RESEARCH ARTICLE

Verifiable secret sharing based on the Chinese remainder theorem

Lein Harn¹, Miao Fuyou² and Chin-Chen Chang³, ⁴*

¹ Department of Computer Science and Electrical Engineering, University of Missouri, Kansas City, MO, U.S.A.
² School of Computer Science and Technology, University of Science & Technology of China, China
³ Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan
⁴ Department of Computer Science and Information Engineering, Asia University, Taichung 413, Taiwan

ABSTRACT

A (t,n) secret sharing scheme (SS) enables a dealer to divide a secret into n shares in such a way that (i) the secret can be recovered successfully with t or more than t shares, and (ii) the secret cannot be recovered with fewer than t shares. A verifiable secret sharing scheme (VSS) has been proposed to allow shareholders to verify that their shares are generated by the dealer consistently without compromising the secrecy of both shares and the secret. So far, there is only one secure Chinese remainder theorem-based VSS using the RSA assumption. We propose a Chinese remainder theorem-based VSS scheme without making any computational assumptions, which is a simple extension of Azimuth–Bloom (t,n) SS. Just like the most well-known Shamir’s SS, the proposed VSS is unconditionally secure. We use a linear combination of both the secret and the verification secret to protect the secrecy of both the secret and shares in the verification. In addition, we show that no information is leaked when there are fewer than t shares in the secret reconstruction. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS

Chinese remainder theorem; secret sharing scheme; verifiable secret sharing; t-threshold consistency

*Correspondence

Chin-Chen Chang, Department of Computer Science and Information Engineering, Asia University, Taichung 413, Taiwan.
E-mail: alan3c@gmail.com

1. INTRODUCTION

Secret sharing schemes (SS) were originally introduced by both Blakley [1] and Shamir [2] independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literature. SS has become one of the most basic tools in cryptographic research. In Shamir’s (t,n) SS, a secret s is divided into n shares by a dealer. The secret is shared among n shareholders in such a way that (i) the secret can be reconstructed with any t or more than t shares, and (ii) the secret cannot be obtained with fewer than t shares. Shamir’s (t,n) SS is based on polynomial and is unconditionally secure. There are other types of threshold SSs. For example, Blakely’s scheme [1] is based on the geometry; Mignotte’s scheme [3] and Azimuth–Bloom’s scheme [4] are based on the Chinese remainder theorem (CRT).

Shamir’s (t, n) SS scheme is based on a linear polynomial and is unconditionally secure. The security of cryptographic schemes can be classified into two types, computational security and unconditional security. Computational security assumes that the adversary has bounded computing power that limits the adversary solving hard mathematical problem, such as factoring a large composite integer into two primes. Unconditional security means that the security holds even if the adversary has unbounded computing power. Research on developing cryptographic schemes with unconditional security has received wide attention recently.

In 1985, Chor et al. [5] presented the notion of verifiable secret sharing scheme (VSS). In a VSS, shareholders are able to verify that their shares are generated by the dealer consistently without compromising the secrecy of both shares and the secret. There are many research papers on the VSS in the literature. According to security assumptions, we can classify VSSs into two different types, schemes are computationally secure and schemes are unconditionally secure. For example, Feldman [6] and Pedersen [7] developed non-interactive VSSs using cryptographic commitments. The security of Feldman’s VSS is based on the hardness of solving the discrete logarithm, whereas the privacy of Pedersen’s VSS is unconditionally secure, and the correctness of the shares is based on a computational assumption. Benaloh [8] proposed an interactive VSS, and the security is unconditionally secure. Stinson et al. [9] proposed an
unconditionally secure VSS, and later, Patra et al. [10] proposed a generalized VSS.

There are many papers on the polynomial-based VSSs, but only a few papers are focused on the CRT-based VSSs. Ifene [11] and Qiong et al. [12] have proposed two CRT-based VSSs. However, Kaya et al. [13] pointed out that both schemes cannot prevent a corrupted dealer to distribute inconsistent shares to shareholders. They have proposed a CRT-based VSS, which uses a range proof technique proposed by Boudot [8]. The security of their VSS is based on the RSA assumption [14]. In addition, in 2009, Sarkar et al. [15] have proposed a CRT-based RSA-threshold cryptography for a mobile ad hoc network, and in 2011, Lu et al. have proposed a secret key distributed storage scheme [16] based on CRT-VSS and trusted computing technology. In this paper, we introduce notions of \( t \)-threshold range and \( t \)-threshold consistency. We show that shares generated by a secret selected in the \( t \)-threshold range satisfy the security requirements of an \((t,n)\) SS. We propose a CRT-based VSS scheme, which is a simple extension of Azimuth–Bloom \((t,n)\) SS. Because Azimuth–Bloom \((t,n)\) SS is a perfect SS (i.e., like Shamir’s \((t,n)\) SS in which no information is leaked when there are fewer than \( t \) shares), the security of our proposed VSS is also perfectly secure. We use multiple verification secrets to verify the \( t \)-threshold consistency of shares without revealing the secrecy of both the secret and shares. By examining the revealed sum and difference of the secret and verification secrets, we can conclude that shares are generated by the secret in the \( t \)-threshold range. The proposed VSS is unconditionally secure, and the secret reconstruction is the same as the Azimuth–Bloom’s SS that is perfectly secret.

The rest of this paper is organized as follows. In the next section, we introduce some preliminaries including the CRT, Mignotte’s and Azimuth–Bloom’s \((t,n)\) SSs based on the CRT. In Section 3, we introduce the model of our proposed VSS including definitions, entities, informal model, and properties. Our VSS is introduced in Section 4. In Section 5, we include security analysis and performance. Conclusion is given in Section 6.

2. PRELIMINARIES

2.1. Chinese remainder theorem [17]

Given following system of equations as

\[ x = s_1 \mod p_1; \]
\[ x = s_2 \mod p_2; \]
\[ \vdots \]
\[ x = s_t \mod p_t, \]

there is one unique solution as

\[ x = \sum_{i=1}^{t} \frac{N}{p_i} y_i s_i \mod N, \]

where \( \frac{N}{p_i} y_i \mod p_i = 1 \), and \( N = p_1 \cdot p_2 \cdot \ldots \cdot p_t \), if all moduli are pairwise coprime (i.e., \( \gcd(p_i, p_j) = 1 \), for every \( i \neq j \)).

2.2. Review of Mignotte’s \((t,n)\) SS

Share generation

A sequence consisting of pairwise coprime positive integers, \( p_1 < p_2 < \ldots < p_n \), with \( p_{n-1+r} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_n \), where \( p_i \) is the public information associated with each shareholder, \( U_i \). For this given sequence, the dealer chooses the secret \( s \) as an integer in the set \( \{ \text{secret} \mid \text{secret} \mod p_i = 1, \text{for i=1,2,\ldots,n}\} \). We have proposed a secret key distribution secrets to verify the \( t \)-threshold range and \( t \)-threshold consistency of shares without revealing the secrecy of both the secret and shares. By examining the revealed sum and difference of the secret and verification secrets, we can conclude that shares are generated by the secret in the \( t \)-threshold range. The proposed VSS is unconditionally secure, and the secret reconstruction is the same as the Azimuth–Bloom’s SS that is perfectly secret.

Remark 1.

The numbers in the \( t \)-threshold range, \( \{p_1 \cdot p_2 \cdot \ldots \cdot p_n \mid \text{secret} \mod p_i = 1, \text{for i=1,2,\ldots,n}\} \), where \( \text{secret} \mod p_i = 1 \), \( i=1,2,\ldots,n \), and \( \text{secret} \mod p_i = 1 \), \( i=1,2,\ldots,n \), with \( \gcd(p_i, p_j) = 1 \), for every \( i \neq j \).

Secret reconstruction

We want to point out that Mignotte’s \((t,n)\) threshold SS is not a perfect SS because information of the secret can be leaked with fewer than \( t \) shares.

2.3. Review of Azimuth–Bloom \((t,n)\) SS [4]

Share generation

In Azimuth–Bloom \((t,n)\) SS, the dealer selects \( p_0 \) and a sequence of pairwise co-prime positive integers, \( p_1 < p_2 < \ldots < p_n \), such that \( p_0 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n = 1 \), \( i=1,2,\ldots,n \), where \( p_i \) is the public information associated with each shareholder, \( U_i \). For this given sequence, the dealer chooses the
secret $s$ as an integer in the set $Z_{p_0}$. The dealer selects an integer, $x$, such that $x + 2p_0 \in Z_{p_0}$, needs to be in the $t$-threshold range, $Z_{p_0}, ..., z_{p_0}, ..., z_{p_0}$; otherwise, the value, $s + 2p_0$, can be obtained with fewer than $t$ shares. However, in the original paper [4], it specifies that the value, $s + 2p_0$, is in the set, $Z_{p_1}, ..., z_{p_n}$. This range is different from the $t$-threshold range. In other words, if $s + 2p_0$ is selected to be smaller than the lower bound of the $t$-threshold range (i.e., it is still in the set $Z_{p_1}, ..., z_{p_n}$), then the value, $s + 2p_0$, can be obtained with fewer than $t$ shares. It is obvious that this situation violates one of the security requirements of the $(t,n)$ SS. Share for the shareholder, $U_i$, is generated as $s_i = s + 2p_0 \mod p_i$, and $s_i$ is sent to shareholder, $U_i$, secretly, for $i = 1, 2, ..., n$.

**Secret reconstruction**

Given a subset of $t$ distinct shares, for example, $\{s_1, s_2, s_t\}$, the secret $s$ can be reconstructed by solving the following system of equations as

$$
\begin{align*}
    x &\equiv s_1 \mod p_1; \\
    x &\equiv s_2 \mod p_2; \\
    \vdots \\
    x &\equiv s_t \mod p_t.
\end{align*}
$$

Using the standard CRT, a unique solution $x$ is given as

$$
x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \cdot s_i \mod N,
$$

where $N = p_1 \cdot p_2 \cdot ... \cdot p_t$, and $N \cdot y_i \cdot s_i \mod p_i = 1$. Then, the secret $s$ can be recovered by computing $s = x \mod p_0$.

Azimuth–Bloom $(t,n)$ SS is a perfect SS because no information is leaked when there are fewer than $t$ shares. Interested readers can refer to the original paper [4] for detailed discussion. Azimuth–Bloom’s secret reconstruction scheme can be generalized to take more than $t$ shares. For example, when there are $j$ (i.e., $t < j < n$) shareholders with their shares, $\{s_1, s_2, ..., s_j\}$, participated in the secret reconstruction, the secret, $s$, can be reconstructed using the standard CRT to find a unique solution $x$ for the system of $j$ equations.

### 3. MODELS OF PROPOSED VSS

#### 3.1. Definitions

A VSS enables shareholders to verify that their shares of an $(t,n)$ SS are generated by the dealer consistently. In other words, without revealing the secret and the shares, shareholders can verify that any subset of $t$ or more than $t$ shares defines the same secret, but any subset of fewer than $t$ shares cannot define the same secret. Benaloh [1] presented a notion of $t$-consistency and uses it to define the objective of a VSS. We include the notion here.

**Definition 1:** $t$-consistency. A set of $n$ shares is said to be $t$-consistent if any subset of $t$ of the $n$ shares defines the same secret.

Benaloh observed that the shares in Shamir’s $(t,n)$ SS are $t$-consistent if and only if the interpolation of the $n$ shares yields a polynomial of degree at most $t - 1$. This implies that if the interpolating polynomial of $n$ shares has degree at most $t - 1$, then all shares are $t$-consistent. However, the property of $t$-consistency does not guarantee that all shares satisfy the security requirements of an $(t,n)$ SS. For example, if the interpolating polynomial of $n$ shares has degree $t - 2$, then all shares are both $(t - 1)$-consistent and $t$-consistent. The polynomial having degree $t - 2$ can be reconstructed with only $t - 1$ shares (i.e., which is less than the threshold). Similarly, if shares of a CRT-based SS are generated by a secret selected in the $(t - 1)$-threshold range, then all shares are both $(t - 1)$-consistent and $t$-consistent. In other words, the secret can be recovered with only $t - 1$ shares. This situation violates one of the security requirements of an $(t,n)$ SS. That is, the secret cannot be obtained with fewer than $t$ shares. Thus, Benaloh’s $t$-consistency cannot satisfy the security requirement of an $(t,n)$ SS. We modify the definition of $t$-consistency and introduce a new notion, called $t$-threshold consistency, which can satisfy the security requirements of an $(t,n)$ SS.

**Definition 2:** $t$-threshold consistency. A set of $n$ shares are said to be $t$-threshold consistent (i.e., $t < n$) if (i) any subset of $t$ or more than $t$ out of the $n$ shares defines the same secret, and (ii) any subset of fewer than $t$ out of the $n$ shares cannot define the same secret.

It is obvious that, in a CRT-based SS, shares generated by a secret selected in the $t$-threshold range are $t$-threshold consistent. Shares with the property of $t$-threshold consistency satisfy the security requirements of an $(t,n)$ SS. Verifying the $t$-threshold consistency of shares is the objective of our proposed VSS.

#### 3.2. Entities

In our VSS, the dealer is the prover, and all shareholders are the verifiers. The verifiers want to verify that their shares are generated by a secret selected in the $t$-threshold range without compromising the secrecy of their shares and the secret.
In our proposed VSS, we do not consider the situation when the dealer (the prover) colludes with a shareholder (the verifier). This is because if dealer wants to collude with any shareholder, the dealer can just reveal the secret to the shareholder directly. VSS cannot prevent this type of attack. Furthermore, we do not consider the situation when any verifier acts dishonestly in the verification. If any shareholder acts dishonestly by releasing an invalid value, where allows shareholders to verify that all shares are sure that their shares,这时 in our proposed VSS, we assume shareholder gains no advantage over other honest shareholders. Thus, in our proposed VSS, we assume that all shareholders (verifiers) act honestly to verify the t-threshold consistency of their shares.

3.3. Informal model of our proposed VSS

We assume that there are n shareholders, Ui, for i = 1, 2, . . . , n, participated in the VSS. These shareholders want to make sure that their shares, si, for i = 1, 2, . . . , m, obtained from the dealer are t-threshold consistent. In our proposed VSS, each shareholder computes, ci = F(sij), as his/her released value, where F is a public function. The algorithm, VSS, allows shareholders to verify that all shares are t-threshold consistent. That is,

\[
\text{VSS}\{c_i = F(s_i)|i = 1, 2, \ldots, n\} = \begin{cases} 
0 \rightarrow \text{exists inconsistent shares}; \\
1 \rightarrow \text{all shares are t-threshold consistent}.
\end{cases}
\]

Our proposed VSS is different from most VSSs, which verify one share at a time; but our VSS verifies all shares at once. There are only two possible outcomes of our proposed VSS, that are, either all shares are t-threshold consistent or there are inconsistent shares. Thus, our proposed VSS is sufficient if all shares are t-threshold consistent. However, if there are inconsistent shares, additional VSS is needed to identify inconsistent shares. Our proposed VSS can be used as a preprocess before applying other VSS to identify invalid shares.

3.4. Properties

We propose a non-interactive VSS with the following properties:

- **Correctness.** The outcome of our proposed VSS is positive if all shares are t-threshold consistent; otherwise, there are inconsistent shares.
- **Efficiency.** If the outcome of the proposed scheme is negative, the proposed VSS can only be used as a preprocess of other VSS to identify inconsistent shares. Thus, our proposed VSS must be efficient.
- **Security.** The VSS must be able to protect the secrecy of both shares and the secret in the verification.

4. PROPOSED VSS

4.1. Outline of our design

Our VSS is based on the Azimuth–Bloom’s SS. We want to prove that the shares, si, i = 1, 2, . . . , n, generated by the dealer correspond to the secret, A = s + 2p0, which is selected from the t-threshold range, \(Z_{p_0-1, p_0, \ldots, p_0} = p_0 - 2p_0 - p_0, p_0 \cdots \). To achieve this objective, we use the verification secrets, Bi, i = 1, 2, . . . , k. It is obvious that if the verification secret, Bi, is in the t-threshold range and shareholders can show that A + Bi is also in the t-threshold range, then shareholders can conclude A < p1 · p2 · · · pt (i.e., A is smaller than the upper bound of the t-threshold range). Similarly, if the verification secret, Bi, is in the t-threshold range and shareholders can show that A − Bi is in the t-threshold range, then shareholders can conclude p0 · t + 2 · p0 · t + 3 · · · pn < A (i.e., A is larger than the lower bound of the t-threshold range). In summary, shareholders can obtain p0 · t+2 · p0 · t+3 · · · pn < A < p1 · p2 · · · pt. There is one remaining problem needed to be overcome in this approach. If the verification secret, Bi, is known to shareholders, shareholders can also obtain the secret, A. VSS should protect the secrecy of both shares and the secret. In our proposed scheme, we use the linear combination to protect the secrecy.

**Remark 2.** If both A + Bi mod N where N = p1 · p2 · · · pt, and Bi are in the t-threshold range, then either (i) A is smaller than the upper bound of the t-threshold range (i.e., A < p1 · p2 · · · pt), or (ii) A is larger than the upper bound of the t-threshold range (i.e., A > p1 · p2 · · · pt). However, verifiers can distinguish between these two cases easily. If A < p1 · p2 · · · pt, then the solution of CRT computation using any t + 1 out of n shares of A + Bi is smaller than the upper bound of the t-threshold range (i.e., A + Bi < p1 · p2 · · · pt); otherwise, if A > p1 · p2 · · · pt, then the solution of CRT computation using any t + 1 out of n shares of A + Bi is larger than the upper bound of the t-threshold range (i.e., A + Bi > p1 · p2 · · · pt).

4.2. Proposed VSS

The proposed VSS is illustrated in Figure 2.

**Share generation**

Just like the Azimuth–Bloom (t,n) SS, the dealer selects an integer p0 and a sequence of pairwise coprime positive integers, p1 < p2 < . . . < pn, such that p0 · p0 · t+2 · · · pt+3 · · · pn · p1 · p2 · · · pt, where p0 is the public information associated with each shareholder, U0. For this given sequence, the dealer chooses the secret s as a random integer in the set Zp0. The dealer selects an integer, x, such that A = s + 2p0 \(Z_{p_0-1, p_0, \ldots, p_0} = p_0 - 2p_0 - p_0, p_0 \cdots \). Share for the shareholder, U0, is generated as s = s + 2p0 mod p0, i = 1, 2, . . . , n. sj is sent to shareholder, Ui, secretly.
Shares generation
Step 1. Dealer selects \( n + 1 \) positive integers, \( p_0 < p_1 < p_2 < \ldots < p_n \), satisfying (a) \( \text{GCD}(p_i, p_j) = 1, \forall i \neq j \); and (b) \( p_0 \cdot p_{n+1} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_i \).

Step 2. Dealer selects the secret \( s \) in the set \( Z_{p_1} \). The dealer selects an integer, \( \alpha \), such that
\[
A = s + \alpha p_0 \in Z_{p_0 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n}.
\]
Share for the shareholder, \( U_i \), is generated as \( s_i = s + \alpha p_0 \mod p_i, i = 1, 2, \ldots, n \).

\( s_i \) is sent to shareholder, \( U_i \), secretly.

Step 3. Dealer selects \( k \) (say \( k = 100 \)) verification secrets, \( B_i \), in \( Z_{p_0 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n} \), such that \( A + B_i < p_1 \cdot p_2 \cdot \ldots \cdot p_i \) and \( A > B_i \), for \( i = 1, 2, \ldots, k \). The dealer generates shares, \( s_{ij} = B_i \mod p_j, i = 1, 2, \ldots, k \), of verification secrets and distributes them to each shareholder, \( U_j \). At the end of this phase, each shareholder has received \( k + 1 \) shares from the dealer.

Shares verification
Step 1. All shareholders work together to randomly determine a subset \( B \) (say \(|B| = 50\)) of shares corresponding to the verification secrets. Each shareholder needs to reveal shares of this subset \( B \). According to the CRT, using these released shares, shareholders can recover the verification secrets corresponding to the subset \( B \). Shareholders can verify whether each recovered verification secret is in the \( t \)-threshold range. If all recovered verification secrets are in the \( t \)-threshold range, then continue.

Step 2. Shareholders work together again to divide “unopened” verification secrets into two disjoint subsets, say \( \forall B_i \in \) the first subset, and \( \forall B_j \in \) the second subset (\( i \neq j \)), and to reveal the additive sums and the differences of shares of the secret, \( A \), with respect to each verification secret (i.e., for all \( B_i \) and \( B_j \)), respectively.

Step 3. Using CRT on these released values, shareholders can recover both \( A + B_i \) and \( A - B_j \). Shareholders can verify whether \( A + B_i < p_1 \cdot p_2 \cdot \ldots \cdot p_i \) and \( 0 < A - B_j < p_1 \cdot p_2 \cdot \ldots \cdot p_i - p_{n-i+2} \cdot p_{n-i+3} \ldots \cdot p_n \). If the verification is passed for all verification secrets, shareholders can conclude that their shares corresponding to the secret, \( A \), are \( t \)-threshold consistent.

Secret reconstruction
Given \( t \) distinct shares, for example, \( \{s_1, s_2, \ldots, s_t\} \), the secret \( s \) is reconstructed by using the standard CRT as
\[
x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \mod N, \text{ where } N = p_1 \cdot p_2 \cdot \ldots \cdot p_t, \text{ and } \frac{N}{p_i} \cdot y_i \mod p_i = 1. \text{ Then, by computing } x \mod p_0, \text{ the secret } s \text{ can be recovered.}
\]

**Figure 2.** Proposed verifiable secret sharing scheme.
\( \forall i,j \in \text{subsets of the unopened verification secrets. If all verifications are passed, shareholders can conclude that their shares corresponding to the secret, } A, \text{ are } t\text{-threshold consistent.} \)

**Theorem 1.**

If \( A + B_i < p_1 \cdot p_2 \cdot \ldots \cdot p_t \) and \( 0 < A - B_j < p_1 \cdot p_2 \cdot \ldots \cdot p_t - p_{t-1} \cdot p_{t-2} \cdot \ldots \cdot p_{t-r} \cdot p_{t-r+1} \cdot \ldots \cdot p_n \), for \( \forall i, j \in \text{subsets of the unopened verification secrets, the shares are } t\text{-threshold consistent; otherwise, there are inconsistent shares.} \)

Proof.

If all shares are generated consistently by the dealer and shareholders act honestly to compute the additive sum of shares, \( s_1 + s_{2,l} \), \( l = 1, 2, \ldots, n \), and the difference of shares, \( s_1 - s_{2,l} \), \( l = 1, 2, \ldots, n \), they can recover both \( A + B_i \) and \( A - B_j \), respectively, from system of equations of shares using the CRT. In the earlier steps of the VSS, shareholders have already verified that all “unopened” verification secrets are in the \( t\)-threshold range. Thus, they obtain \( p_{n-r+2} \cdot p_{n-r+3} \cdot \ldots \cdot p_n < B_i < p_{1} \cdot p_{2} \cdot \ldots \cdot p_t \). Furthermore, if \( A + B_i < p_1 \cdot p_2 \cdot \ldots \cdot p_t \) and \( A - B_j \) is the first subset, shareholders can conclude \( A < p_1 \cdot p_2 \cdot \ldots \cdot p_t \) with very high probability. Similarly, if \( A - B_j > 0 \), the second subset, shareholders can also conclude \( p_{n-r+2} \cdot p_{n-r+3} \cdot \ldots \cdot p_n < A \) \( p_1 \cdot p_2 \cdot \ldots \cdot p_t \). Therefore, shares of the secret, \( A \), are \( t\)-threshold consistent. Otherwise, there are inconsistent shares.

**Secret reconstruction**

This process is the same as the Azimuth–Bloom \((t,n)\) SS. Given \( t \) distinct shares, for example, \( \{s_1, s_2, \ldots, s_t\} \), the secret \( s \) is reconstructed by solving the following system of equations as

\[
x = s_1 \mod p_1; \\
x = s_2 \mod p_2; \\
\vdots \\
x = s_t \mod p_t.
\]

Using the standard CRT, a unique solution \( x \) is given as

\[
x = \sum_{l=1}^{t} \frac{N}{p_l} y_l s_l \mod N, \text{ where } N = p_1 \cdot p_2 \cdot \ldots \cdot p_t \text{ and } \sum_{l=1}^{t} \frac{N}{p_l} y_l \mod p_l = 1. \text{ Then, by computing x mod } p_0, \text{ the secret s can be recovered.} \]

## 5. SECURITY ANALYSIS AND PERFORMANCE

### 5.1. Security analysis of the shares verification

In the VSS, the released values are \( s_i + s_{j,l} \) and \( s_i - s_{j,l} \) for \( l = 1, 2, \ldots, n \). Because both \( s_{i,j} \) and \( s_{j,i} \) are unopened shares, it is computationally impossible to obtain the share, \( s \), from the released values. Furthermore, it is computationally impossible to obtain the secret, \( A \), from the recovered values, \( A + B_i \) and \( A - B_j \), because both \( B_i \) and \( B_j \) are unopened verification secrets. The security of this verification does not depend on any computational assumption and it is unconditionally secure.

### 5.2. Security analysis of the secret reconstruction

It is obvious that the secret can be successfully reconstructed if all shareholders act honestly to release their shares. Just like the Azimuth–Bloom \((t,n)\) SS [4], this proposed scheme is a perfect SS because no information is leaked when there are fewer than \( t \) shares in the secret reconstruction. Let us assume that \( t - 1 \) shareholders, for example, \( \{U_1, U_2, \ldots, U_{t-1}\} \) with their shares \( \{s_1, s_2, \ldots, s_{t-1}\} \), work together to obtain \( A' = \sum_{i=1}^{t-1} \frac{N'}{p_i} y_i s_i \mod N' \), where \( N' = p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1} \) and \( \sum_{i=1}^{t-1} \frac{N'}{p_i} y_i \mod p_i = 1. \) However, the real secret, \( A \), is in the \( t\)-threshold range. According to the CRT, the real secret, \( A \), is related to the recovered value, \( A' \), in the following way as \( A = A' + 2N' \).

By properly shifting \( A' \) to some values in the \( t\)-threshold range as \( A' + 2N' \) may obtain the secret. There are \( \frac{p_{t-1}}{p_{t-2} \cdots p_0} > p_0 \) values of \( \lambda \), which can shift \( A' \) into the \( t\)-threshold range; but, there is only one exact value of \( \lambda \), which shifts \( A' \) to the real secret, \( A \). Because the collection of possible \( \lambda \) is greater than the collection of possible secret \( s \), no useful information is leaked from the collection of any \( t - 1 \) shares.

Let us examine the other possibility that \( t - 1 \) shareholders, for example, \( \{U_1, U_2, \ldots, U_{t-1}\} \), can determine a parameter, \( \beta \), to shift the secret, \( A \), in the \( t\)-threshold range to a secret in the range, \( Z_{p_{t-1} \cdot p_{t-2} \cdots p_0} \), as \( A = \beta p_0 \). Then, these \( t - 1 \) shareholders can recover the secret by themselves. However, there are \( \frac{p_{t-1}}{p_{t-2} \cdots p_0} \) possible values of \( \beta \) corresponding to the secret, \( A \), in the \( t\)-threshold range; but, there are only \( \frac{p_{t-1} \cdot p_{t-2} \cdots p_0}{p_{t-1} \cdot p_{t-2} \cdots p_0} \) values of \( \beta \) that can shift the secret to some secret in \( Z_{p_{t-1} \cdot p_{t-2} \cdots p_0} \). The probability of figuring out a correct \( \beta \) is \( \frac{p_{t-1} \cdot p_{t-2} \cdots p_0}{p_{t-1} \cdot p_{t-2} \cdots p_0} \). Thus, the probability of correctly guessing \( \beta \) is smaller than the probability of guessing the secret \( s \). The security of the secret reconstruction is the same as the Azimuth–Bloom’s SS, which is perfectly secure.

### 5.3. Performance

The proposed VSS is a simple modification of the Azimuth–Bloom’s SS, which is a classical SS. In share generation, the dealer selects a secret and \( k \) additional verification secrets, and generates shares for shareholders. In shares verification, shareholders work together to open
a subset of verification secrets and to verify whether these verification secrets are in the $t$-threshold range. Then, shareholders reveal the additive sum and the difference of shares of the secret with respect to shares of different unopened verification secret, respectively. There is no secure channel needed among shareholders. The most time-consuming computation in the VSS is to reconstruct 50 verification secrets using the CRT. To reconstruct each verification secret, each shareholder, $U_i$, uses his share, $s_i$, of the verification secret to compute $c_i = \sum p_j x_j s_i \mod N$, where $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$, and $\sum y_i \mod p_i = 1$. After receiving all $c_i$'s from other shareholders, the verification secret can be obtained as $x = \sum c_i \mod N$. We should point out that the value, $y_i$, of each shareholder only needs to be computed one time, and it can be computed off-line. The value, $y_i$, can be reused for reconstructing other verification secrets. In addition, the size of moduli in the CRT does not need to be as large as the module used in most public key algorithms. Furthermore, there is no modulo exponentiation in the CRT. Therefore, the proposed VSS is very efficient in terms of computation and communication.

Our proposed VSS is different from most VSSs, which verify one share at a time; but our proposed VSS verifies all shares at once. Therefore, our proposed VSS is very efficient. There are only two possible outcomes of our proposed VSS, that are, either all shares are $t$-threshold consistent or there are inconsistent shares. Thus, the proposed VSS is sufficient if all shares are $t$-threshold consistent. However, if there are inconsistent shares, other VSS is needed to identify inconsistent shares.

6. CONCLUSION

We proposed a CRT-based VSS, which is a simple extension of the Azimuth–Bloom’s SS. Just like the Azimuth–Bloom’s SS, the proposed VSS is perfectly secure. We use multiple verification secrets to verify the $t$-threshold consistency of shares without revealing the secrecy of both the secret and shares. In the security analysis, we show that shares and the secret are protected unconditionally in the verification process. In addition, no information is leaked when there are fewer than $t$ shares in the secret reconstruction.

REFERENCES


