Cheating Detection and Cheater Identification in CRT-based Secret Sharing Schemes

Daniel Pasailă, Vlad Alexa, Sorin Iftene
Department of Computer Science
"Al. I. Cuza" University
Iasi, Romania
Email: {daniel.pasaila,vlad.alexa,siftene}@info.uaic.ro

***Abstract*—In this paper we analyze the cheating detection and cheater identification problems for the secret sharing schemes based on the Chinese remainder theorem (CRT), more exactly for Mignotte [1] and Asmuth-Bloom [2] schemes. We prove that the majority of the solutions for Shamir's scheme [3] can be translated to these schemes and, moreover, there are some interesting specific solutions.**

I. Introduction

A *secret sharing scheme* starts with a secret and then derives from it certain shares (or shadows) which are distributed to some parties. The secret may be reconstructed only by certain predetermined groups which belong to the access structure. Secret sharing schemes have been independently introduced by Blakley [4] and Shamir [3] 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 bank vaults or launching a nuclear missile. Modern applications of the secret sharing schemes can be categorized as secure multiparty computation protocols, i.e., protocols which allow to some users to compute $f(x_1, \ldots, x_m)$ such that the input x_i is known only by the i^{th} user. Threshold cryptographic protocols and some e-voting or e-auction protocols are special cases of secure multiparty computation protocols.

Usually, a secret sharing scheme is coordinated by a *dealer* (or *administrator*) who has to be a mutually trusted party, but there are secret sharing schemes which can be configured without the presence of a dealer. The reconstruction of the secret can be made by the participants after they pool together their shares or by a special party, called *combiner*, after receiving the shares from the users of an authorized group.

Several solutions for the case in which the dealer or some users may behave maliciously have been proposed in the literature. The case of a possible dishonest dealer has been discussed for the first time by Chor, Goldwasser, Micali, and Awerbuch [5], who have introduced the notion of *verifiable secret sharing schemes* in which every user can verify that he has received a valid share. The problem of cheating in the reconstruction phase has been discussed by McEliece and Sarwate [6], and later on, by Tompa and Wool [7]. All the mentioned papers refer to Shamir's secret sharing scheme, which is the most popular (and used) secret sharing scheme.

The study of the secret sharing schemes based on the Chinese remainder theorem (Mignotte [1] and Asmuth-Bloom [2]) has been recently reactivated, due to the applications of these schemes in threshold cryptography (see [8], [9], [10]), e-voting (see [11]) or private integer comparison (see [12]). In this paper, we analyze the cheating detection and cheater identification problems for these secret sharing schemes. We prove that the majority of the solutions for Shamir's scheme can be translated to these schemes and, moreover, there are some interesting specific solutions. To the best of our knowledge, this is the first paper dedicated to this topic.

The paper is organized as follows. In Section 2 we present the Chinese remainder theorem (the standard variant and the general one). In the next section, after a short introduction to secret sharing, we present the secret sharing schemes based on the Chinese remainder theorem. In Section 4 we present our solutions to the cheating detection and cheater identification problems for the secret sharing schemes based on the Chinese remainder theorem. The last section concludes the paper.

II. The Chinese Remainder Theorem

We recall first some basic facts on number theory (for more details, the reader is referred to [13]).

Let $a, b, m \in \mathbf{Z}$, $m \geq 2$. The *remainder* of the integer division of a by m will be denoted by $a \texttt{ mod } m$. We say that a and b are *congruent* modulo m, and we use the notation $a \equiv b \ mod \ m$, if $a \texttt{ mod } m = b \texttt{ mod } m$. $\mathbf{Z}_m$ denotes the set $\{0, 1, \ldots, m-1\}$.

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 $[a_1, \ldots, a_n]$.

We will present first the standard variant of the Chinese remainder theorem:

Theorem 1: Let $k \geq 2$, $m_1, \ldots, m_k \geq 2$, $b_1, \ldots, b_k \in \mathbf{Z}$. If $(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$, then the system of equations

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

has a unique solution in $\mathbf{Z}_{m_1 \cdots m_k}$.

We will present next a more general variant of the Chinese remainder theorem:

Theorem 2: (Ore [14]) The system of equations

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

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

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

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

Fraenkel has proposed an efficient algorithm in [15]. The main idea of his algorithm is that, having x, the solution for the first i equations of the system, by adding a well-chosen multiple of the least common multiple of the first i modules to x, we may obtain an integer that is also a solution for the $(i+1)^{th}$ equation and iterate this construction until the final solution is obtained. The algorithm is presented next:

```
CRT_Fraenkel(b_1,..., b_k,m_1,..., m_k)
input: b_1,... b_k, m_1,... m_k ∈ Z that satisfy (2);
output: x, the unique solution modulo [m_1,... m_k] of the system (1);
begin
1.    for i:=1 to k − 1 do c_i := [m_1,..., m_i];
2.    x := b_1 mod m_1;
3.    for i:=1 to k − 1 do
          begin
4.            y := ((b_{i+1} − x)/(c_i, m_{i+1})) · ((c_i/(c_i, m_{i+1}))^{-1} mod m_{i+1}/(c_i, m_{i+1}));
5.            x := x + y · c_i;
          end
end.
```

In case $(m_i, m_j) = 1$, for all $1 \leq i < j \leq k$, we obtain Garner's algorithm [16].

The Chinese remainder theorem has many applications in computer science (see [17] for an interesting survey on this topic).

III. 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 users. The secret may be reconstructed only by certain predetermined groups which belong to the *access structure*.

Suppose we have n users labeled with the numbers $1, \ldots, n$ and let $\mathcal{A}$ be a set of subsets of $\{1, 2, \ldots, n\}$. Informally[1], 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 intractable.

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, $\mathcal{A}$ will be referred to as the *authorized access structure* (or simply as the *access structure*), the elements of the authorized access structure are called *authorized groups* and the rest are called *unauthorized groups*.

The schemes in which the unauthorized groups gain no information about the secret are referred to as *perfect*. In an *ideal* (perfect) secret sharing scheme the shares are as long as the secret.

In the first secret sharing schemes (e.g., Blakley's scheme [4] and Shamir's scheme [3]) 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 this case, the access structure is

$$\mathcal{A} = \{A \subseteq \{1, 2, \ldots, n\} \mid \ |A| \geq k\},$$

for some $n \geq 2$, $2 \leq k \leq n$ - this access structure will be referred to as the (k, n)-*threshold* access structure and, in this case, any $\mathcal{A}$-secret sharing scheme will be referred to as an (k, n)-*threshold secret sharing scheme*.

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

A. Mignotte's Scheme

Mignotte's threshold secret sharing scheme [1] 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 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 $I_i = S \ \mathtt{mod} \ p_i$, for all $1 \leq i \leq n$;
- Given k distinct shares $I_{i_1}, \ldots, I_{i_k}$, the secret S is reconstructed using the standard variant of the Chinese remainder theorem, as the unique solution modulo $p_{i_1} \cdots p_{i_k}$ of the system

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

Indeed, the secret S is an integer solution of the above system by the choice of the shares. 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 $S \equiv x_0 \ \mathtt{mod} \ p_{i_1} \cdots p_{i_{k-1}}$, where x_0 is the unique

[1] For the most important mathematical models for secret sharing, the reader is referred to Chapter 2 of [18].

solution modulo $p_{i_1} \cdots p_{i_{k-1}}$ of the resulted system (indeed, $S \neq x_0$ because $S > \beta \geq p_{i_1} \cdots p_{i_{k-1}} > x_0$). 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 [19, page 9], these sequences being formed by consecutive primes).

We have extended Mignotte's threshold secret sharing scheme in [20] by introducing the generalized Mignotte sequences whose elements are not necessarily pairwise coprime.

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 $p_1, \ldots, p_n$ 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 reconstructing the secret.

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

B. Asmuth-Bloom Scheme

Asmuth and Bloom have proposed a slightly different scheme in [2], by choosing the shares as

$$I_i = (S + \gamma \cdot p_0) \bmod p_i,$$

for all $1 \leq i \leq n$, where γ is an arbitrary integer such that $S + \gamma \cdot p_0 \in \mathbf{Z}_{p_1 \cdots p_k}$, providing that p_0 is a prime number less than $\frac{\alpha}{\beta}$ and the secret S is a positive integer less than p_0 - in this case the secret is reconstructed as $S = x_0 \bmod p_0$, where x_0 is the solution of the system of k modular equations. Goldreich, Ron, and Sudan [21] have proposed choosing $p_0, p_1, \ldots, p_n$ as prime numbers of the same size. Quisquater, Preneel, and Vandewalle [22] have proven that, by choosing $p_0, p_1, \ldots, p_n$ as consecutive primes, the resulted schemes are asymptotically perfect and asymptotically ideal (for technical details, the reader is referred to [22]).

In [11] we have proved that more general access structures can be realized using the Chinese remainder theorem.

IV. Cheating Detection and Cheater Identification in CRT-based Secret Sharing Schemes

Usually, a secret sharing scheme is coordinated by a *dealer* (or *administrator*) who has to be a mutually trusted party, but there are secret sharing schemes which can be configured without the presence of a dealer. The reconstruction of the secret can be made by the participants after they pool together their shares or by a special party, called *combiner*, after receiving the shares from the users of an authorized group.

Dealing with a possible malicious behavior of some users in the reconstruction phase has two aspects:

- *cheating detection* - when the frauds are detected but not the parties involved;
- *cheater identification* - when the authors of the frauds are identified.

Two main models for secret sharing schemes that deal with cheating have been proposed in the literature:

- The *CDV* Model, proposed by Carpentieri, De Santis, and Vaccaro in [23], in which the cheaters know the secret and they try to make another user obtain an invalid secret;
- The *OKS* Model, proposed by Ogata, Kurosawa, and Stinson in [24], in which the cheaters do not know the secret in advance.

In our opinion, the most natural model is when the cheaters form an unauthorized group and they combine with a group of honest users in order to reconstruct the secret. The cheaters modify their shares such that the reconstruction phase leads to an invalid secret but they will be able to obtain the correct secret.

As Schoenmakers has remarked in [25], *verifiable secret sharing* can also be seen as a solution for the problem of cheating - the shares presented in the reconstruction phase may be verified with respect to the distribution phase. Thus, the method proposed by Kaya and Selçuk in [26] for assuring verifiability in CRT-based secret sharing schemes, can also be used in order to detect cheating, but this method is rather expansive, requiring zero-knowledge proofs and special[2] sequences of modules.

We further discuss our solutions for cheating detection and cheater identification.

A. Cheating Detection for Mignotte's Scheme

In this subsection we prove that, in the case of the original Mignotte secret sharing scheme, a single participant can deceive other $k-1$ users with probability 1 in the *CDV* model and with high probability in the *OKS* model.

Suppose that the participants $i_1, i_2, \ldots, i_k$ pool their shares and that the participant i_1 decides to cheat. Then, the user i_1 should change his share I_{i_1} in I'_{i_1} such that a new secret $S' \neq S$, $S' \in (\beta, \alpha)$ is reconstructed. Let $l = p_{i_2} p_{i_3} \cdots p_{i_k}$ and $r = p_{i_1} p_{i_2} \cdots p_{i_k}$. From the reconstruction phase, it follows that S has the form $pl + q$, where $p \in \mathbf{Z}_{p_1}$ and $q \in \mathbf{Z}_l$. Moreover, using the Chinese remainder theorem, we can conclude that $S \bmod l = S' \bmod l = q$. Thus, S' has the form $p'l + q$. Since the Mignotte sequence $p_1, \ldots, p_k$ is publicly known, the cheater can easily compute l. Thus, he can choose $p' = p \pm 1$,

[2]The verifiability feature described in [26] requires Asmuth-Bloom sequences $p_0, p_1, ..., p_n$ such that $p_1, \ldots, p_n$ are Sophie Germain primes - the existence of such sequences and the magnitude of their elements have not been precisely stated.

adjusts his share $I'_{i_1} = (I_{i_1} \pm l) \bmod p_{i_1}$, thus leading to $S' = (p \pm 1)l + q = (S \pm l) \bmod r$.

In the *CDV* model the cheater knows the secret, so, using the relation $S' = (S \pm l) \bmod r$ he can assure that $S' \in (\beta, \alpha)$ (see Figure 1). The existence of such S' is granted since $k-1$ participants cannot uniquely determine the secret. Thus, the cheater can deceive honest participants with probability 1. Moreover, in the *CDV* model the cheater has control over the fake secret S'. Instead of using the relation $S' = (S \pm l) \bmod r$, he can compute q directly from S. The cheater can use $I'_{i_1} = S' \bmod p_{i_1}$, where $S' = p'l + q$, by choosing $p' \in \mathbf{Z}_\beta$ such that $S' \in (\beta, \alpha)$.

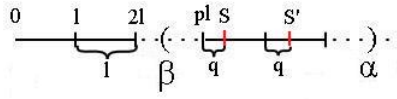

Fig. 1.

The above statement does not hold in the *OKS* model. Since the cheater does not know the secret, he cannot verify whether $S - l < \beta$ or $S + l > \alpha$. In this case he may always use $I'_{i_1} = (I_{i_1} + l) \bmod p_1$. The only case when cheating is detected is $S + l > \alpha$, this leading to $S' = (S + l) \bmod r < \beta$ (see Figure 2) or $S' = (S + l) \bmod r > \alpha$ (see Figure 3). Thus, honest participants are deceived with probability $1 - \frac{1}{\lceil \frac{\alpha - \beta}{l} \rceil}$.

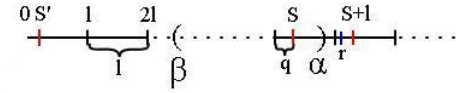

Fig. 2.

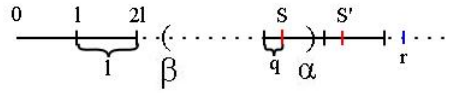

Fig. 3.

The next example illustrates this kind of attack:

Example 1: (with artificially small parameters)
Let $n = 5$, $k = 3$, and $p_1 = 661$, $p_2 = 673$, $p_3 = 677$, $p_4 = 683$, $p_5 = 691$. In this case, $\alpha = 301165481$ and $\beta = 471953$.

For the secret $S = 500000$, the dealer computes the shares $I_1 = 284$, $I_2 = 634$, $I_3 = 374$, $I_4 = 44$, and $I_5 = 407$.

Now, suppose that participants 1, 2, and 3 pool their shares and participant 1 decides to cheat. Then, he can easily compute $p_2 \cdot p_3 = 455621$ and adjust his share according to$I'_1 = (I_1 + p_2p_3) \bmod p_1 = 476$. Thus, by solving the system of equations

$$\begin{cases} x \equiv 476 \ mod \ 661 \\ x \equiv 634 \ mod \ 673 \\ x \equiv 374 \ mod \ 677 \end{cases},$$

the participants reconstruct the invalid secret $S' = (S + p_2p_3) \bmod p_1p_2p_3 = 955621$ that is also between β and α. The user 1 can obtain the real secret as $S = (S' - p_2p_3) \bmod p_1p_2p_3 = 500000$.

We propose the following solution for cheating detection in Mignotte's secret sharing scheme:

- The dealer generates an (k, n)-Mignotte sequence $p_1, p_2, \ldots, p_n$. The dealer also generates n distinct prime numbers $m_1, \ldots, m_n$ such that $\frac{\alpha - \beta}{\beta max_{1 \le i_1 < \cdots < i_{k-1} \le n}(m_{i_1} \cdot m_{i_2} \cdots m_{i_{k-1}})}$ is large enough;
- The secret S is chosen such that $\beta < S < \alpha$;
- The shares I_i are $(S \bmod p_i, S \bmod m_i, p_i, m_i)$.

The reconstruction phase is done exactly the same as in the original Mignotte's secret sharing scheme. After the secret S' is reconstructed, any participant i can detect cheating by comparing $S' \bmod m_i$ with the information provided by the dealer. Thus, the cheaters can deceive participant j with probability $\frac{1}{m_j}$.

B. Cheating Detection for Asmuth-Bloom Scheme

The attack presented in the previous subsection can be adapted to the Asmuth-Bloom secret sharing scheme. Here, we must note that $(S + \gamma p_0) = pl + q$, where $q \in \mathbf{Z}_l$ and $p \in \mathbf{Z}_{p_1}$. It follows that $(S + \gamma p_0) \bmod l = (S' + \gamma p_0) \bmod l = q$, thus $(S' + \gamma p_0)$ has the form $p'l + q$. Indeed, the cheater i_1 only controls the parameter p' in the above expression. Moreover, if the cheater chooses $p' = p + y$, then his fake share would be $I'_{i_1} = (I_{i_1} + yl) \bmod p_{i_1}$. Thus, the reconstructed fake secret S' would satisfy the equality

$$S' = ((pl + yl + q) \bmod r) \bmod p_0. \quad (3)$$

In both the OKS and CDV models the cheater can deceive the other participants with probability $1 - 1/p_0$, by choosing y randomly. Indeed, the only case when he does not succede is when $S = S'$. Furthermore, we prove that if the cheater has access to the other shares (i.e, if he pools his share last), he has full control over the secret S'. More exactly, for any secret $S' \in \mathbf{Z}_{p_0}$ he can find y such that the equality (3) holds. Knowing the other shares, the cheater can compute $x_0 = (S + \gamma p_0)$ by solving the system of k modular equations. Then he can compute p and q such that $x_0 = pl + q$, by taking $q = x_0 \bmod l$ and $p = (x_0 - q)/l$. Now, the cheater has to find y such that (3) is satisfied. Let $y = y_0 + y_1$, where y_0 is chosen such that $(pl + y_0l + q) \bmod r = q$. From $p_1l = r$, it follows that $y_0 = p_1 - p$. Next, we prove that for any fake secret $S' \in \mathbf{Z}_{p_0}$ the cheater can choose y_1 such that equality (3) written as $S' = ((pl + (y_0 + y_1)l + q) \bmod r) \bmod p_0$ holds. The above relation can be written as $S' = ((pl + y_0l + y_1l + q) \bmod r) \bmod p_0$. Since $pl + y_0l = r$, it follows that $S' = ((y_1l + q) \bmod r) \bmod p_0$.

When $y_1 \in \mathbf{Z}_{p_0}$ we obtain $S' = (y_1 l + q) \bmod p_0$, because $q \in \mathbf{Z}_l$ and $p_{i_0} < p_{i_1}$. Since $(p_0, l) = 1$ it follows that such y_1 exists for any $S' \in \mathbf{Z}_{p_0}$.

The next example illustrates this type of attack, when the cheater knows others' shares and controls the secret:

Example 2: (with artificially small parameters)
Let $n = 5,\ k = 3$ and $p_1 = 661, p_2 = 673, p_3 = 677, p_4 = 683, p_5 = 691,\ p_0 = 23,\ \gamma = 1254895$, and $S = 10$. The dealer computes $S + \gamma p_0 = 28862595$ and the shares $I_1 = 30$, $I_2 = 317$, $I_3 = 54$, $I_4 = 381$, and $I_5 = 216$. Now, suppose that participants $1, 2$ and 3 pool their shares and the participant 1 decides to cheat, and chooses $S' = 18$. The cheater computes $l = 455621$ and $r = 301165481$. Solving the modular equation system, he can compute $x_0 = 28862595$. After that, he obtains $q = 158472$ and $p = 63$. Furthermore, the cheater computes $y_0 = p_1 - p = 598$, and solving the equation $S' = (y_1 l + q) \bmod p_0$ he obtains $y_1 = 11$. Thus, he can adjust his share $I_1' = (I_1 + (y_0 + y_1)l) \bmod p_1 = 622$.

Then, by solving the system of equations

$$\begin{cases} x & \equiv & 622\ mod\ 661 \\ x & \equiv & 317\ mod\ 673 \\ x & \equiv & 54\ mod\ 677 \end{cases}$$

the participants obtain the solution $x_0' = 5170303$ and $S' = 5170303 \bmod p_0 = 18$.

We propose the following solution for cheating detection in Asmuth-Bloom secret sharing scheme:

- The dealer computes an (k, n)-Asmuth-Bloom sequence $p_0, p_1, p_2, \ldots, p_n$;
- The secret S is chosen as a random element in $\mathbf{Z}_{p_0}$;
- The shares I_i are chosen as

  $$I_i = ((S + \gamma \cdot p_0) \bmod p_i, (S + f(\gamma) \cdot p_0) \bmod p_i),$$

  where f is a pseudo random function such that $f(\gamma) \in \mathbf{Z}_{p_1 \cdots p_k}$.

The reconstruction is done same as in the original Asmuth-Bloom secret sharing scheme. Every participant can now verify if the reconstructed secret S' is the real secret. He can compute γ and check if $(S' + f(\gamma) \cdot p_0) \bmod p_i$ is equal with the information provided by the dealer. In this way, $k-1$ cheaters can deceive the k^{th} participant with probability $\frac{1}{p_k}$. Now we prove that in our scheme $k-1$ participants cannot narrow down the key space. Let $i_1, ..., i_{k-1}$ be the coalition that tries to find the secret, $l = p_{i_1} \cdots p_{i_k - 1}$. Let q' be the solution in $\mathbf{Z}_l$ of the first resulted system of equations and q'' the solution of the second resulted system of equations (with the values used for verification). It is easy to see that for any honest participant i_k, the solutions modulo p_0 for the two systems (with k equations) satisfy the relation $(q' + j' \cdot l) \bmod p_0 = (q'' + j'' \cdot l) \bmod p_0$. From $p_0 \cdot p_{n-k+2} \cdots p_n < p_1 \cdots p_k$, both $q' + j' \cdot l$ and $q = q'' + j'' \cdot l$ are smaller than $l * p_{i_k}$, for any $i_k \neq i_{j,(j<k)}$ and $j', j'' \in \mathbf{Z}_{p_0}$. Thus, since $(p_0, l) = 1$, if we take $j' = 0, 1, \ldots, p_0 - 1$, $q' + j' \cdot l$ will all be different. This is also valid for j''. Since we have p_0 different values less than p_0, it follows that for any $q \in \mathbf{Z}_{p_0}$ there exist $j', j'' \leq p_0$ such that $q = (q' + j' \cdot l) \bmod p_0$ and $q = (q'' + j'' \cdot l) \bmod p_0$.

C. A Cheating Detection Method based on Doubling the Shares

This method has been proposed by Ghodosi and Pieprzyk in [27] for cheating detection in Shamir's secret sharing scheme. For simplicity, we will present it only for Mignotte secret sharing scheme but it can be adapted to Asmuth-Bloom scheme in a straightforward manner. The main idea is to double the shares, using the second component for detecting a possible malicious behavior of some users in the reconstruction phase.

- Generate a $(2k-1, 2n)$-Mignotte sequence $p_1, \ldots, p_{2n}$;
- The secret S is chosen as a random integer such that $\beta < S < \alpha$, where $\alpha = \prod_{i=1}^{2k-1} p_i$ and $\beta = \prod_{i=0}^{2k-3} p_{2n-i}$;
- The shares I_i are chosen as

  $$I_i = (S \bmod p_{2i-1}, S \bmod p_{2i}),$$

  for all $1 \leq i \leq n$;
- Given the shares $I_{i_1} = (I_{i_1}^1, I_{i_1}^2), \ldots, I_{i_k} = (I_{i_k}^1, I_{i_k}^2)$, the secret S is recovered using the standard variant of the Chinese remainder theorem, as the unique solution modulo $p_{2i_1-1} p_{2i_1} \cdots p_{2i_{k-1}-1} p_{2i_{k-1}} p_{2i_k-1}$ of the system

  $$\begin{cases} x & \equiv & I_{i_1}^1\ mod\ p_{2i_1-1} \\ x & \equiv & I_{i_1}^2\ mod\ p_{2i_1} \\ & \vdots & \\ x & \equiv & I_{i_k}^1\ mod\ p_{2i_k-1} \end{cases}.$$

  The cheating detection can been performed by verifying

  $$S \equiv I_{i_k}^2\ mod\ p_{2i_k}.$$

The next example illustrates this method of cheating detection:

Example 3: (with artificially small parameters)
Let $n = 5$ and $k = 3$. Let us consider the following $(5, 10)$-Mignotte sequence: 661, 673, 677, 683, 691, 701, 709, 719, 727, and 733. In this case, $\alpha = 142135952254393$ and $\beta = 271652377961$. Let the secret be $S = 500000000000$.

The dealer computes the shares of each user: $I_1 = (28, 350)$, $I_2 = (151, 457)$, $I_3 = (309, 539)$, $I_4 = (547, 52)$, and $I_5 = (157, 80)$.

Let us consider the case when the first three users try to reconstruct the secret and the second user tries to cheat and sends the value 470.

$$\begin{cases} x & \equiv & 28\ mod\ 661 \\ x & \equiv & 350\ mod\ 673 \\ x & \equiv & 151\ mod\ 677 \\ x & \equiv & 470\ mod\ 683 \\ x & \equiv & 309\ mod\ 691 \end{cases}$$

By solving the system, the secret obtained (S') is 59601918653364 (fake). However, the cheater is detected because $S' \mod 701 = 138$ which is different from 539.

D. Methods based on Extra Shares

In the paper [28] of Harn and Lin, the detection/identification of cheaters is done using the extra shares - if the threshold is k, then the number of participants required in the reconstruction phase, denoted by j, is strictly greater than k ($j > k$). The main idea is that, if the number of honest users (denoted by h) is strictly greater than the number of cheaters (denoted by c) then the most frequent reconstructed secret (considering all groups of k users from the total j participants), will be the one reconstructed by the honest users, thus, the correct secret. In the rest of this subsection, we will show that the methods described by Harn and Lin can be adapted to Mignotte's scheme (and, similary, to Asmuth-Bloom scheme).

Let X be a set of j users. X is *consistent* if by solving all the systems of equations corresponding to any k users from X, the result obtained is the same for each system. For Mignotte's scheme we can use a more efficient algorithm. We choose arbitrary k users from X and solve the resulted system. Let S be the value we obtain. For all the other users from X we verify the following congruence:

$$S \equiv I_i \ mod \ p_i.$$

It is obvious that the set X is consistent if and only if all these congruences are satisfied. In order to detect if there are cheaters, we test if the given set of j users is consistent or not. If this set is consistent then there are no cheaters and the result obtained is the correct secret.

In order to identify the cheaters, we have to solve all the $\binom{j}{k}$ systems in order to obtain the most frequent reconstructed secret. A more efficient solution is to solve all the systems of $k-1$ equations and then solve the systems resulted by adding an equation to these systems (using Fraenkel's algorithm). In this way, we reduce the number of operations required for solving the original systems. Now that we have obtained the most frequent reconstructed secret, denoted by S, we can identify the cheaters by verifying the following congruence:

$$S \equiv I_i \ mod \ p_i.$$

If the above congruence is satisfied then the current user is honest and will be put in the set of the honest users (the initial users that have reconstructed the secret S will be put in the set of the honest users); otherwise, the user is a cheater and will be put in the set of the cheaters.

We will analyse next three types of attacks. The bounds for detection and identification, for these attacks, remain the same as those described by Harn and Lin in [28].

The first type of attack considers honest users who accidentally give bad shares or cheaters who give fake shares, but do not collaborate with other cheaters (stand-alone cheaters). The bounds in this case are:

- Detection : $j \geq k+1$ (we must have strictly more than k users participating in the reconstruction phase);
- Identification : $j - c \geq k$ (number of honest users must be greater than the threshold so that the most frequent reconstructed secret will be the one reconstructed by the honest users, thus, the correct one).

The next example illustrates this type of attack:

Example 4: (with artificially small parameters)
Let $n = 5$, $j = 5$, $k = 3$, and one cheater. Let us consider the following $(3, 5)$-Mignotte sequence: 661, 673, 677, 683, 691. In this case, $\alpha = 301165481$ and $\beta = 471953$. Let the secret be $S = 500000$.

The dealer computes the shares of each user: $I_1 = 284$, $I_2 = 634$, $I_3 = 374$, $I_4 = 44$, and $I_5 = 407$.

Let us consider the case when the first user accidentally types the value 280 (instead of the correct share 284). The solutions to all the systems corresponding to 3 users are presented next:

- System for $I_1\ I_2\ I_3$: 82056159
- System for $I_1\ I_2\ I_4$: 5096590
- System for $I_1\ I_2\ I_5$: 208839264
- System for $I_1\ I_3\ I_4$: 156788158
- System for $I_1\ I_3\ I_5$: 157683152
- System for $I_1\ I_4\ I_5$: 2387812
- System for $I_2\ I_3\ I_4$: 500000
- System for $I_2\ I_3\ I_5$: 500000
- System for $I_2\ I_4\ I_5$: 500000
- System for $I_3\ I_4\ I_5$: 500000

The set of all the 5 users is not consistent, therefore there are cheaters. The most frequent reconstructed secret is $S = 500000$ and, thus, the users 2, 3, 4, 5 are honest. All the systems in which the first user has taken part lead to different results and, therefore, the cheater (the first user) is easily identified.

The second type of attack is when the cheaters collaborate in order to obtain "better faked" shares but they do not see the shares of the honest users (all shares are released simultaneously). The bounds in this case are:

- Detection : $(c < k \ \wedge \ j \geq k+1) \ \vee \ (c \geq k \ \wedge \ j-c \geq k)$;
- Identification : $(c < k \ \wedge \ j - c \geq k+1) \ \vee$
  $(c \geq k \ \wedge \ j - c > c + k - 1)$.

The next example illustrates this type of attack, for the case $c < k$.

Example 5: (with artificially small parameters)
Let $n = 6$, $j = 6$, $c = 3$, $h = 3$, and $k = 4$. In this example we will show that we cannot always identify the cheaters. We can only detect cheating. Let us consider the following $(4, 6)$-Mignotte sequence: 719 , 727 , 733 , 739, 743, 751. We obtain $\alpha = 283146836831$ and $\beta = 412356827$. Let the secret be $S = 500000000$.

The dealer computes the shares of each user: $I_1 = 210$, $I_2 = 661$, $I_3 = 176$, $I_4 = 729$, $I_5 = 379$, and $I_6 = 722$.

Let us consider the case when the first three users are cheaters. They cannot reconstruct the secret only by themselves. They can only modify their shares. Suppose the new (faked) shares for the first three users are: $I_1 = 200$, $I_2 = 660$, and $I_3 = 170$.

The solutions to all the systems corresponding to 4 users are presented next:

- System for : $I_1\ I_2\ I_3\ I_4$: 93542325129
- System for : $I_1\ I_2\ I_3\ I_5$: 148332579076
- System for : $I_1\ I_2\ I_3\ I_6$: 41050962956
- System for : $I_1\ I_2\ I_4\ I_5$: 88134336431
- System for : $I_1\ I_2\ I_4\ I_6$: 159210759319
- System for : $I_1\ I_2\ I_5\ I_6$: 195326045915
- System for : $I_1\ I_3\ I_4\ I_5$: 26942450166
- System for : $I_1\ I_3\ I_4\ I_6$: 279320923710
- System for : $I_1\ I_3\ I_5\ I_6$: 113481864647
- System for : $I_1\ I_4\ I_5\ I_6$: 9571850194
- System for : $I_2\ I_3\ I_4\ I_5$: 138830066764
- System for : $I_2\ I_3\ I_4\ I_6$: 48254583494
- System for : $I_2\ I_3\ I_5\ I_6$: 2231452279
- System for : $I_2\ I_4\ I_5\ I_6$: 82146651746
- System for : $I_3\ I_4\ I_5\ I_6$: 163380946665

As you can see, there is no result that appears more than once. Therefore, we detect the presence of the cheaters, but we cannot identify them.

Interesting is the case when $c \geq k$. In this case the cheaters can reconstruct the secret by themselves. Moreover, they can create fake shares so that they will not be detected. This attack succeeds only if the number of cheaters is greater than the number of honest users ($c > h$). If $c \geq k \wedge j-c > c+k-1$, the cheaters, even if they can reconstruct to the secret, they cannot produce fake shares that will lead to a fake secret (because $h > c$). They can at most produce fake shares, combining with groups of $k-1$ honest users, but this is not enough. The most frequent reconstructed secret will be the one obtained by the honest users.

The next example illustrates the case $c \geq k$:

Example 6: (with artificially small parameters)

Let $n = 14$, $j = 12$, $c = 4$, $h = 8$, and $k = 3$. Let us consider the following $(3, 14)$-Mignotte sequence: 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811. We obtain $\alpha = 383148629$ and $\beta = 656099$. Let the secret be $S = 700000$.

The dealer computes the shares of each user: $I_1 = 413$, $I_2 = 626$, $I_3 = 718$, $I_4 = 167$, $I_5 = 94$, $I_6 = 68$, $I_7 = 532$, $I_8 = 641$, $I_9 = 210$, $I_{10} = 435$, $I_{11} = 357$, $I_{12} = 234$, $I_{13} = 215$, $I_{14} = 107$.

Suppose that only the first twelve users participate in the reconstruction phase and that the first four users are cheaters. The first user can create a fake share in combination with only a group of $k - 1 = 2$ honest users. Suppose that these users are the user 10 and the user 11. Suppose the first user changes his share to 222. The new secret obtained in association with the shares from user 10 and 11 is 192330565. Now, the other three cheaters will adjust their shares.

The new shares will be : $I_1 = 222$, $I_2 = 534$, $I_3 = 161$, $I_4 = 642$, $I_5 = 94$, $I_6 = 68$, $I_7 = 532$, $I_8 = 641$, $I_9 = 210$, $I_{10} = 435$, $I_{11} = 357$, and $I_{12} = 234$.

After solving all the $\binom{12}{3} = 220$ systems, the original secret will appear 56 times, the fake secret will appear 20 times, and the other results, only once. Therefore, the cheaters will be easily identified.

If $c > h$, the cheaters can give fake shares so that the honest users are lead to a wrong secret or, worse, they can be pointed out as cheaters (the cheaters can reconstruct S by themselves, and, thus, they have access to the shares of the honest users (see Example 7).

The third type of attack is that when the cheaters collaborate and, moreover, have access to the shares of the honest users. The bounds in this case are:

- Detection : $j - c \geq k$;
- Identification : $j \geq k + 1\ \wedge\ j - c > c + k - 1$.

The next example illustrates this type of attack:

Example 7: (with artificially small parameters)

We will consider the worst case scenario: the cheaters are not identified and the honest users reconstruct an invalid secret.

Let $n = 12$, $j = 9$, $c = 7$, $h = 2$, and $k = 3$. Let us consider the following $(3, 12)$-Mignotte sequence: 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, and 743. We obtain $\alpha = 301165481$ and $\beta = 549077$. Let the secret be $S = 750000$.

We now compute the shares of each user: $I_1 = 426$, $I_2 = 278$, $I_3 = 561$, $I_4 = 66$, $I_5 = 265$, $I_6 = 631$, $I_7 = 587$, $I_8 = 83$, $I_9 = 463$, $I_{10} = 141$, $I_{11} = 654$, and $I_{12} = 313$.

Let us consider the case when the first nine users participate in the reconstruction, the first seven users are cheaters. The cheaters (any 3 of them) can easily reconstruct the secret. The cheaters also know the shares of the honest users. For instance, the 7^{th} user (who is a cheater) computes a new share and a new secret with the help of the shares of the two honest users:

- $I_7 : 200 \qquad p_7 = 709$
- $I_8 : 83 \qquad p_8 = 719$
- $I_9 : 463 \qquad p_9 = 727$

By solving this system, the obtained secret (an invalid one) is 129337398 which is also between β and α. Now, the other cheaters just have to compute their new share in the following manner: $I_i = 129337398 \bmod p_i$, for all $i \in \{1, 2, 3, 4, 5, 6\}$. The new shares will be: $I_1 = 189$, $I_2 = 258$, $I_3 = 610$, $I_4 = 420$, $I_5 = 164$, $I_6 = 94$, $I_7 = 200$, $I_8 = 83$, and $I_9 = 463$. Now, all the systems will have the same solution, namely, 129337398. In this way, the cheaters are not detected, they obtain the correct secret and the honest users obtain an invalid secret.

V. Conclusions and Future Work

In this paper, we analyze the cheating detection and cheater identification problems for Mignotte and Asmuth-Bloom secret sharing schemes. We prove that the majority of the solutions for Shamir's scheme can be translated to these schemes and, moreover, there are some interesting specific solutions due to particularities of the reconstruction phase based on the (general) Chinese remainder theorem.

An interesting problem is preventing the cheaters from acquiring the secret. Indeed, let us suppose that, for instance, the secret is the launching code of a nuclear missile. If a group of cheaters have succeeded in reconstructing the correct code (for example, in the case $c \geq k$), it is irrelevant if the cheating is detected or if the cheaters are identified. It is too late -

the missile has been already launched. The simplest solution, suggested by Tompa and Wool [7], is to iterate the process of secret sharing on a sequence of m secrets that includes, besides the real secret S, some "dummy" secrets. The probability that the cheaters acquire the correct secret before being detected and identified is $\frac{1}{m}$. The main disadvantage of this method is that each user will receive m shares, one for each secret. In our future work, we will consider finding more efficient methods for preventing the cheaters from acquiring the secret in CRT-based secret sharing schemes.

REFERENCES

[1] M. Mignotte, "How to share a secret," in *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982*, ser. Lecture Notes in Computer Science, T. Beth, Ed., vol. 149. Springer-Verlag, 1983, pp. 371–375.

[2] C. A. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. IT-29, no. 2, pp. 208–210, 1983.

[3] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

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

[5] 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*. IEEE Press, 1985, pp. 383–395.

[6] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Communications of ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[7] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 2, pp. 133–138, 1988, (a preliminary version of this paper appeared in "Advances in Cryptology – CRYPTO '86", A. M. Odlyzko, ed., Lecture Notes in Computer Science 263 (1987), 261-265).

[8] K. Kaya and A. Selçuk, "Threshold cryptography based on Asmuth-Bloom secret sharing," *Information Sciences*, vol. 177, no. 19, pp. 4148–4160, 2007, (a preliminary version of this paper has been presented at ISCIS 2006).

[9] 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*. IEEE Computer Society Press, 2007, pp. 175–181.

[10] K. Kaya and A. Selçuk, "Robust threshold schemes based on the Chinese remainder theorem," in *Progress in Cryptology - AFRICACRYPT 2008*, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed., vol. 5023. Springer-Verlag, 2008, pp. 94–108.

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

[12] S. Iftene and D. Pasailă, "A CRT-based Solution to Yao's Millionaires' Problem," in *Proceedings of the 9th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2008*. IEEE Computer Society Press, 2008, pp. 189–192.

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

[14] O. Ore, "The general Chinese remainder theorem," *American Mathematical Monthly*, vol. 59, pp. 365–370, 1952.

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

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

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

[18] S. Iftene, "Secret Sharing Schemes with Applications in Security Protocols," "Al.I.Cuza" University of Iaşi, Faculty of Computer Science, Tech. Rep. TR 07-01, 2007, URL:http://www.infoiasi.ro/ tr/tr.pl.cgi.

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

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

[21] O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering with errors," *IEEE Transactions on Information Theory*, vol. IT-46, no. 4, pp. 1330–1338, 2000, (a preliminary version of this paper appeared in Proceedings of the thirty-first annual ACM symposium on Theory of computing (1999), 225-234).

[22] M. Quisquater, B. Preneel, and J. Vandewalle, "On the security of the threshold scheme based on the Chinese remainder theorem," in *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002*, ser. Lecture Notes in Computer Science, D. Naccache and P. Paillier, Eds., vol. 2274. Springer-Verlag, 2002, pp. 199–210.

[23] M. Carpentieri, A. D. Santis, and U. Vaccaro, "Size of shares and probability of cheating in threshold schemes," in *Advances in Cryptology - EUROCRYPT '93*, ser. Lecture Notes in Computer Science, T. Helleseth, Ed., vol. 765. Springer-Verlag, 1994, pp. 118–125.

[24] W. Ogata, K. Kurosawa, and D. Stinson, "Optimum secret sharing scheme secure against cheating," *SIAM Journal on Discrete Mathematics*, vol. 20, no. 1, pp. 79–95, 2006.

[25] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology - CRYPTO '99*, ser. Lecture Notes in Computer Science, M. Wiener, Ed., vol. 1666. Springer-Verlag, 1999, pp. 148–164.

[26] K. Kaya and A. Selçuk, "A verifiable secret sharing scheme based on the Chinese remainder theorem," in *Progress in Cryptology - INDOCRYPT 2008*, ser. Lecture Notes in Computer Science, D. Chowdhury, V. Rijmen, and A. Das, Eds., vol. 5365. Springer-Verlag, 2008, pp. 414–425.

[27] H. Ghodosi and J. Pieprzyk, "Cheating prevention in secret sharing," in *Information Security and Privacy, 5th Australasian Conference, ACISP 2000*, ser. Lecture Notes in Computer Science, E. Dawson, A. Clark, and C. Boyd, Eds., vol. 1841. Springer-Verlag, 2000, pp. 328–341.

[28] L. Harn and C. Lin, "Detection and identification of cheaters in (*t*,*n*) secret sharing scheme," *Designs, Codes and Cryptography*, vol. 52, no. 1, pp. 15–24, 2009, http://dx.doi.org/10.1007/s10623-008-9265-8.