \equiv 1 \; mod \; \phi(N);$$
- `encryption`: a plaintext $x \in \mathbf{Z}_N$ is encrypted as $y = x^e \bmod N$;
- `decryption`: a cryptotext $y \in \mathbf{Z}_N$ is decrypted as $x = y^d \bmod N$.

The *RSA* cryptosystem can be transformed in a digital signature scheme as follows:

- `public key` and `private key`: as above;
- `signature generation`: the digital signature corresponding to a message $x \in \mathbf{Z}_N$ is $y = x^d \bmod N$;
- `signature verification`: having a pair $(x, y) \in \mathbf{Z}_N \times \mathbf{Z}_N$, y is the correct signature with respect to x if and only if $x = y^e \bmod N$.

The correctness of the cryptosystem and of the digital signature scheme is based on the fact that

$$x^{ed} \equiv x \; mod \; N,$$

for all $x \in \mathbf{Z}_N$ and e, d, N as above.

Threshold RSA signatures have been considered for the first time by Boyd [3], for some particular threshold access structures. Desmedt and Frankel have also considered the problem of threshold *RSA* in [6]. They have remarked that Shamir's threshold secret sharing scheme cannot be used directly for this purpose because Lagrange interpolation requires a field structure. Desmedt and Frankel have reconsidered this problem in [7], giving a solution in the case that p and q are *safe* primes, i.e., $p = 2p' + 1$ and $q = 2q' + 1$ with p' and q' primes. Shoup has presented a more efficient solution when p and q are safe primes in [20], and Damgård and Dupont described an efficient solution for general modules in [5]. All the mentioned schemes consider that the users are organized in a threshold access structure and all these schemes rely on Shamir's secret sharing scheme.

As an alternative, some interesting approaches relying on the secret sharing schemes based on the Chinese remainder theorem have been recently considered in [11] and [14] for the threshold case and in [13] for the weighted threshold case.

The problem of threshold RSA over general access structures has been considered in [9]. However, this construction is too general, and the efficiency of this scheme strongly depends on the particularities of the underlying access structure. Thus, better solutions are required for specific classes of access structures. We will present next a dedicated solution for the compartmented case.

In order to realize compartmented threshold RSA, the *administrator* derives the shares $I_i = (c_i, g_i), 1 \leq i \leq n$ corresponding to the secret exponent d using the method described in Section 3.2 (in this case $d \equiv \sum_{j=0}^{m} s_j \; mod \; [p-1, q-1]$, $g_i = s_0 \bmod p_{0,i}$, $c_i = s_{c(i)} \bmod p_{c(i),i}$, where $c(i)$ is the unique element j, $1 \leq j \leq m$, such that $i \in C_j$, for all $1 \leq i \leq n$) and then he securely distributes the shares to the users.

Suppose now that an authorized group of users A wants to compute $y = x^d \bmod N$, for some $x \in \mathbf{Z}_N$. By the choice of the elements $s_0, s_1, \ldots, s_m$, the desired result can be also expressed as $y = \prod_{j=0}^{m} x^{s_j} \bmod N$. Thus, the threshold computation can be divided into $m + 1$ components: a global component (computing $y_0 = x^{s_0} \bmod N$) and m compartment components (computing $y_j = x^{s_j} \bmod N$, for $1 \leq j \leq m$). The final result will be obtained as $y = \prod_{j=0}^{m} y_j \bmod N$. Let us focus on the global component of the threshold computation (the same reasoning can

[2] The parameters e and d may be also chosen such that

$$e \cdot d \equiv 1 \; mod \; [p-1, q-1].$$

be made for the compartment components of the threshold computation). Using Ore's algorithm (see Section 2), the element s_0 can be expressed as

$$s_0 = \sum_{i \in A} f_{(i,A)}(g_i) \bmod [\{p_{0,i} | i \in A\}],$$

where the function $f_{(i,A)} : \mathbf{N} \rightarrow \mathbf{N}$ is given by

$$f_{(i,A)}(x) = \alpha_{(i,A)} c_{(i,A)} x \bmod [\{p_{0,i} | i \in A\}], \text{ where}$$

- $c_{(i,A)} = \frac{[\{p_{0,i} | i \in A\}]}{p_{0,i}}$ (these numbers are coprime);
- the numbers $\alpha_{(i,A)}$ are arbitrary integers such that $\sum_{i \in A} \alpha_{(i,A)} c_{(i,A)} = 1$.

Thus, for computing the global component of the desired result, each user i of the group A individually computes the *partial global result* $y_{0,i} = x^{f_{(i,A)}(g_i)} \bmod N$ and sends it to the *combiner* who will compute the *incomplete global result* $z_0 = \prod_{i \in A} y_{0,i} \bmod N$.

In order to obtain the correct global component y_0, we follow the technique described in [14] for correcting z_0 by repeatedly performing

$$z_0 := z_0 \cdot x^{-[\{p_{0,i} | i \in A\}]} \bmod N$$

until the correct global result is obtained. Initially, $z_0 = x^{\sum_{i \in A} f_{(i,A)}(g_i)} \bmod N$ - in order to obtain $\sum_{i \in A} f_{(i,A)}(g_i) \bmod [\{p_{0,i} | i \in A\}]$ as the exponent, we will perform the reduction modulo $[\{p_{0,i} | i \in A\}]$ of the initial exponent by repeated subtractions. At most $|A| - 1$ operations will be required in order to perform the correction stage for the global component (because the initial exponent satisfies the relation $\sum_{i \in A} f_{(i,A)}(g_i) < |A| \cdot [\{p_{0,i} | i \in A\}]$).

The main problem is testing that the correct result is obtained. This can be made by correlating the correction steps for the global and compartment components. Thus, each user i individually computes, besides the partial global result $y_{0,i}$, a *partial compartment result* $y_{c(i),i}$ and sends these values to the combiner. The combiner computes the incomplete global result z_0 and the *incomplete compartment results* $z_j = \prod_{i \in A \cap C_j} y_{j,i} \bmod N$, for all $1 \leq j \leq m$. Finally, the combiner computes all combinations $z = \prod_{j=0}^{m} (z_j \cdot_{repeated} x^{-[\{p_{j,i} | i \in A \cap C_j\}]} \bmod N$, with at most $|A \cap C_j| - 1$ multiplications for each j, until $z^e \bmod N = x$.

Example 1 illustrates this technique.

Example 1 (with artificially small parameters)
Let us consider $n = 6$, $\mathcal{C} = \{\{1, 2, 3\}, \{4, 5, 6\}\}$, the compartment thresholds $k_1 = 2$, $k_2 = 2$, and the global threshold $k_0 = 5$. We use the $(5, 6)$-Mignotte sequence $5, 7, 11, 13, 17, 19$ (with $\alpha_0 = 85085$ and $\beta_0 = 46189$) for the global component and the $(2, 3)$-Mignotte sequence $7, 11, 13$ (with $\alpha_1 = \alpha_2 = 77$ and $\beta_1 = \beta_2 = 13$) for the two compartments.

Let us consider the RSA scheme with $p = 131$, $q = 257$, and $d = 1199$. The administrator derives $s_0 = 51059$, $s_1 = 23$, and $s_2 = 37$ (remark that $s_0 + s_1 + s_2 \equiv d \, mod \, [p-1, q-1]$). The users receive the following shares: $(g_1, c_1) = (4, 2)$, $(g_2, c_2) = (1, 1)$, $(g_3, c_3) = (8, 10)$, $(g_4, c_4) = (8, 2)$, $(g_5, c_5) = (8, 4)$, and $(g_6, c_6) = (6, 11)$.

The authorized group $A = \{1, 2, 4, 5, 6\}$ wants to compute $x^d \bmod N$ for $x = 17$. In the case of the global component, we obtain $c_{(1,A)} = 29393$, $c_{(2,A)} = 20995$, $c_{(4,A)} = 11305$, $c_{(5,A)} = 8645$, $c_{(6,A)} = 7735$. By the extended Euclid algorithm, we find $\alpha_{(1,A)} = 2$, $\alpha_{(2,A)} = 11757$, $\alpha_{(4,A)} = -42325200$, $\alpha_{(5,A)} = -8408606400$ and $\alpha_{(6,A)} = 9459682200$, such that $\sum_{i \in A} \alpha_{(i,A)} \cdot c_{(i,A)} = 1$.

The partial global results $y_{(0,1)} = 14876$, $y_{(0,2)} = 30262$, $y_{(0,4)} = 17491$, $y_{(0,5)} = 13363$ and $y_{(0,6)} = 9955$ are multiplied and we obtain the incomplete global result $z_0 = 29358$. Similarly, the partial compartment results are $y_{1,1} = 9959$, $y_{1,2} = 19773$ (therefore, $z_1 = 1024$), $y_{2,4} = 13304$, $y_{2,5} = 20697$ and $y_{2,6} = 7969$ (therefore, $z_2 = 5405$).

Considering all possible combinations $z_0 \cdot z_1 \cdot z_2 \cdot x_0^u \cdot x_1^v \cdot x_2^w \bmod N$ (where $x_j = x^{-[\{p_{j,i} | i \in A \cap C_j\}]} \bmod N$, for all $0 \leq j \leq 2$), with $u \in \{0, 1, 2, 3, 4\}$ and $v, w \in \{0, 1\}$, we obtain $u = 2$, $v = w = 1$ and the final result $z = 2192$.

We have obtained the final result by enumerating and computing the combinations $z = \prod_{j=0}^{m} z_j \cdot x_j^{u_j} \bmod N$ (where $x_j = x^{-[\{p_{j,i} | i \in A \cap C_j\}]} \bmod N$ and u_j is the number of times the multiplication by x_j is performed) until $z^e \bmod N = x$. Because $u_j < |A \cap C_j|$, for all $0 \leq j \leq m$, the entire correction process may require at most $(\prod_{j=0}^{m} |A \cap C_j|) - 1$ steps.

A way to speed up the computation is to reconsider the equation

$$\prod_{j=0}^{m} z_j^e \cdot x_j^{(u_j + e)} \equiv x \, mod \, N$$

(u_j are the unknowns). By splitting it into two parts

$$\prod_{j=0}^{\lfloor m/2 \rfloor} z_j^e \cdot x_j^{(u_j + e)} \equiv x \prod_{j=\lfloor m/2 \rfloor + 1}^{m} z_j^{-e} \cdot x_j^{-(u_j + e)} \, mod \, N,$$

we can enumerate separately the possible values for the left-hand side and the possible values for the right-hand side and use a meet-in-the-middle technique to find the appropriate u_j values. This method may significantly decrease the running time.

5. Conclusions and Future Work

In this paper, we have presented, as a novelty, a dedicated solution for compartmented threshold RSA. Our method

uses a correction stage which, for reasonably small compartments, behaves reasonably well. Moreover, we propose a meet-in-the-middle variant of the correction stage which can lead to significant improvement of the running time. We will consider improving the efficiency of the scheme in our further research.

It will be interesting to consider threshold RSA in the context of other classes of access structures. We will consider hierarchical threshold variants of RSA in our future work.

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] 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.

[3] C. Boyd. Digital multisignatures. In H. Beker and F. Piper, editors, *Cryptography and Coding, 1986*, pages 241–246. Oxford University Press, 1989.

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

[5] I. Damgård and K. Dupont. Efficient threshold RSA signatures with general moduli and no extra assumptions. In S. Vaudenay, editor, *Public Key Cryptography 2005*, volume 3386 of *Lecture Notes in Computer Science*, pages 346–361, 2005.

[6] 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.

[7] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer-Verlag, 1992.

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

[9] J. Herranz, C. Padró, and G. Sáez. Distributed RSA signature schemes for general access structures. In C. Boyd and W. Mao, editors, *Information Security, 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003*, volume 2851 of *Lecture Notes in Computer Science*, pages 122–136. Springer-Verlag, 2003.

[10] 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, SYNASC 2004*, pages 196–201. Mirton Publishing House, 2004.

[11] 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. (available at http://www.infoiasi.ro/~tr/tr.pl.cgi).

[12] S. Iftene. General secret sharing based on the Chinese remainder theorem with applications in E-voting. *Electronic Notes in Theoretical Computer Science*, 186:67–84, 2007. (Proceedings of ICS 2006).

[13] S. Iftene and M. Grindei. Weighted threshold RSA based on the Chinese remainder theorem. In *Proceedings of the 9th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2007*, pages 175–181. IEEE Computer Society Press, 2007.

[14] K. Kaya, A. A. Selçuk, and Z. Tezcan. Threshold cryptography based on Asmuth-Bloom secret sharing. In A. Levi, E. Savas, H. Yenigün, S. Balcisoy, and Y. Saygin, editors, *Proceedings of Computer and Information Sciences - ISCIS 2006*, volume 4263 of *Lecture Notes in Computer Science*, pages 935–942. Springer-Verlag, 2006.

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

[16] 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.

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

[18] 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.

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

[20] V. Shoup. Practical threshold signatures. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 207–220. Springer-Verlag, 2000.