INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. (2014)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2760

A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets

Yanjun Liu[1,2], Lein Harn[3] and Chin-Chen Chang[2,4,*,†]

[1]*Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Hefei, 230039, China*
[2]*Department of Computer Science and Information Engineering, Asia University, Taichung, 413, Taiwan*
[3]*Department of Computer Science and Electrical Engineering, University of Missouri—Kansas City, Kansas City, Missouri 64110-2499, USA*
[4]*Department of Information Engineering and Computer Science, Feng Chia University, Taichung, 407, Taiwan*

SUMMARY

Verifiable secret sharing (VSS) has been extensively used as a cryptographic tool in many applications of information security in recent years. A VSS enables a dealer to divide a secret s into n shares and allows shareholders to verify whether their shares are generated by the dealer consistently without revealing the secrecy of both shares and the secret. More specifically, shareholders can verify that (i) the secret can be recovered by any t or more than t shares and (ii) the secret cannot be obtained by fewer than t shares. Many VSSs are based on polynomial, and only a few of them are based on the Chinese Remainder Theorem (CRT). Recently, Harn *et al*. proposed a CRT-based VSS in which multiple verification secrets are used during the phase of verification. In this paper, we propose a VSS based on Asmuth-Bloom's (t, n) SS scheme, which depends on the CRT. Our proposed VSS is simpler and more efficient than the scheme of Harn *et al*. Our proposed VSS is unconditionally secure. Copyright © 2014 John Wiley & Sons, Ltd.

Received 23 May 2013; Revised 14 January 2014; Accepted 16 January 2014

KEY WORDS: secret sharing (SS); verifiable secret sharing (VSS); Chinese Remainder Theorem (CRT); modified t-threshold range; t-threshold consistency

1. INTRODUCTION

In 1979, Shamir [1] and Blakley [2] first introduced the (t, n) secret sharing (SS) scheme separately as a key safeguarding scheme. In Shamir's (t, n) SS, a dealer partitions a secret s into n shares. The value t is called the *threshold value*, which determines the minimal number of shares needed to recover the secret s. Any secure (t, n) SS must satisfy two requirements [3], that is, (i) the secret s can be recovered by any t or more than t shares and (ii) the secret s cannot be reconstructed by fewer than t shares. Shamir's (t, n) SS is based on the Lagrange interpolating polynomial. Nowadays, SS [3–5] has become a prevalent mechanism in the fields of cryptography and information security. Although most SSs are based on an interpolating polynomial, other kinds of SSs are also researched deeply in scientific publications, especially the ones based on the Chinese Remainder Theorem (CRT) [6–8], such as Mignotte's SS scheme [9] and Asmuth-Bloom's SS scheme [10].

Secret sharing can be classified into two types, that is, SSs of computational security and SSs of unconditional security. Computational security is based on some computational assumptions so that some mathematical problems cannot be solved by the attackers due to their limited computational

*Correspondence to: Chin-Chen Chang, Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 407, Taiwan.
†E-mail: alan3c@gmail.com

power. These mathematical problems include the prime factorization of a large composite integer and the solving of discrete logarithm. On the other hand, unconditional security indicates that the security can be guaranteed without making any computational assumption. Shamir's (*t, n*) SS is unconditionally secure, that is, it can satisfy the two security requirements mentioned previously without making any computational assumption.

However, a secure (*t, n*) SS cannot detect whether there exists any deception between the dealer and shareholders. In 1985, Chor *et al*. [11] extended the notion of SS and proposed the first verifiable SS (VSS). Verifiability is the property of a VSS, which ensures that each shareholder has received a valid share. Invalid shares may be caused either by the dealer or by transmission errors. VSS is executed by shareholders after receiving their shares from the dealer but before using their shares to reconstruct the secret. If VSS has detected/identified some invalid shares, shareholders can request the dealer to regenerate new shares. Thus, VSS can ensure shareholders that their shares can be used to reconstruct a secret when the secret reconstruction is needed in the future. In a VSS, shareholders work together to verify that their shares are generated by the dealer consistently without revealing the secrecy of both shares and the secret. The property of verifiability can check if the shares of shareholders are consistent before performing secret reconstruction. If shares are inconsistent, shareholders can request the dealer to regenerate shares. Benaloh claimed that the *t*-consistency of shares [2] ensures that the secret can be recovered by any subset of *t* shares.

There are two types of VSSs, that is, interactive and non-interactive VSSs. Generally speaking, non-interactive VSSs are more efficient than interactive VSSs because the communication delay among shareholders of interactive VSSs is significant. Like SS, VSS can also be classified into two types, that is, VSSs of computational security and VSSs of unconditional security. VSSs have been used in a great number of research works in the areas of threshold cryptography, e-commerce, and multi-party computation [12–24].

Although an interpolating polynomial [25, 26] is the common method used in designing VSSs, VSSs based on the CRT have been received some attention recently. In 2005, Qiong *et al*. [27] presented a non-interactive VSS based on the CRT using Asmuth-Bloom's SS scheme. In 2007, Iftene [28] proposed another CRT-based VSS extended from Mignotte's SS scheme. Unfortunately, Kaya and Selcuk [29] pointed out that in these two VSSs, shareholders' shares can be generated by a corrupted dealer inconsistently without being detected. They proposed a VSS based on Asmuth-Bloom's SS scheme, and the security of their VSS depends on the RSA assumption [30] which was firstly proposed by Rivest, Shamir and Adleman in 1978. Recently, Harn *et al.* [31] proposed a CRT-based VSS in which multiple verification secrets are used during the phase of verification. Their VSS can verify the *t*-threshold consistency of shares, and their VSS is unconditionally secure.

In this paper, we propose a non-interactive VSS based on Asmuth-Bloom's SS scheme. In our proposed VSS, all shareholders can verify that their shares are generated by the dealer consistently. The contributions of our proposed VSS are listed in the succeeding text:

- We give the definition of modified *t*-threshold range, which is used in the verification.
- Our proposed VSS is simpler and more efficient than the VSS of Harn *et al*.
- The security of our proposed VSS is unconditionally secure. Moreover, we show that no useful information is disclosed when there are fewer than *t* shares in the secret reconstruction.

The rest of this paper is organized as follows. Section 2 provides some fundamentals. Our proposed VSS is described in Section 3. Section 4 gives security analysis of our proposed VSS. Section 5 is the comparison of performance between our proposed VSS and the VSS proposed by Harn *et al*. Conclusion is given in Section 6.

2. PRELIMINARIES

In this section, we briefly introduce some basic knowledge for our proposed VSS in Section 3. First, we introduce the CRT. Second, we review Asmuth-Bloom's (*t*, *n*) SS [10]. We also review the VSS of Harn *et al*. [31].

DOI: 10.1002/dac

2.1. Chinese Remainder Theorem

The CRT [6–8] has been widely used in applications of cryptography. Assume that there are t pairwise, co-prime integers, $p_1, p_2, \ldots, p_t$, that is, $\mathrm{GCD}(p_i,p_j)=1$ for $i \neq j$. A system of simultaneous congruencies can be constructed as follows:

$$\begin{aligned} X &= x_1 (\bmod p_1), \\ X &= x_2 (\bmod p_2), \\ &\vdots \\ X &= x_t (\bmod p_t). \end{aligned}$$

The CRT computes the solution X as $X = \sum_{i=1}^{t} M_i \cdot M_i^{'} \cdot x_i (\bmod P)$, where $P = \prod_{i=1}^{t} p_i$, $M_i = \frac{P}{p_i}$, and $M_i \cdot M_i^{'} \equiv 1 (\bmod p_i)$. Notice that X is the unique solution in Z_P, where Z_P represents the integers in the range of $[0,P)$.

2.2. Asmuth-Bloom's (t, n) secret sharing

Asmuth-Bloom's (t, n) SS is a CRT-based SS, which was proposed in 1983 [10]. It consists of two phases, that is, share generation and secret reconstruction.

Share generation

A set of positive integers, $\{q, p_1 < p_2 < \ldots < p_n\}$, also called Asmuth-Bloom sequence, is selected satisfying the following conditions:

1) $\mathrm{GCD}(p_i, p_j) = 1$ for $i \neq j$,
2) $\mathrm{GCD}(q, p_i) = 1$ for all i,
3) $q \cdot p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_t$,

where p_i is the public information assigned to the shareholder, u_i. The dealer selects the secret s in Z_q. Then, the dealer chooses an integer, d, to calculate an integer $X = s + dq$ in the range of $(p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t)$. Here, the range of $(p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t)$ can be denoted as $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \cdots \cdot p_n, p_1 \cdot p_2 \cdot \cdots \cdot p_t}$, which is called the ***t-threshold range*** in [31].

The share s_i of shareholder, u_i, is generated by computing $s_i = X (\bmod p_i)$, $i = 1, 2, \ldots, n$. Each share, s_i, is sent to shareholder, u_i, in a secure channel.

DOI: 10.1002/dac

Secret reconstruction

Given any t distinct shares, $s_{lj} \in \{s_1, s_2, \ldots, s_n\}$, and their corresponding moduli, $p_{lj} \in \{p_1, p_2, \ldots, p_n\}$ for $j = 1, 2, ..., t$, the integer X can be recovered by solving the following system of simultaneous congruencies using the CRT as described in Subsection 2.1:

$$X = s_{l1} (\mathrm{mod}\ p_{l1}),$$

$$X = s_{l2} (\mathrm{mod}\ p_{l2}),$$

$$\vdots$$

$$X = s_{lt} (\mathrm{mod}\ p_{lt}).$$

Therefore, the secret s can be obtained by computing $s = X (\mathrm{mod}\ q)$.

Now we explain why the integer X must be selected by the dealer in the t-threshold range. Let us examine the lower bound and upper bound of the t-threshold range, $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$. The lower bound of the t-threshold range is $p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n$, which is the largest product of any $t-1$ moduli in the set of n positive integers, $\{p_1, p_2, \ldots, p_n\}$, whereas the upper bound is $p_1 \cdot p_2 \cdot \ldots \cdot p_t$, which is the smallest product of any t moduli. Consequently, selecting X in the t-threshold range guarantees that two security requirements of an SS can be satisfied. Because the product of any t moduli associated with t shares is larger than or equal to the upper bound, the secret s can be recovered by any t or more than t shares. On the other hand, the product of any $t-1$ moduli associated with $t-1$ shares, which is smaller than or equal to the lower bound, determines that the secret s cannot be reconstructed by fewer than t shares.

Furthermore, Asmuth-Bloom's (t, n) SS is a perfect SS because no information of the secret is revealed with knowing fewer than t shares. Interest reader can refer to the original paper [10] for detailed discussion.

2.3. Review of the verifiable secret sharing of Harn et al.

In this subsection, we review the VSS of Harn *et al*. [31], which is an extension of Asmuth-Bloom's (t, n) SS. Their VSS uses linear combination of both the secret and the verification secret to verify the t-threshold consistency of shares without compromising the secrecy of both shares and the secret. Here, we introduce the definition of t-threshold consistency [31].

Definition 1
t-threshold consistency

A set of n shares are t-threshold consistent if the following two requirements are satisfied: (i) the secret can be recovered by any t or more than t out of the n shares and (ii) the secret cannot be obtained by fewer than t out of the n shares.

Harn *et al*. proved that in their VSS, if the secret is selected in the t-threshold range, its shares are t-threshold consistent. Their VSS consists of three phases, that is, the share generation phase, share

DOI: 10.1002/dac

verification phase, and secret reconstruction phase. In the share generation phase, according to the Asmuth-Bloom sequence, $\{q, p_1 < p_2 < \ldots < p_n\}$, the dealer selects the secret s in Z_q and then chooses an integer, d, in such a way that $A = s + dq$ in the t-threshold range. In addition, the dealer selects k verification secrets and then generates and distributes shares of secret A and verification secrets to each shareholder secretly. In the share verification phase, shareholders need to ensure that unopened verification secrets are selected from the t-threshold range first. Then, they reveal the liner combinations of shares of the secret A and unopened verification secrets. Shareholders use these revealed values to recover the additive sums and the differences of the secret A and each unopened verification secret by the CRT. By examining the range of the recovered values, shareholders can conclude whether the secret A is in the t-threshold range. Therefore, they can verify the t-threshold consistency of shares. In the secret reconstruction phase, the secret is reconstructed from any t or more than t distinct shares via the CRT.

3. OUR PROPOSED VERIFIABLE SECRET SHARING

In this section, we propose a non-interactive VSS based on Asmuth-Bloom's SS scheme. We first introduce the participants involved in the proposed VSS and then give the outline of this VSS. Finally, the design of the proposed VSS is introduced in detail.

3.1. Participants in the proposed verifiable secret sharing

In our proposed VSS, there are two types of participants, that is, the dealer and the shareholders. The dealer is the prover who partitions a secret s into n shares and sends each share to each shareholder in a secure channel. The shareholders are the verifiers who work together to verify that their shares are consistent.

Two assumptions on the dealer and the shareholders must be made in our proposed VSS: (i) the dealer does not collude with any shareholder, that is, VSS cannot prevent the colluded shareholder to obtain the secret from the dealer and (ii) the shareholders act honestly in performing the verification, that is, the shareholders release valid values for verification.

3.2. Outline of the proposed verifiable secret sharing

Our proposed VSS can enable shareholders to verify that their shares distributed by the dealer are t-threshold consistent. In other words, the secret is selected in the t-threshold range. In the proposed VSS, the dealer generates an Asmuth-Bloom sequence and selects the secret s in Z_q. Then, the dealer chooses an integer, d, in such a way that $X = s + dq \in Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2T,\ p_1 \cdot p_2 \cdot \ldots \cdot p_t - 2T}$, where $T = \sum_{i=1}^{n} p_i$. The dealer sends share, $s_i = X (\mathrm{mod}\, p_i)$ for $i = 1, 2, \ldots, n$, to shareholder, u_i, secretly. In order to verify the t-threshold consistency of the shares, each shareholder, u_i, selects an adjusting value, $\lambda_i \in [-(p_i - 1), p_i - 1]$. According to the CRT, shareholders can use their adjusting values to recover an integer, X', which has a relation with respect to X. It can be further implied that if $X' \in Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + T,\ p_1 \cdot p_2 \cdot \ldots \cdot p_t - T}$, shareholders can conclude that X is in the t-threshold range. Therefore, the shares generated by X are t-threshold consistent.

3.3. Proposed verifiable secret sharing

Our proposed VSS consists of three phases: (i) the share generation; (ii) the share verification; and (iii) the secret reconstruction. Details of our proposed VSS are described in the following.

DOI: 10.1002/dac

3.3.1. Share generation. Assume that there are one dealer and n shareholders involving in the proposed VSS. The dealer generates a set of positive integers, $\{q < p_1 < p_2 < \ldots < p_n\}$, which is selected satisfying the following conditions:

(1) $\mathrm{GCD}(p_i, p_j) = 1$ for $i \neq j$,
(2) $\mathrm{GCD}(q, p_i) = 1$ for all i,
(3) $q \cdot (p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2T) < p_1 \cdot p_2 \cdot \ldots \cdot p_t\text{-}2T$,

where p_i is the public information assigned to shareholder, u_i, and $T = \sum_{i=1}^{n} p_i$.

The dealer selects the secret s in Z_q. Then, the dealer chooses an integer, d, in such a way that $X = s + dq \in Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2T,\ p_1 \cdot p_2 \cdot \ldots \cdot p_t - 2T}$. The share s_i of shareholder, u_i, is generated by computing $s_i = X (\mathrm{mod}\, p_i)$, $i = 1, 2, \ldots, n$. Each share, s_i, is sent to shareholder, u_i, in a secure channel.

3.3.2. Share verification. Each shareholder, u_i, randomly selects an *adjusting value*, $\lambda_i \in [-(p_i - 1), p_i - 1]$. According to the CRT, the shareholder u_i uses the adjusting value λ_i, his or her share s_i, and $\{p_1, p_2, \ldots, p_n\}$ to compute and release $s_i' = (M_i \cdot M_i' \cdot s_i + \lambda_i) \mathrm{mod} P$, where $P = \prod_{i=1}^{n} p_i$, $M_i = \frac{P}{p_i}$, and $M_i \cdot M_i' \equiv 1 (\mathrm{mod}\, p_i)$.

After collecting s_i' for $i = 1, 2, \ldots, n$, shareholders can work together based on the CRT to recover an integer X' by computing as $X' = \sum_{i=1}^{n} s_i' \,(\mathrm{mod} P)$. Shareholders then examine whether the value of X' is in the modified t-threshold range. If X' is in the modified t-threshold range, shareholders can conclude that X is in the t-threshold range, which indicates that the shares are t-threshold consistent.

In the following, Definition 2 will describe the definition of modified t-threshold range.

Definition 2

Modified t-threshold range

The range of $(p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + T, p_1 \cdot p_2 \cdot \ldots \cdot p_t - T)$, that is, $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + \mathrm{T},\ p_1 \cdot p_2 \cdot \ldots \cdot p_t - T}$, is called the modified t-threshold range, where $T = \sum_{i=1}^{n} p_i$.

Remark 1

In the scheme, in order to verify that all shares are t-threshold consistent, it requires every shareholder to honestly act in the process. Only one dishonest shareholder can ruin the verification process. This is the major difference between our scheme and most other VSSs. In our proposed scheme, all shares are verified at once; but in most other VSSs, one share is verified at one time. The efficiency of our proposed VSS is better than most other VSSs if all shares are valid. However, if there are invalid shares, our scheme cannot identify invalid shares. Thus, our proposed scheme can be used as a pre-processing of other VSSs. If all shares are valid, our scheme is sufficient; otherwise, other VSSs can be used to identify invalid shares.

3.3.3. Secret reconstruction. Secret reconstruction can be performed easily by using the CRT. Given any t distinct shares, $s_{lj} \in \{s_1, s_2, \ldots, s_n\}$, and their corresponding moduli, $p_{lj} \in \{p_1, p_2, \ldots, p_n\}$ for $j = 1, 2, \ldots, t$, the integer X can be recovered by constructing the following system of simultaneous congruencies:

$$
\begin{aligned}
X &= s_{l1} (\mathrm{mod}\, p_{l1}),\\
X &= s_{l2} (\mathrm{mod}\, p_{l2}),\\
&\vdots\\
X &= s_{lt} (\mathrm{mod}\, p_{lt}).
\end{aligned}
$$

DOI: 10.1002/dac

From CRT, the unique solution X in the t-threshold range can be computed as $X = \sum_{j=1}^{t} M_j \cdot M_j' \cdot s_{lj} (\mathrm{mod} P)$, where $P = \prod_{j=1}^{t} p_{lj}$, $M_j = \frac{P}{p_{lj}}$, and $M_j \cdot M_j' \equiv 1 (\mathrm{mod} p_{lj})$. Therefore, the secret s can be obtained by computing $s = X (\mathrm{mod}\, q)$.

The process of our proposed VSS is shown in Figure 1.

4. SECURITY ANALYSES

In this section, we give security analysis of our proposed VSS. We first prove the correctness of the proposed VSS. Let us recall that the objective of a VSS is to verify the consistency of shares without revealing the secrecy of both the secret and shares. Then, in this section, we will discuss the secrecy of shares and the secret in the VSS separately. Finally, we discuss the secrecy of the secret when there are less than t colluded shareholders to try to recover the secret.

4.1. Correctness of the proposed verifiable secret sharing

We use the following theorem to prove the correctness of our proposed VSS.

Theorem 1

If X' is in the modified t-threshold range, shareholders can verify that their shares are t-threshold consistent; otherwise, the shares are inconsistent.

Share generation

Step 1. The dealer generates a set of positive integers, $\{q < p_1 < p_2 < \ldots < p_n\}$, which satisfies 1) $GCD(p_i, p_j) = 1$ for $i \neq j$, 2) $GCD(q, p_i) = 1$ for all i, and 3) $q \cdot (p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2T) < p_1 \cdot p_2 \cdot \ldots \cdot p_t - 2T$, where $T = \sum_{i=1}^{n} p_i$.

Step 2. The dealer selects the secret s in Z_q. Then, the dealer chooses an integer, d, in such a way that $X = s + dq \in Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2T, p_1 \cdot p_2 \cdot \ldots \cdot p_t - 2T}$.

Step 3. The share $s_i = X (\mathrm{mod}\, p_i)$ for $i = 1, 2, \ldots, n$, is sent to shareholder, u_i, in a secure channel.

Share verification

Step 1. According to the CRT, each shareholder, u_i, selects an adjusting value, $\lambda_i \in [-(p_i - 1), p_i - 1]$, to compute and release $s_i' = (M_i \cdot M_i' \cdot s_i + \lambda_i) \mathrm{mod}\, P$, where $P = \prod_{i=1}^{n} p_i$, $M_i = \frac{P}{p_i}$ and $M_i \cdot M_i' \equiv 1 (\mathrm{mod}\, p_i)$.

Step 2. Shareholders work together to recover an integer X' by computing as $X' = \sum_{i=1}^{n} s_i' (\mathrm{mod}\, P)$.

Step 3. Shareholders examine whether the value of X' is in the modified t-threshold range. If X' is in the modified t-threshold range, shareholders can conclude that the shares are t-threshold consistent.

Secret reconstruction

Given any t distinct shares, $s_{ij} \in \{s_1, s_2, \ldots, s_n\}$, and their corresponding moduli, $p_{ij} \in \{p_1, p_2, \ldots, p_n\}$ for $j = 1, 2, \ldots, t$, the unique solution X can be computed as $X = \sum_{j=1}^{t} M_j \cdot M_j' \cdot s_{ij} (\mathrm{mod}\, P)$, from CRT, where $P = \prod_{j=1}^{t} p_{ij}$, $M_j = \frac{P}{p_{ij}}$ and $M_j \cdot M_j' \equiv 1 (\mathrm{mod}\, p_{ij})$. Therefore, the secret s can be obtained by computing $s = X (\mathrm{mod}\, q)$.

Figure 1. Process of our proposed verifiable secret sharing.

DOI: 10.1002/dac

Proof

In the verification, shareholders use their released values s_i' for $i = 1, 2, \ldots, n$, to compute X' as $X' = \sum_{i=1}^{n} s_i' \,(\mathrm{mod}P) = \sum_{i=1}^{n} \left(M_i \cdot M_i' \cdot s_i + \lambda_i\right) \mathrm{mod}P$. Because X can be recovered by $X = \sum_{i=1}^{n} \left(M_i \cdot M_i' \cdot s_i\right) \mathrm{mod}P$ according to the CRT, X' and X have the relation as $X' = \left(X + \sum_{i=1}^{n} \lambda_i\right) \mathrm{mod}P$. On the other hand, because λ_i is selected by each shareholder in the range of $[-(p_i - 1), p_i - 1]$, we can obtain $-T < \sum_{i=1}^{n} \lambda_i < T$, where $T = \sum_{i=1}^{n} p_i$. Therefore, $-T < X' - X < T$. If X' is in the modified t-threshold range (i.e., $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + \mathrm{T},\, p_1 \cdot p_2 \cdot \ldots \cdot p_t - T}$), shareholders can conclude that X is in the t-threshold range (i.e., $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n,\, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$). This can ensure that the shares generated by X are t-threshold consistent; otherwise, the shares are inconsistent.

Remark 2

Because the value, T ($T = \sum_{i=1}^{n} p_i$), is quite small in comparing with the size of length of the t-threshold range, $(p_1 \cdot p_2 \cdot \ldots \cdot p_t - p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n)$, the X selected by the dealer from the smaller range, $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2\mathrm{T},\, p_1 \cdot p_2 \cdot \ldots \cdot p_t - 2T}$, is insignificantly different from the t-threshold range. This can ensure that the shares of shareholders are t-threshold consistent.

Remark 3

Theorem 1 has proved that if X' is in the modified t-threshold range, X is in the t-threshold range. However, in the share generation, the dealer needs to select X in the range of $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n + 2\mathrm{T},\, p_1 \cdot p_2 \cdot \ldots \cdot p_t - 2T}$, which is 4 T smaller than the length of the t-threshold range $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n,\, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$. It is because if the dealer selects X out of the smaller range but still in the t-threshold range, then depending on adjusting values of shareholders, X' may not be in the modified t-threshold range. Consequently, shareholders are unable to verify that their shares are t-threshold consistent according to Theorem 1. However, if the dealer selects X in the smaller range, then shareholders are able to verify that their shares are t-threshold consistent. As noted in the Remark 1, although the dealer selects X in the smaller range, this range is insignificantly different from the t-threshold range.

4.2. Secrecy of shares in verifiable secret sharing

In VSS, each shareholder, u_i, releases a value $s_i' = (M_i \cdot M_i' \cdot s_i + \lambda_i) \mathrm{mod}\, P$ for $i = 1, 2, \ldots, n$, where λ_i is a secret random value selected by u_i in the range of $[-(p_i - 1), p_i - 1]$. Because the released value s_i' is a combination of the secret share s_i, and the secret λ_i, there has no sufficient information to derive the secret share s_i of each shareholder from s_i'. Therefore, the shares of shareholders are protected unconditionally in VSS.

4.3. Secrecy of the secret in verifiable secret sharing

From Theorem 1, the recovered value X' in VSS is $X' = \sum_{i=1}^{n} s_i' \,(\mathrm{mod}\, P) = \sum_{i=1}^{n} (M_i \cdot M_i' \cdot S_i + \lambda_i) \,\mathrm{mod}\, P$. On the other hand, the real secret X can be recovered by shares, s_i, $i = 1, 2, \ldots, n$, as $X = \sum_{i=1}^{n} \left(M_i \cdot M_i' \cdot s_i\right) \mathrm{mod}P$ according to the CRT. We can establish the relation between X' and X as $X' = \left(X + \sum_{i=1}^{n} \lambda_i\right) \mathrm{mod}P$. However, λ_i is a secret random value selected by each shareholder, u_i, there has no sufficient information to derive the secret X of shares from X'. Thus, the secret of shares is protected unconditionally in VSS.

DOI: 10.1002/dac

4.4. Secrecy of the secret for less than t colluded shareholders to try to recover the secret

Let us consider the situation that $t-1$ colluded shareholders, for example, u_i, for $i=1,2,\ldots,t-1$, try to work together to recover the secret s. These $t-1$ colluded shareholders can establish the system of equations in the succeeding text:

$$\begin{aligned} X'' &= s_1(\bmod p_1),\\ X'' &= s_2(\bmod p_2),\\ &\cdot\\ &\cdot\\ &\cdot\\ X'' &= s_{t-1}(\bmod p_{t-1}). \end{aligned}$$

According to the CRT, shareholders can obtain X'' by computing $X^{''} = \sum_{i=1}^{t-1} N_i \cdot N_i^{'} \cdot s_i \left(\bmod P^{'}\right)$, where $P^{'} = \prod_{i=1}^{t-1} p_i$, $N_i = \frac{P^{'}}{p_i}$, and $N_i \cdot N_i^{'} \equiv 1(\bmod p_i)$. Unfortunately, X'' and X are not in the same range, that is, X is in the t-threshold range but X'' is in $Z_{P'}$. So, the $t-1$ shareholders cannot recover X by using their shares.

Next, we show that these $t-1$ colluded shareholders cannot obtain any information of the real X from the value of X''. X'' has the following relation with X as $X = X'' + \beta \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1}$. If the value of β can be determined, $X \in Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \cdots \cdot p_n,\, p_1 \cdot p_2 \cdot \cdots \cdot p_t}$ can be obtained from $X'' \in Z_{P'}$. However, there are $\frac{p_1 \cdot p_2 \cdot \cdots \cdot p_t - p_{n-t+2} \cdot p_{n-t+3} \cdot \cdots \cdot p_n}{p_1 \cdot p_2 \cdot \cdots \cdot p_{t-1}} > p_0$ possible values of β that can shift $X'' + \beta \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1}$ to be in the t-threshold range; but only one value of β corresponds to the correct X. Therefore, the probability of finding the exact value of β is not greater than the probability of guessing the secret s. The security in the phase of secret reconstruction is unconditionally secure. Thus, our proposed VSS is perfectly secure because no useful information of the secret s is disclosed from fewer than t shares.

5. COMPARISON OF PERFORMANCE

According to the introduction described in Section 1, so far, there are only two secure CRT-based VSSs in the literature, one proposed by Kaya and Selcuk [29], which the security is based on the RSA assumption [30], and the other one proposed by Harn *et al*. [31], which the security is unconditionally secure. The VSS proposed by Kaya and Selcuk [29] verifies one share at a time, and the verification involves modulo exponentiations. However, the VSS proposed by Harn *et al*. [31] verifies all shares at once, and the verification involves only polynomial computations. Therefore, the VSS proposed by Harn *et al*. [31] is much faster than the VSS proposed by Kaya and Selcuk [29]. Because our proposed VSS is based on the VSS proposed by Harn *et al*. [31], in this section, we will give detail performance analysis of our proposed VSS and compare our VSS with the VSS of Harn *et al*. [31].

In the share generation of our proposed VSS, the dealer generates a secret and distributes its shares to n shareholders. Then, in the share verification, shareholders use adjusting values to recover an integer X' by the CRT and then check the range of X'. Now we analyze the computational cost of the share verification of our proposed VSS. According to the CRT, shareholders work together to recover an integer X' by computing as $X' = \sum_{i=1}^{n} s_i^{'}(\bmod P) = \sum_{i=1}^{n} \left(M_i \cdot M_i^{'} \cdot s_i + \lambda_i\right) \bmod P$, where $P = \prod_{i=1}^{n} p_i$, $M_i = \frac{P}{p_i}$, and $M_i \cdot M_i' \equiv 1(\bmod p_i)$. It is obvious that $M_i \cdot M_i'$ can be computed offline. Therefore, the process of computing X' requires n multiplications, $(2n-1)$ additions, and one modular operation. Supposing that p_i has a digits, the computational cost is $n \cdot a^2 + (2n-1) \cdot a + (n \cdot a)^2$. Thus, the time complexity is $O(n^2 a^2)$. In addition, the computational cost of the secret reconstruction can be computed in the same way.

DOI: 10.1002/dac

Table I. Comparison of computational cost.

	Share generation	Share verification	Secret reconstruction
VSS of Harn *et al*.	$O(n+k)$	$O(kn^2a^2)$	$O(t^2a^2)$
Our VSS	$O(n)$	$O(n^2a^2)$	$O(t^2a^2)$

VSS, verifiable secret sharing.

Table II. Comparison of communication cost in share generation.

	Dealer sends messages	Each u_i sends messages	Each u_i receives messages
VSS of Harn *et al*.	$n(k+1)$	—	$k+1$
Our VSS	n	—	1

Note: n is the number of shares, a is the number of bits of operands, and k (i.e., $k = 100$) is the number of verification secrets.
VSS, verifiable secret sharing.

On the other hand, the VSS of Harn *et al*. needs to select k additional verification secrets and sends their shares to shareholders in the share generation. In the share verification, their VSS uses linear combination of both the secret and the verification secret to verify the t-threshold consistency of shares. First, the shareholders need to recover $\frac{k}{2}$ verification secrets by using the CRT. Then, the shareholders recover the additive sums and the differences of the secret A and each unopened verification secret by the CRT. These are two time-consuming processes.

Table I lists the comparison of computational cost, which indicates that our VSS has lower computational cost than the VSS of Harn *et al*. Table II lists the communication cost, which indicates that our VSS also has advantage in communication cost than the VSS of Harn *et al*. In summary, from both tables, it shows that our VSS is more efficient than the VSS of Harn *et al*.

6. CONCLUSION

In this paper, we proposed a non-interactive VSS based on Asmuth-Bloom's SS scheme. Our proposed VSS uses adjusting values to recover an integer X' related to the secret by the CRT and then to check the range of X'. If X' is in the modified t-threshold range, shareholders can verify that their shares are t-threshold consistent. Analysis shows that our proposed VSS is unconditionally secure and is simpler and more efficient than the VSS of Harn *et al*.

ACKNOWLEDGEMENTS

This research was supported in part by the National Nature Science Foundation of China (grant number: 61202228) and the College Natural Science Key Project of Anhui Province of China (grant number: KJ2012A008).

REFERENCES

1. Shamir A. How to share a secret. *Communications of the ACM* 1979; **22**(11):612–613.
2. Blakley GR. Safeguarding cryptographic keys. *Proceedings of American Federation of Information Processing Societies National Computer Conference*, New York, USA, Nov. 1979; **48**:313–317.
3. Guo C, Chang CC. A construction for secret sharing scheme with general access structure. *Journal of Information Hiding and Multimedia Signal Processing* 2013; **4**(1):1–8.
4. Parakh A, Kak S. Space efficient secret sharing for implicit data security. *Information Sciences* 2011; **181**(2):335–341.
5. Zhu H, Liu T, Zhu D, Li H. Robust and simple N-party entangled authentication cloud storage protocol based on secret sharing scheme. *Journal of Information Hiding and Multimedia Signal Processing* 2013; **4**(2):110–117.
6. Chang CC, Lee HC. A new generalized group-oriented cryptoscheme without trusted centers. *IEEE Journal on Selected Areas in Communications* 1993; **11**(5):725–729.
7. Lai YP, Chang CC. Parallel computational algorithms for generalized Chinese remainder theorem. *Computers and Electrical Engineering* 2003; **29**(8):801–811.
8. Guo C, Chang CC. An authenticated group key distribution protocol based on the generalized Chinese remainder theorem. *International Journal of Communication Systems* 2012; article in press, DOI: 10.1002/dac.2348.

9. Mignotte M. How to share a secret. *Proceedings of the Workshop on Cryptography*, Lecture Notes in Computer Science 1983; **149**:371–375.
10. Asmuth C, Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory* 1983; **IT-29**(2):208–210.
11. Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science*, Oregon, Portland, Oct. 1985; 383–395.
12. Maurer U. Secure multi-party computation made simple. *Discrete Applied Mathematics* 2006; **154**(2):370–381.
13. Goldreich O. Secure multiparty computation. Available from: http://www.wisdom.weizman.ac.il/oded/pp.html, 2007.
14. Zhou L. APSS: proactive secret sharing in asynchronous systems. *ACM Transactions on Information and System Security* 2005; **8**(3):259–286.
15. He DB, Chen JH, Hu J. A pairing-free certificateless authenticated key agreement protocol. *International Journal of Communication Systems* 2012; **25**(2):221–230.
16. Cramer R, Damgard I, Maurer U. General secure multi-party computation from any linear secret sharing scheme. *Proceedings of the Eurocrypt' 00*, Bruges, Belgium, May 2000; **1807**:316–334.
17. Xie Q. A new authenticated key agreement for session initiation protocol. *International Journal of Communication Systems* 2012; **25**(1):47–54.
18. Pedersen TP. A threshold cryptosystem without a trusted party. *Proceedings of the Eurocrypt' 91*, Brighton, UK, Apr. 1991; **547**:522–526.
19. Harn L, Lin C. Strong (*n*, *t*, *n*) verifiable secret sharing scheme. *Information Sciences* 2010; **180**(16):3059–3064.
20. Lou DC, Huang HF. Efficient three-party password-based key exchange scheme. *International Journal of Communication Systems* 2011; **24**(4):504–512.
21. Tang HB, Liu XS. Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme. *International Journal of Communication Systems* 2012; **25**(12):1639–1644.
22. Marcos A, Simplicio JR, Sakuragui RM. Cryptanalysis of an efficient three-party password-based key exchange scheme. *International Journal of Communication Systems* 2012; **25**(11):1443–1449.
23. Cheng ZY, Liu Y, Chang CC, Guo C. A fault-tolerant group key agreement protocol exploiting dynamic setting. *International Journal of Communication Systems* 2013; **26**(2):259–275.
24. He DJ, Chen C, Ma MD, Chan SM, Bu JJ. A secure and efficient password-authenticated group key exchange protocol for mobile ad hoc networks. *International Journal of Communication Systems* 2013; **26**(4):495–504.
25. Feldman P. A practical scheme for non-interactive verifiable secret sharing. *Proceedings of 28th IEEE Symposium on Foundations of Computer Science*, Los Angeles, California, Oct. 1987; 427–437.
26. Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. *Advances in Cryptology-CRYPTO '91*, Lecture Notes in Computer Science, 1992; **576**:129–140.
27. Qiong L, Zhifang W, Xiamu N, Shenghe S. A non-interactive modular verifiable secret sharing scheme. *Proceedings of International Conference on Communications, Circuits and Systems (ICCCAS 2005)*, Los Alamitos, 2005; 84–87.
28. Iftene S. Secret sharing schemes with applications in security protocols. Technical report, University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science, 2007.
29. Kaya K, Selcuk AA. A verifiable secret sharing scheme based on the Chinese remainder theorem. *Advances in Cryptology - INDOCRYPT '08*, Lecture Notes in Computer Science, 2008; **5365**:414–425.
30. Rivest R, Shamir A, Adleman L. A method for obtaining digital signature and public-key cryptosystem. *Communications of the ACM* 1978; **21**(2):120–126.
31. Harn L, Miao F, Chang CC. Verifiable secret sharing based on the Chinese remainder theorem. *Security and Communication Networks* 2012; article in press, DOI: 10.1002/sec.807.

DOI: 10.1002/dac