A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem

Kamer Kaya* and Ali Aydın Selçuk

Department of Computer Engineering
Bilkent University
Ankara, 06800, Turkey
{kamer,selcuk}@cs.bilkent.edu.tr

Abstract. In this paper, we investigate how to achieve verifiable secret sharing (VSS) schemes by using the Chinese Remainder Theorem (CRT). We first show that two schemes proposed earlier are not secure by an attack where the dealer is able to distribute inconsistent shares to the users. Then we propose a new VSS scheme based on the CRT and prove its security. Using the proposed VSS scheme, we develop a joint random secret sharing (JRSS) protocol, which, to the best of our knowledge, is the first JRSS protocol based on the CRT.

Keywords: Verifiability, joint random secret sharing, Chinese Remainder Theorem, Asmuth-Bloom secret sharing scheme.

1 Introduction

Threshold cryptography deals with the problem of sharing a highly sensitive secret among a group of users so that only when a sufficient number of them come together can the secret be reconstructed. Well-known secret sharing schemes (SSS) in the literature include Shamir [18] based on polynomial interpolation, Blakley [2] based on hyperplane geometry, and Asmuth-Bloom [1] based on the Chinese Remainder Theorem (CRT).

A t-out-of-n secret sharing scheme contains two phases: In the *dealer phase*, the dealer shares a secret among n users. In the *combiner phase*, a coalition of size greater than or equal to t constructs the secret. We call a SSS *verifiable* if each user can verify the correctness of his share in the dealer phase and no user can lie about his share in the combiner phase. Hence, neither the dealer nor the users can cheat in a VSS scheme. Verifiable secret sharing schemes based on Shamir's SSS have been proposed in the literature [6,15]. These schemes have been extensively studied and used in threshold cryptography and secure multiparty computation [9,14,15].

* Supported by the Turkish Scientific and Technological Research Agency (TÜBİTAK) Ph.D. scholarship.

D.R. Chowdhury, V. Rijmen, and A. Das (Eds.): INDOCRYPT 2008, LNCS 5365, pp. 414–425, 2008.

There have been just two CRT-based VSS schemes by Iftene [10] and Qiong et al. [16]. In this paper, we show that these schemes are vulnerable to attacks where a corrupted dealer can distribute *inconsistent* shares without detection such that different coalitions will obtain different values for the secret. To the best of our knowledge, these are the only VSS schemes that have been proposed so far based on the CRT.

A typical application of a VSS scheme is the joint random secret sharing (JRSS) primitive frequently used in threshold cryptography [9,11,14,15]. In a JRSS scheme, all players act as a dealer and jointly generate and share a random secret. So far, there have been no JRSS protocols proposed based on the CRT.

In this paper, we first show why existing attempts for a CRT-based verifiable secret sharing scheme fail by attacks on the existing schemes. We then propose a VSS scheme based on the Asmuth-Bloom secret sharing [1] and using this VSS scheme, we propose a JRSS scheme. To the best of our knowledge the VSS and JRSS schemes we propose are the first secure CRT-based schemes of their kind in the literature.

The rest of the paper is organized as follows: In Section 2, we describe the Asmuth-Bloom SSS in detail and introduce the notation we followed in the paper. The VSS schemes proposed in [10,16] are described Section 3 and their flaws are analyzed. After presenting our VSS scheme in Section 4, we propose the joint random scheme in Section 5. Section 6 concludes the paper.

2 Asmuth-Bloom Secret Sharing Scheme

The Asmuth-Bloom SSS [1] shares a secret d among n parties by modular arithmetic such that any t users can reconstruct the secret by the CRT. The scheme presented in Figure 1 is a slightly modified version by Kaya and Selcuk [12] in order to obtain better security properties.

According to the Chinese Remainder Theorem, y can be determined uniquely in $\mathbb{Z}_{M_S}$ since $y < M \leq M_S$ for any coalition S of size t.

Kaya and Selcuk [12] showed that the Asmuth-Bloom version presented here is *perfect* in the sense that no coalition of size smaller than t can obtain any information about the secret.

Quisquater et al. [17] showed that when m_is are chosen as consecutive primes, the scheme has better security properties. In this paper, we will also assume that all m_is are prime and we will choose them such that $p_i = 2m_i + 1$ is also a prime for $1 \leq i \leq n$. The notation used in the paper is summarized in Table 1.

For the protocols in this paper, we assume that private channels exist between the dealer and users. The share of each user is sent via these private channels; hence no one except the user himself knows the share. Besides, we assume that a broadcast channel exists and if some data is broadcast each user will read the same value. Hence an adversary cannot send two different values to two different users for a broadcast data.

– *Dealer Phase:* To share a secret d among a group of n users, the dealer does the following:
  - A set of relatively prime integers $m_0 < m_1 < \ldots < m_n$ are chosen where m_0 is a prime and
$$\prod_{i=1}^{t} m_i > {m_0}^2 \prod_{i=1}^{t-1} m_{n-i+1}. \quad (1)$$
  - Let M denote $\prod_{i=1}^{t} m_i$. The dealer computes $y = d + Am_0$ where A is a positive integer generated randomly subject to the condition that $0 \leq y < M$.
  - The share of the ith user, $1 \leq i \leq n$, is $y_i = y \bmod m_i$.
– *Combiner Phase:* Let S be a coalition of t users gathered to construct the secret. Let M_S denote $\prod_{i \in S} m_i$.
  - Let $M_{S\setminus\{i\}}$ denote $\prod_{j \in S, j \neq i} m_j$ and $M'_{S,i}$ be the multiplicative inverse of $M_{S\setminus\{i\}}$ in $\mathbb{Z}_{m_i}$, i.e., $M_{S\setminus\{i\}} M'_{S,i} \equiv 1 \pmod{m_i}$. First, the ith user computes
$$u_i = y_i M'_{S,i} M_{S\setminus\{i\}} \bmod M_S.$$
  - The users first compute
$$y = \left(\sum_{i \in S} u_i \right) \bmod M_S$$
and then obtain the secret d by computing
$$d = y \bmod m_0.$$

Fig. 1. Asmuth-Bloom secret sharing scheme

Table 1. Notations

Notation	Explanation
n	The number of users.
t	The threshold, the minimum number of users required to construct the secret.
d	The secret to be shared.
m_0	A prime; specifies the domain of $d \in \mathbb{Z}_{m_0}$.
$m_i : 1 \leq i \leq n$	The prime modulus for user i.
$p_i : 1 \leq i \leq n$	A safe prime, $2m_i + 1$.
P	$\prod_{i=1}^{n} p_i$.
y	$d + Am_0$, where A is a random number.
M	The domain of $y \in \mathbb{Z}_M$.
$y_i : 1 \leq i \leq n$	$y \bmod m_i$, the share of user i.
$E(y)$	The commitment value of an integer y.
S	A coalition of users.
M_S	The modulus of coalition S, $\prod_{i \in S} m_i$.

3 Analysis of the Existing CRT-Based VSS Schemes

There have been two different approaches to achieve VSS by a CRT-based secret sharing scheme. The first one, proposed by Iftene [10], obtains a VSS scheme from Mignotte's SSS [13] which is another CRT-based SSS similar to Asmuth-Bloom. Here, we adapt Iftene's approach to the Asmuth-Bloom SSS. The scheme is given in Figure 2.

If the dealer is honest and the discrete logarithm problem is hard, the scheme in Figure 2 is secure against a dishonest user because the verification data, ${g_i}^y \bmod p_i$, can be used to detect an invalid share from a corrupted user in the first step of the combiner phase.

However, if the dealer is dishonest, he can mount an attack despite the additional verification data above: Let y be an integer and $y_i = y \bmod m_i$ for $1 \leq i \leq n$. In the combiner phase of Asmuth-Bloom SSS, the minimum number of users required to obtain the secret is t; hence, $y = d + Am_0$ must be smaller than $M = \prod_{i=1}^{t} m_i$. Note that, to reconstruct the secret d, each coalition S must first compute $y \bmod M_S$ where $M_S \geq M$. If the dealer distributes the shares for some $y > M$, then y will be greater than M_S for some coalition S of size t. Hence, S may not compute the correct y value and the correct secret d even though $y_i = y \bmod m_i$ for all i. Therefore, the given VSS scheme cannot detect this kind of inconsistent shares from the dealer where different coalitions end up with different d values. The same problem also arises in Iftene's original VSS scheme [10].

- *Dealer Phase:* To share a secret $d \in \mathbb{Z}_{m_0}$ among a group of n users with verifiable shares, the dealer does the following:
  1. Use the dealing procedure of the Asmuth-Bloom SSS to obtain the shares $y_i = y \bmod m_i$ for each $1 \leq i \leq n$ where $y = d + Am_0 < M$. Choose m_is such that each $p_i = 2m_i + 1$ is also a prime.
  2. Let $g_i \in \mathbb{Z}_{p_i}^*$ be an element of order m_i. The dealer sends y_i to the ith user privately and makes the values p_i, g_i and $z_i = g_i^y \bmod p_i$ public for $1 \leq i \leq n$. The ith user can find whether his share is valid or not by checking
$$z_i \stackrel{?}{\equiv} {g_i}^{y_i} \bmod p_i. \tag{2}$$
- *Combiner Phase:* Let S be a coalition gathered to construct the secret.
  1. The share y_i of user $i \in S$ can be verified by the other users in S by the verification equation $z_i \stackrel{?}{\equiv} {g_i}^{y_i} \bmod p_i$.
  2. If all shares are valid then the coalition S can obtain the secret d: First, the ith user computes
$$u_i = y_i M'_{S,i} M_{S\setminus\{i\}} \bmod M_S.$$
  3. Then the users compute $y = \left(\sum_{i \in S} u_i\right) \bmod M_S$ and obtain the secret d by computing $d = y \bmod m_0$.

Fig. 2. Iftene's CRT-based VSS extension

– *Dealer Phase:* To share a secret $d \in \mathbb{Z}_{m_0}$ among a group of n users with verifiable shares, the dealer does the following:
  1. Use the dealing procedure of the Asmuth-Bloom SSS to obtain the shares $y_i = y \bmod m_i$ for all $1 \leq i \leq n$ where $y = d + Am_0 < M$.
  2. Let p, q be primes such that $q|(p-1)$. Construct the unique polynomial $f(x) \in \mathbb{Z}_q[x]$ where $deg(f(x)) = n-1$ and $f(m_i) = y_i$. Construct a random polynomial $f'(x) \in \mathbb{Z}_q[x]$ where $deg(f'(x)) = n-1$. Let $z_i = f'(m_i)$ for all $1 \leq i \leq n$.
  3. Let $g \in \mathbb{Z}_p$ with order q, h be a random integer in the group generated by g and $E(a,b) = g^a h^b \bmod p$ for inputs $a, b \in \mathbb{Z}_q^*$. Compute
  $$E_i = E(f_i, f_i') = g^{f_i} h^{f_i'} \bmod p,$$
  where f_i and f_i' are the $(i-1)$th coefficients of $f(x)$ and $f'(x)$, respectively, for all $1 \leq i \leq n$. Broadcast E_is to all users.
  4. Send (y_i, z_i) secretly to the ith user for all $1 \leq i \leq n$.
  5. To verify the validity of his share, each user checks
  $$E(y_i, z_i) \stackrel{?}{\equiv} \prod_{j=1}^{n} {E_j}^{{m_i}^{j-1}} \equiv \prod_{j=1}^{n} g^{f_j {m_i}^{j-1}} \prod_{j=1}^{n} h^{f_j' {m_i}^{j-1}} \equiv g^{y_i} h^{z_i} \bmod p. \quad (3)$$

– *Combiner Phase:* Let S be a coalition gathered to construct the secret.
  1. The share (y_i, z_i) of user $i \in S$ can be verified by the other users in S with the verification equality $E(y_i, z_i) \stackrel{?}{\equiv} \prod_{j=1}^{n} {E_j}^{{m_i}^{j-1}} \bmod p$.
  2. If all shares are valid; the coalition S can obtain the secret d by using the reconstruction procedure described in Section 2.

Fig. 3. Qiong et al.'s CRT-based VSS extension

Another VSS scheme based on Asmuth-Bloom secret sharing was proposed by Qiong et al. [16]. Their approach is similar to the VSS of Pedersen [15] based on Shamir's SSS. Their scheme is given in Figure 3.

As the scheme shows, Qiong et al. treated the shares of Asmuth-Bloom SSS as points on a degree-$(n-1)$ polynomial and adopted the approach of Pedersen by evaluating the polynomial in the exponent to verify the shares. If the dealer is honest, the scheme in Figure 3 is secure because the verification data can be used to detect an invalid share from a corrupted user in the first step of the combiner phase.

However, similar to the attack on Iftene's VSS scheme, if the dealer uses some $y > M$ and computes the verification data by using the shares $y_i = y \bmod m_i$, $1 \leq i \leq n$, the verification equation (3) holds for each user. But, for a coalition S where $y > M_S$, the coalition S cannot compute the correct y value and the secret d.

Note that Iftene's VSS scheme uses a separate verification data for each user; hence even if all the verification equations hold, the secret can still be inconsistent for different coalitions. Quiong et al.'s VSS scheme generates a polynomial $f(x)$ from the shares as in Feldman's and Pedersen's VSS schemes. This polynomial

is used to check all verification equations. But Asmuth-Bloom SSS depends on the CRT and unlike Shamir's SSS, here f is not inherently related to the shares. Hence, even if all the equations hold, the shares can still be inconsistent as we have shown.

4 Verifiable Secret Sharing with Asmuth-Bloom SSS

As discussed in Section 3, existing CRT-based VSS schemes in the literature cannot prevent a dealer from cheating. To solve this problem, we will use a range proof technique originally proposed by Boudot [4] and modified by Cao et al. [5].

4.1 Range Proof Techniques

Boudot [4] proposed an efficient and non-interactive technique to prove that a committed number lies within an interval. He used the Fujisaki-Okamoto commitment scheme [8], where the commitment of a number y with bases (g, h) is computed as

$$E = E(y, r) = g^y h^r \bmod N$$

where g is an element in $\mathbb{Z}_N^*$, h is an element of the group generated by g, and r is a random integer. As proved in [4,8], this commitment scheme is statistically secure assuming the factorization of N is not known.

After Boudot, Cao et al. [5] applied the same proof technique with a different commitment scheme

$$E = E(y) = g^y \bmod N$$

to obtain shorter range proofs. Here, we will use Cao et al.'s non-interactive range-proof scheme as a black box. For further details, we refer the user to [4,5]. For our needs, we modified the commitment scheme as

$$E = E(y) = g^y \bmod PN$$

where $P = \prod_{i=1}^{n} p_i$ and N is an RSA composite whose factorization is secret. Note that even if $\phi(P)$ is known, $\phi(PN)$ cannot be computed since $\phi(N)$ is secret. Throughout the section, we will use $\mathrm{RngPrf}(E(y), M)$ to denote the range proof that a secret integer y committed with $E(y)$ is in the interval $[0, M)$.

4.2 A CRT-Based VSS Scheme

In our VSS scheme, the RSA composite N is an integer generated jointly by the users and the dealer where its prime factorization is not known. Such an integer satisfying these constraints can be generated by using the protocols proposed for shared RSA key generation [3,7] at the beginning of the protocol. Note that we do not need the private and the public RSA exponents in our VSS scheme as in the original protocols [3,7]; hence those parts of the protocols can be omitted.

Let $g_i \in \mathbb{Z}_{p_i}^*$ be an element of order m_i. Let $P = \prod_{i=1}^{n} p_i$ and

$$g = \left(\sum_{i=1}^{n} g_i \frac{P}{p_i} P_i' \right) \bmod P \tag{4}$$

- *Dealer Phase:* To share a secret $d \in \mathbb{Z}_{m_0}$ among a group of n users with verifiable shares, the dealer does the following:
  1. Use the dealing procedure of the Asmuth-Bloom secret sharing scheme described in Section 2 to obtain the shares
  $$y_i = y \bmod m_i$$
  for each $1 \leq i \leq n$ where $y = d + Am_0 < M = \prod_{i=1}^{t} m_i$. Note that the m_is are large primes where $p_i = 2m_i + 1$ is also a prime for $1 \leq i \leq n$.
  2. Let N be an integer whose prime factorization is not known by the users and the dealer. Compute $E(y) = g^y \bmod PN$. Send y_i to the ith user secretly for all $1 \leq i \leq n$ and broadcast $(E(y), \text{RngPrf}(E(y), M))$.
  3. The ith user checks
  $$g_i{}^{y_i} \stackrel{?}{\equiv} E(y) \bmod p_i \tag{5}$$
  to verify $y_i = y \bmod m_i$. Then he checks the validity of the range proof to verify $y < M$.
- *Combiner Phase:* Let S be a coalition gathered to construct the secret.
  1. The share y_i of user $i \in S$ can be verified by the other users in S with the verification equality $g_i{}^{y_i} \stackrel{?}{\equiv} E(y) \bmod p_i$.
  2. If all shares are valid, the participants can obtain the secret d by using the reconstruction procedure described in Section 2. Otherwise, the corrupted users are disqualified.

Fig. 4. CRT-based verifiable secret sharing scheme

where $P_i' = \left(\frac{P}{p_i}\right)^{-1} \bmod p_i$ for all $1 \leq i \leq n$, i.e., g is the unique integer in $\mathbb{Z}_P$ satisfying $g \equiv g_i \bmod p_i$ for all i. Our VSS scheme is described in Figure 4.

4.3 Analysis of the Proposed VSS Scheme

We analyze the correctness of the scheme and its security against passive and active attackers below:

Correctness. Aside from the verification equation, the scheme uses the original Asmuth-Bloom scheme. Hence, for correctness, we only need to show that when the dealer and the users are honest, the verification equations in the dealer and combiner phases hold. Note that, the condition $y < M$ is checked in Step 3 of the dealer phase by using $\text{RngPrf}(E(y), M))$. Furthermore, for a valid share y_i,

$$\begin{aligned} E(y) \bmod p_i &= g^y \bmod PN \bmod p_i = g^y \bmod p_i \\ &= g_i{}^y \bmod p_i = g_i{}^{y_i} \bmod p_i. \end{aligned}$$

Hence if the dealer and the users behave honestly, the verification equation holds and the ith user verifies that his share is a residue modulo m_i of the integer $y < M$ committed with $E(y)$.

Security. For the security analysis, we will first show that the underlying SSS is perfect as proved by Kaya et al. [12], i.e., no coalition of size smaller than t can obtain any information about the secret.

Theorem 1 (Kaya and Selcuk [12]). *For a passive adversary with $t-1$ shares in the VSS scheme, every candidate for the secret is equally likely, i.e., the probabilities* $\Pr(d = d')$ *and* $\Pr(d = d'')$ *are approximately equal for all* $d', d'' \in \mathbb{Z}_{m_0}$.

Proof. Suppose the adversary corrupts $t-1$ users and just observes the inputs and outputs of the corrupted users without controlling their actions, i.e., the adversary is honest in user actions but curious about the secret. Let S' be the adversarial coalition of size $t-1$, and let y' be the unique solution for y in $Z_{M_{S'}}$. According to (1), $M/M_{S'} > m_0$, hence $y' + jM_{S'}$ is smaller than M for $j < m_0$. Since $\gcd(m_0, M_{S'}) = 1$, all $(y' + jM_{S'}) \bmod m_0$ are distinct for $0 \leq j < m_0$, and there are m_0 of them. That is, d can be any integer from $\mathbb{Z}_{m_0}$. For each value of d, there are either $\lfloor M/(M_{S'}m_0) \rfloor$ or $\lfloor M/(M_{S'}m_0) \rfloor + 1$ possible values of y consistent with d, depending on the value of d. Hence, for two different integers in $\mathbb{Z}_{m_0}$, the probabilities of d equals these integers are almost equal. Note that $M/(M_{S'}m_0) > m_0$ and given that $m_0 \gg 1$, all d values are approximately equally likely.

Besides the shares, the only additional information a corrupted user can obtain is $E(y)$ and $\mathrm{RngPrf}(E(y), M)$. Given that the discrete logarithm problem is hard and Cao et al.'s range proof technique is computationally secure, the proposed VSS scheme is also computationally secure. □

The shares distributed by a dealer are said to be inconsistent if different coalitions of size at least t obtain different values for the secret. The following theorem proves that the dealer cannot distribute shares inconsistent with the secret.

Theorem 2. *A corrupted dealer cannot cheat in the VSS scheme without being detected. I.e., if the shares are inconsistent with the secret d then at least one verification equation does not hold.*

Proof. Let $U = \{1, \ldots, n\}$ be the set of all users. If the shares are inconsistent, for two coalitions S and S' with $|S|, |S'| \geq t$,

$$\left(\sum_{i \in S} y_i M'_{S,i} M_{S \setminus \{i\}} \right) \bmod M_S \neq \left(\sum_{i \in S'} y_i M'_{S',i} M_{S' \setminus \{i\}} \right) \bmod M_{S'}.$$

hence,

$$y = \left(\sum_{i=1}^{n} y_i M'_{U,i} M_{U \setminus \{i\}} \right) \bmod M_U > M,$$

because we need at least $t+1$ congruences to hold. If this is true then the dealer cannot provide a valid range proof $\mathrm{RngPrf}(E(y), M)$. So, when a user tries to verify that $y < M$, the range proof will not be verified.

If the dealer tries to use a different $y' \neq y$ value in the commitment $E(y')$ and generates a valid proof $\mathrm{RngPrf}(E(y'), M)$, the verification equation (5) will not hold for some user i. Hence, the VSS scheme guarantees that the n distributed shares are consistent and they are residues of some number $y < M$. □

Theorem 3. *A user cannot cheat in the VSS scheme without being detected; i.e., if a share given in the combiner phase is inconsistent with the secret, then the verification equation does not hold.*

Proof. When a user i sends an incorrect share $y_i' \neq y_i = y \bmod m_i$ in the combiner phase, the verification equation

$$E(y) \stackrel{?}{\equiv} {g_i}^{y_i} \bmod p_i$$

will not hold because $E(y) = g^y \bmod PN$, $p_i | P$ and since the order of $g_i \in \mathbb{Z}_{p_i}$ is m_i, the only value satisfying the verification equation is y_i. □

5 Joint Random Secret Sharing

Joint random secret sharing (JRSS) protocols enable a group of users to jointly generate and share a secret where a trusted dealer is not available. Although there have been JRSS schemes based on Shamir's SSS, so far no JRSS scheme has been proposed based on CRT. Here we describe a JRSS scheme based on the VSS scheme in Section 4. We first modify (1) used in the Asmuth-Bloom secret sharing scheme in Section 2 as

$$\prod_{i=1}^{t} m_i > n {m_0}^2 \prod_{i=1}^{t-1} m_{n-i+1}. \tag{6}$$

We also change the definition of M as $M = \left\lfloor (\prod_{i=1}^{t} m_i)/n \right\rfloor$. The proposed JRSS scheme is given in Figure 5.

5.1 Analysis of the Proposed JRSS Scheme

Correctness. Observe that when all users behave honestly, the JRSS scheme works correctly. Let $y = \sum_{i \in \mathcal{B}} y^{(i)}$. It is easy to see that $y < \prod_{i=1}^{t} m_i$ since $y^{(i)} < M$ for all $i \in \mathcal{B}$, where $|\mathcal{B}| \leq n$ and $M = \left\lfloor (\prod_{i=1}^{t} m_i)/n \right\rfloor$. One can see that $y_j = y \bmod m_j$ for all $j \in \mathcal{B}$ by checking

$$y \bmod m_j = \left(\sum_{i \in \mathcal{B}} y_j^{(i)} \right) \bmod m_j = y_j \bmod m_j = y_j.$$

Hence, each y_i satisfies $y_i = y \bmod m_i$ and $y < \prod_{i=1}^{t} m_i$; so, y can be constructed with t shares.

For correctness of the verification procedure in (7), one can observe that

$$\left(\prod_{i \in \mathcal{B}} E(y^{(i)}) \right) \equiv g^{\sum_{i \in \mathcal{B}} y^{(i)}} \equiv g^y \equiv {g_i}^{y_i} \pmod{p_i}.$$

– *Dealing Phase:* To jointly share a secret $d \in \mathbb{Z}_{m_0}$ the users do the following:
  1. Each user chooses a secret $d_i \in \mathbb{Z}_{m_0}$ and shares it by using the VSS scheme as follows: He first computes
  $$y^{(i)} = d_i + A_i m_0$$
  where $y^{(i)} < M = \lfloor (\prod_{i=1}^{t} m_i)/n \rfloor$. Then the secret for the jth user is computed as
  $$y_j^{(i)} = y^{(i)} \bmod m_j.$$
  He sends $y_j^{(i)}$ to user j secretly for all $1 \leq i \leq n$ and broadcasts $(E(y^{(i)}), \mathrm{RngPrf}(E(y^{(i)}), M))$.
  2. After receiving shares the jth user verifies them by using the verification procedure in (5). Let $\mathcal{B}$ be the set of users whose shares are verified correctly. The jth user computes his overall share
  $$y_j = \left(\sum_{i \in \mathcal{B}} y_j^{(i)} \right) \bmod m_j$$
  by using the verified shares.
– *Combiner Phase:* Let S be a coalition of t users gathered to construct the secret.
  1. The share y_i of user $i \in S$ can be verified by the other users in S with the verification equation,
  $$g^{y_i} \stackrel{?}{\equiv} \left(\prod_{j \in \mathcal{B}} E(y^{(j)}) \right) \bmod p_i. \tag{7}$$
  2. If all shares are valid, the participants obtain the secret $d = \left(\sum_{i \in \mathcal{B}} d_i \right) \bmod m_0$ by using the reconstruction procedure described in Section 2.

Fig. 5. CRT-based joint random secret sharing scheme.

Security. We will show that no coalition of size smaller than t can obtain any information about the secret.

Theorem 4. *For a passive adversary with $t-1$ shares in the JRSS scheme, every candidate for the secret is equally likely. I.e., the probabilities* $\Pr(d = d')$ *and* $\Pr(d = d'')$ *are approximately equal for all* $d', d'' \in \mathbb{Z}_{m_0}$.

Proof. Suppose the adversary corrupts $t-1$ users and just observes the inputs and outputs of the corrupted users without controlling their actions, i.e., the adversary is honest in user actions but curious about the secret. Let S' be the coalition of the users corrupted by the adversary. The shares are obtained when each user shares his partial secret d_i, i.e., the adversary will obtain $t-1$ share for each d_i. We will prove that the probabilities that $d_i = d_i'$ and $d = d_i''$ are almost equal for two secret candidates $d_i', d_i'' \in \mathbb{Z}_{m_0}$.

We already proved that the Asmuth-Bloom SSS described in Section 2 is perfect with equation (1). By using the shares of S', the adversary can compute $y'^{(i)} = y^{(i)} \bmod M_{S'}$. But even with these shares, there are $\frac{M}{M_{S'}}$ consistent $y^{(i)}$s

which are smaller than M and congruent to $y'^{(i)}$ modulo $M_{S'}$. By replacing (1) with (6) and changing the definition of M to $\left\lfloor (\prod_{i=1}^{t} m_i)/n \right\rfloor$, the value of the ratio

$$\frac{M}{M_{S'}} > \frac{M}{\prod_{i=1}^{t-1} m_{n-i+1}} \approx \frac{\prod_{i=1}^{t} m_i}{n \prod_{i=1}^{t-1} m_{n-i+1}}$$

is greater than ${m_0}^2$. Hence, even with $t-1$ shares, there are still ${m_0}^2$ candidates for each $y^{(i)}$ which is used to share the secret d_i. Since $\gcd(m_0, M_{S'}) = 1$, there are approximately m_0 $y^{(i)}$s, consistent with a secret candidate d'_i. Hence, for a secret candidate d'_i the probability that $d_i = d'_i$ is approximately equal to $\frac{1}{m_0}$ and the perfectness of the scheme is preserved.

Besides the shares, the only other information the adversary can observe is the commitments and range proofs. Given that the discrete logarithm problem is hard and Cao et al.'s range proof scheme is secure, the proposed JRSS scheme is also computationally secure. □

A corrupted user cannot cheat in the JRSS scheme without being detected. Since we are using a VSS scheme, while user i is sharing his partial secret d_i, the conditions of the Asmuth-Bloom SSS must be satisfied as proved in Theorem 2. Furthermore, if user i sends an incorrect share in the combiner phase, the verification equation (7) will not hold. As a result, we can say that the JRSS scheme is secure for up to $t-1$ corrupted users and no user can cheat in any phase of the scheme.

6 Conclusion

In this paper, a CRT-based verifiable secret sharing scheme is proposed. We showed that previous solutions for this problem did not guarantee the consistency of the shares. A secure JRSS scheme based on Asmuth-Bloom scheme is also proposed as a practical application of a VSS scheme. To the best of our knowledge, the proposed schemes are the first CRT-based secure VSS and JRSS schemes in the literature.

References

1. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Information Theory 29(2), 208–210 (1983)
2. Blakley, G.: Safeguarding cryptographic keys. In: AFIPS 1979, pp. 313–317 (1979)
3. Boneh, D., Franklin, M.: Efficient generation of shared RSA keys. J. ACM 48(4), 702–722 (2001)
4. Boudot, F.: Efficient proofs that a committed number lies in an interval. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 431–444. Springer, Heidelberg (2000)
5. Cao, Z., Liu, L.: Boudot's range-bounded commitment scheme revisited. In: Qing, S., Imai, H., Wang, G. (eds.) ICICS 2007. LNCS, vol. 4861, pp. 230–238. Springer, Heidelberg (2007)

6. Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: FOCS 1987: IEEE Symposium on Foundations of Computer Science, pp. 427–437 (1987)
7. Frankel, Y., MacKenzie, P.D., Yung, M.: Robust and efficient distributed RSA-Key generation. In: STOC 1998: ACM Symposium on Theory of Computing, pp. 663–672. ACM Press, New York (1998)
8. Fujisaki, E., Okamoto, T.: Statistical zero knowledge protocols to prove modular polynomial relations. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 16–30. Springer, Heidelberg (1997)
9. Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Robust threshold DSS signatures. Information and Computation 164(1), 54–84 (2001)
10. Iftene, S.: Secret sharing schemes with applications in security protocols. Technical report, University Alexandru Ioan Cuza of Iaşi, Faculty of Computer Science (2007)
11. Ingemarsson, I., Simmons, G.J.: A protocol to set up shared secret schemes without the assistance of a mutually trusted party. In: EUROCRYPT 1991, pp. 266–282. Springer, Heidelberg (1990)
12. Kaya, K., Selçuk, A.A.: Threshold cryptography based on Asmuth-Bloom secret sharing. Information Sciences 177(19), 4148–4160 (2007)
13. Mignotte, M.: How to share a secret? In: Proc. of the Workshop on Cryptography, pp. 371–375. Springer, Heidelberg (1983)
14. Pedersen, T.P.: Distributed provers with applications to undeniable signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 221–242. Springer, Heidelberg (1991)
15. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
16. Qiong, L., Zhifang, W., Xiamu, N., Shenghe, S.: A non-interactive modular verifiable secret sharing scheme. In: ICCCAS 2005: International Conference on Communications, Circuits and Systems, pp. 84–87. IEEE, Los Alamitos (2005)
17. Quisquater, M., Preneel, B., Vandewalle, J.: On the security of the threshold scheme based on the Chinese Remainder Theorem. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 199–210. Springer, Heidelberg (2002)
18. Shamir, A.: How to share a secret? Comm. ACM 22(11), 612–613 (1979)