Weighted Secret Sharing Based on the Chinese Remainder Theorem

Lein Harn[1] and Miao Fuyou[2]
(Corresponding author: Lein Harn)

Department of Computer Science Electrical Engineering, University of Missouri- Kansas City [1]
School of Computer Science and Technology, University of Science & Technology of China[2]
(Email: harnlein@gmail.com, mfy@ustc.edu.cn)

(Received June 22, 2013; revised and accepted Sep. 17, 2013)

Abstract

In a (t,n) secret sharing scheme (SS), a dealer divides a secret into n shares in such a way that (a) the secret can be recovered successfully with t or more than t shares, and (b) the secret cannot be recovered with fewer than t shares. In a weighted secret sharing scheme (WSS), each share of a shareholder has a positive weight. The secret can be recovered if the overall weight of shares is equal to or larger than the threshold; but the secret cannot be recovered if the overall weight of shares is smaller than the threshold value. The (t,n) SS is a special type of WSSs in which the weight of all shares is the same. A shareholder having a higher weight needs to keep multiple shares if we adopt a standard (t,n) SS to implement a WSS. In this paper, we propose a WSS based on the Chinese Remainder Theorem (CRT) and the security of our scheme is the same as the (t,n) SS proposed by Asmuth and Bloom. In our proposed WSS, every shareholder including shareholders having higher weights keeps only one share. Furthermore, the modulus associated with shareholders in our proposed scheme is smaller than the modulus in all existing schemes.

Keywords: Chinese remainder theorem, secret reconstruction, Shamir's scheme, weighted secret sharing

1 Introduction

Secret sharing schemes (SSs) were originally introduced by both Blakely [4] and Shamir [20] independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literature. SS has become one of the basic tools in cryptographic research. In Shamir's (t,n) SS, a secret s is divided into n shares by a dealer and is shared among n shareholders in such a way that (a) the secret can be reconstructed with t or more than t shares, and (b)the secret cannot be obtained with fewer than t shares. Shamir's (t,n) SS is based on the polynomial and is unconditionally secure. There are other types of SSs. For example, Blakely's scheme [4] is based on the geometry; Mignotte's scheme [14] and Azimuth-Bloom's scheme [1] are based on the Chinese remainder theorem (CRT).

The weighted secret sharing scheme (WSS) was originally proposed by Shamir [20]. In a WSS, each share of a shareholder has a positive weight. The secret can be recovered if the overall weight of shares is equal to or larger than the threshold; but the secret cannot be recovered if the overall weight of shares is smaller than the threshold value. In fact, Shamir's (t,n) SS is a special type of WSSs in which the weight of all shares is the same. There are some papers to discuss properties and characteristics of a WSS. For example, in [15], it deals with the property of information rate of a WSS. In [2], it characterizes all weighted threshold access structures that are ideal. It shows that a weighted threshold access structure is ideal if and only if it is a hierarchical threshold access structure, or a tripartite access structure, or a composition of two ideal weighted threshold access structures that are defined on smaller sets of users.

It is a very common approach to publish research papers related to the SS based on linear polynomials. But, there are only a few papers based on the CRT. Mignotte's SS [14] and Azimuth-Bloom's SS [1] are based on the CRT. Iftene [9] and Qiong et al. [16] have proposed two CRT-based VSSs. However, Kaya et al. [10] 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 Benaloh [3]. The security of their VSS is based on the RSA assumption [18]. In 2013, Harn et al. proposed a CRT-based VSS [7]. In addition, in 2009, Sarkar et al. [19] proposed a kind of CRT-based RSA-threshold cryptography for a mobile ad hoc network (MANET) and in 2011, Lu et al. proposed a secret key distributed storage scheme [12] based on CRT-VSS and trusted computing technology. Quisquater et al. [17] have shown that Asmuth-Bloom's SS [1] is asymptotically optimal both from an information theoretic and complexity theoretic viewpoint when the parameters satisfy a simplified relationship. Recently, Liu et al. proposed an authenticated group key distribution using the CRT [11] and Guo et al. proposed a quantum secret sharing based on the CRT [6].

So far, we have found two papers [8, 13] in the literature to propose WSS based on the CRT. However, both schemes are based on the Mignotte's scheme [14] which any share substantially decreases the entropy of the secret. Furthermore, in [8], the dealer needs to find out all minimal subsets of authorized access structure and then determines the modulus of each shareholder accordingly. In [13], the modulus associated with each shareholder is proportional to the weight of share. In both schemes, the moduli of shareholders are too large to be implementable.

The (t,n) SS is a special type of WSSs in which the weight of all shares is the same. A shareholder having a larger weight needs to keep multiple shares if we adopt a standard (t,n) SS to implement a WSS. In this paper, we propose a WSS based on the CRT and the security of our scheme is the same as the (t,n) SS proposed by Asmuth and Bloom. In our proposed WSS, every shareholder keeps only one share. In addition, in our proposed scheme, the moduli of shareholders having larger weights are determined by the moduli of shareholders having the minimal weight. In other words, the moduli of all shareholders are bounded by moduli of shareholders having the minimal weight of their shares.

The rest of this paper is organized as follows. In the next Section, we introduce some preliminaries including the CRT, Mignotte's and Asmuth-Bloom schemes based on the CRT. In Section 3, we propose a weighted secret sharing scheme based on a simple modification of Azimuth-Bloom scheme. In Section 4, we include the security analysis of our proposed scheme. Conclusion is given in Section 5.

2 Preliminaries

2.1 Chinese Remainder Theorem(CRT)[1]

Given the following system of equations as

$$x = s_1 \bmod p_1;$$
$$x = s_2 \bmod p_2;$$
$$.$$
$$.$$
$$.$$
$$x = s_t \bmod p_t,$$

There is one unique solution as

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

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

The CRT has been used in the RSA decryption to speed-up the decryption process. With the knowledge of prime decomposition of the RSA composite integer and using the CRT, the complexity of RSA decryption is reduced by a factor. The CRT can also be used in the SS. Each of the shares is represented in congruence, and the solution of the system of congruence using the CRT is the secret to be recovered. SS based on the CRT uses, along with the CRT, a special sequence of integers that guarantee the impossibility of recovering the secret from a set of shares with less than certain cardinality. In the nest subsections, we will review two most well-known SSs based on the CRT.

2.2 Review of Mignotte's SS

<u>Share generation</u>: A sequence consists of pairwise coprime positive integers, $p_1 < p_2 < \ldots < p_n$, with $p_{n-t+2} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_t$, 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 $Z_{p_{n-t+2} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$ (i.e., $Z_{p_{n-t+2} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$ is referred as the range $(p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t)$). We call the range, $Z_{p_{n-t+2} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$, the *t-threshold range,* as shown in Figure 1.

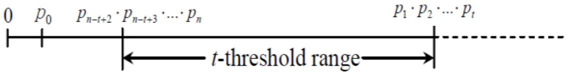
0
p_0
$p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n$
$p_1 \cdot p_2 \cdot \ldots \cdot p_t$
t-threshold range

Figure 1: The t-threshold range

The share for the shareholder, U_i, is generated as $s_i = s \bmod p_i, i = 1,2,\ldots,n.$ s_i is sent to shareholder, U_i, secretly.

{***Remark 1***} The numbers in the t-threshold range, $Z_{p_{n-t+2} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$, are integers upper bounded by $p_1 \cdot p_2 \cdot \ldots \cdot p_t$, which is the smallest product of any t moduli, and lower bounded by $p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n$, which is the largest product of any $t-1$ moduli. Selecting the secret, s, in this range can ensure that (a) the secret can be recovered with any t or more than t shares (i.e., the product of their moduli must be either equal to or larger than $p_1 \cdot p_2 \cdot \ldots \cdot p_t$), and (b) the secret cannot be obtained with fewer than t shares (i.e., the product of their moduli must be either equal to or smaller than $p_{n-t+2} \cdot \ldots \cdot p_n$). Thus, the secret of a (t,n) threshold SS should be selected from the t-threshold range.

Secret reconstruction: Given *t* distinct shares, for example, $\{s_1, s_2, \ldots s_t\}$, the secret s can be reconstructed by solving the following system of equations as

$$x = s_1 \bmod p_1;$$
$$x = s_2 \bmod p_2;$$
$$.$$
$$.$$
$$.$$
$$x = s_t \bmod p_t.$$

Using the standard CRT, a unique solution *x* is given as $x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \cdot s_i \bmod N$, where $N = p_1 \cdot p_2 \cdot \ldots \cdot p_t$, and $\frac{N}{p_i} \cdot y_i \bmod p_i = 1$.

We want to point out that Mignotte's (t,n) threshold SS is not a perfect SS since any share substantially decreases the entropy of the secret.

2.3 Review of Asmuth-Bloom (t,n) SS

Share generation: In Asmuth-Bloom (t,n) SS, the dealer selects p_0 and a sequence of pairwise coprime positive integers, $p_1 < p_2 < \ldots < p_n$, such that $p_0 \cdot p_{n-t+2} \cdot \ldots \cdot p_n < p_1 \cdot p_2 \cdot \ldots \cdot p_t$, and $\gcd(p_0, p_i) = 1, i = 1,2,\ldots,n$, 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, α, such that $s + \alpha p_0 \in Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$. We want to point out that the value, $s + \alpha p_0$, needs to be in the *t*-threshold range, $Z_{p_{n-t+2} \cdot p_{n-t+3} \cdot \ldots \cdot p_n, p_1 \cdot p_2 \cdot \ldots \cdot p_t}$; otherwise, the value, $s + \alpha p_0$, can be obtained with fewer than t shares. However, in the original paper [1], it specifies that the value $s + \alpha p_0$, is in the set, $Z_{p_1 \cdot p_2 \cdot \ldots \cdot p_t}$. This range is different from the *t*-threshold range. In other words, if $s + \alpha p_0$ is selected to be smaller than the lower bound of the *t*-threshold range (i.e., but it is still in the set $Z_{p_1 \cdot p_2 \cdot \ldots \cdot p_t}$), then the value, $s + \alpha p_0$, 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 $s_i = s + \alpha p_0 \bmod p_i$, and s_i is sent to shareholder, U_i, secretly, for $i = 1,2,\ldots,n.$

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

$$x = s_1 \bmod p_1;$$
$$x = s_2 \bmod p_2;$$
$$.$$
$$.$$
$$.$$
$$x = s_t \bmod p_t.$$

Using the standard CRT, a unique solution *x* is given as $x = \sum_{i=1}^{t} \frac{N}{p_i} \cdot y_i \cdot s_i \bmod N$, where $N = p_1 \cdot p_2 \cdot \ldots \cdot p_t$, and $\frac{N}{p_i} \cdot y_i \bmod p_i = 1$. Then, the secret s can be recovered by computing $s = x \bmod p_0$.

Asmuth and Bloom showed that the entropy of the secret decreases "not too much" when $t-1$ shares are known. Interest readers can refer to the original paper [1] for detailed discussion. Asmuth-Bloom's SS can be generalized to take more than *t* shares in the secret reconstruction. For example, when there are *j* (i.e., $t < j \leq n$) shareholders with their shares, $\{s_1, s_2, \ldots, s_j\}$, participating 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 Proposed Scheme

In our proposed scheme, each shareholder has one private share. We assume that the weight of a share can be any integer, j (i.e., $1 \leq j \leq t$), where t is the threshold of the secret sharing scheme. In the secret reconstruction, it needs to satisfy the following conditions: (a) the secret can be reconstructed when the overall weight of shares is t or larger than t, and (b) the secret cannot be reconstructed when the overall weight of shares is smaller than t. The proposed scheme consists of three steps: parameters selection, shares generation and secret reconstruction. We illustrate the scheme in Figure 2.

1. Parameters selection

1.1 The dealer selects an integer p_0 and a sequence of pairwise coprime positive integers, $p_1^1 < p_2^1 ... < p_n^1$, such that $p_0 \cdot p_{n-t+2}^1 \cdot ... \cdot p_n^1 < p_1^1 \cdot p_2^1 \cdot ... \cdot p_t^1$, and $\gcd(p_0, p_i^1) = 1, i = 1,2,...,n,$ where p_i^1 is the public information associated with each shareholder, U_i^1, having his/her share with the minimal weight (i.e., $weight = 1$).

1.2 For this given sequence, the dealer chooses the secret s as an integer in the set Z_{p_0}. The dealer selects an integer, α, such that $s + \alpha p_0 \in Z_{p_{n-t+2}^1 p_{n-t+3}^1 \cdots p_n^1, p_1^1 \cdot p_2^1 \cdots p_t^1}$.

1.3 For each shareholder, U_i^j, having a larger weight, j (i.e., $j > 1$), the dealer selects p_i^j satisfying $\prod_{i=t-j+1}^{t} p_i^1 < p_i^j < \prod_{i=n-t+2}^{n-t+(1+j)} p_i^1$. p_i^j is the public information associated with shareholder, U_i^j. Note that the selected value, p_i^j, should be relatively coprime to all other public parameters of shareholders and $\gcd(p_0, p_i^j) = 1, \forall i, j.$

2. Share generation

Share for the shareholder, U_i^j, is generated as $s_i^j = s + \alpha p_0 \bmod p_i^j$. s_i^j is sent to shareholder, U_i^j, secretly.

3. Secret reconstruction

Given any subset of distinct shares having overall weight *t* or larger than *t*, the secret value, $x = s + \alpha p_0$, can be reconstructed by using the standard CRT. Then, the secret s can be recovered by computing $s = x \bmod p_0$. □

Figure 2: Proposed scheme

Parameters selection:

1. The dealer selects an integer p_0 and a sequence of pairwise coprime positive integers, $p_1^1 < p_2^1 ... < p_n^1$, such that $p_0 \cdot p_{n-t+2}^1 \cdot ... \cdot p_n^1 < p_1^1 \cdot p_2^1 \cdot ... \cdot p_t^1$, where p_i^1 is the public information associated with each shareholder, U_i^1, having his/her share with the minimal weight (i.e., $weight = 1$).

2. For this given sequence, the dealer chooses the secret s as an integer in the set Z_{p_0}. The dealer selects an integer, α, such that $s + \alpha p_0 \in Z_{p_{n-t+2}^1 p_{n-t+3}^1 \cdots p_n^1, p_1^1 \cdot p_2^1 \cdots p_t^1}$.

3. For each shareholder, U_i^j, having a larger weight, j (i.e., $j > 1$), the dealer selects p_i^j satisfying $\prod_{i=t-j+1}^{t} p_i^1 < p_i^j < \prod_{i=n-t+2}^{n-t+(1+j)} p_i^1$. p_i^j is the public information associated with shareholder, U_i^j. Note that the selected value, p_i^j, should be relatively coprime to all other public parameters of shareholders and $\gcd(p_0, p_i^j) = 1, \forall i, j.$

{Remark 2} We want to point out that, in Step 2, the value, $s + \alpha p_0$, needs to be in the t-threshold range, $Z_{p_{n-t+2}^1 p_{n-t+3}^1 \cdots p_n^1, p_1^1 \cdot p_2^1 \cdots p_t^1}$; otherwise, the value, $s + \alpha p_0$, either (a) cannot be obtained with shares having their overall weight equal to or larger than t; or (b) can be obtained with shares having their overall weight smaller than t. The secret value, $s + \alpha p_0$, selected in the t-threshold range can ensure the security requirement of a WSS for shares having the minimal weight. Also, in Step 3, the value, p_i^j, needs to be selected in the specified range, otherwise, the value, $s + \alpha p_0$, either (a) cannot be obtained with shares having their overall weight equal to or larger than t; or (b) can be obtained with shares having their overall weight smaller than t. The following theorem proves this statement.

Theorem 1. If the parameter p_i^j associated with every shareholder, U_i^j, having a larger weight, j (i.e., $j > 1$), satisfies $\prod_{i=t-j+1}^{t} p_i^1 < p_i^j < \prod_{i=n-t+2}^{n-t+(1+j)} p_i^1$, it can ensure that (a) the secret can be reconstructed when the overall weight of shares is t or larger than t, and (b) the secret cannot be reconstructed when the overall weight of shares is smaller than t.

Proof. If the parameter p_i^j associated with every shareholder, U_i^j, having a larger weight, j (i.e., $j > 1$), satisfies $\prod_{i=t-j+1}^{t} p_i^1 < p_i^j < \prod_{i=n-t+2}^{n-t+(1+j)} p_i^1$, then we have $p_{t-j+1}^1 \cdot p_{t-j+2}^1 \cdot ... \cdot p_t^1 < p_i^j < p_{n-t+2}^1 \cdot p_{n-t+3}^1 \cdot ... \cdot p_{n-t+(1+j)}^1$. The condition, $p_{t-j+1}^1 \cdot p_{t-j+2}^1 \cdot ... \cdot p_t^1 < p_i^j$, ensures that the parameter, p_i^j, is larger than the product of j largest parameters, $p_{t-j+1}^1 \cdot p_{t-j+2}^1 \cdot ... \cdot p_t^1$, involved in the upper bound of the t-threshold range. In other words, it ensures that the share associated with the parameter, p_i^j, is to be no smaller than j shares with the minimal weight to be used to recover the secret (i.e., the share of shareholder,

U_i^j, and any $t-j$ shares with the minimal weight can recover the secret). On the other hand, the condition, $p_i^j < p_{n-t+2}^1 \cdot p_{n-t+3}^1 \cdot \ldots \cdot p_{n-t+(1+j)}^1$, ensures that the parameter, p_i^j, is smaller than the product of j smallest parameters, $p_{n-t+2}^1 \cdot p_{n-t+3}^1 \cdot \ldots \cdot p_{n-t+(1+j)}^1$, involved in the lower bound of the t-threshold range. In other words, it ensures that the share associated with this parameter, p_i^j, is limited to be no larger than j shares with the minimal weight to be used to recover the secret (i.e., the share of shareholder, U_i^j, and any $t-j-1$ shares with the minimal weight cannot recover the secret). With both conditions, it ensures that the share associated with the parameter, p_i^j, is equivalent to j shares exactly with the minimal weight.

Let use the following scenarios to illustrate this theorem. We assume that $t=5$ in the following discussion.

(Case 1) If there are 3 shareholders, U_i^2, U_j^2 and U_k^2, with each share having weight 2, the overall weight of their shares is 6. Since parameters associated with these shareholders satisfy $\prod_{i=4}^{5} p_i^1 < p_i^2, p_j^2, p_k^2 < \prod_{i=n-3}^{n-2} p_i^1$, the product of their parameters satisfies

$$p_i^2 \cdot p_j^2 \cdot p_k^2 > \prod_{i=4}^{5} p_i^1 \cdot \prod_{i=4}^{5} p_i^1 \cdot \prod_{i=4}^{5} p_i^1 = p_4^1 \cdot p_4^1 \cdot p_4^1 \cdot p_5^1 \cdot p_5^1 \cdot p_5^1 > p_1^1 \cdot p_2^1 \cdot p_3^1 \cdot p_4^1 \cdot p_5^1.$$

In other words, since the product of their parameters is larger than the upper bound of the *t*-threshold range, they can recover the secret.

(Case 2) If there are 3 shareholders, U_i^1, U_j^2 and U_k^2, with each share having weight either one or two, respectively, the overall weight of their shares is 5. Since parameters associated with shareholders having weight 2 satisfy $\prod_{i=4}^{5} p_i^1 < p_j^2, p_k^2 < \prod_{i=n-3}^{n-2} p_i^1$, the product of their parameters satisfies

$$p_i^1 \cdot p_j^2 \cdot p_k^2 > p_i^1 \cdot \prod_{i=4}^{5} p_i^1 \cdot \prod_{i=4}^{5} p_i^1 = p_i^1 \cdot p_4^1 \cdot p_4^1 \cdot p_5^1 \cdot p_5^1 > p_1^1 \cdot p_2^1 \cdot p_3^1 \cdot p_4^1 \cdot p_5^1.$$

In other words, since the product of their parameters is larger than the upper bound of the *t*-threshold range, they can recover the secret.

(Case 3) If there are 2 shareholders, U_i^2 and U_j^2, with each share having weight two, the overall weight of their shares is 4. Since parameters associated with both shareholders satisfy $\prod_{i=4}^{5} p_i^1 < p_i^2, p_j^2 < \prod_{i=n-3}^{n-2} p_i^1$, the product of their parameters satisfies

$$p_i^2 \cdot p_j^2 < \prod_{i=n-3}^{n-2} p_i^1 = p_{n-3}^1 \cdot p_{n-3}^1 \cdot p_{n-2}^1 \cdot p_{n-2}^1 < p_{n-3}^1 \cdot p_{n-2}^1 \cdot p_{n-1}^1 \cdot p_n^1.$$

In other words, since the product of their parameters is smaller than the lower bound of the *t*-threshold range, they cannot recover the secret.

(Case 4) If there are 2 shareholders, U_i^1 and U_j^3, with each share having weight either one or three, respectively, the overall weight of their shares is 4. Since parameter associated with shareholder, U_j^3, satisfies $\prod_{i=3}^{5} p_i^1 < p_j^3 < \prod_{i=n-3}^{n-1} p_i^1$, the product of their parameters satisfies

$$p_i^1 \cdot p_j^3 < p_i^1 \cdot \prod_{i=n-3}^{n-1} p_i^1 = p_i^1 \cdot p_{n-3}^1 \cdot p_{n-2}^1 \cdot p_{n-1}^1 < p_{n-3}^1 \cdot p_{n-2}^1 \cdot p_{n-1}^1 \cdot p_n^1.$$

In other words, since the product of their parameters is smaller than the lower bound of the *t*-threshold range, they cannot recover the secret.

Remark 3. From Theorem 1, in our proposed scheme, the moduli associated with all shareholders are determined by the moduli associated with shareholders having the minimal weight. For example, let us assume that there are 5 shareholders having the minimal weight one (i.e., $weight=1$), and 1 shareholder having weight two. Then, in our proposed scheme, the modulus associated with the shareholder having weight two is upper bounded by the product, $p_{n-t+2}^1 \cdot p_{n-t+3}^1$. However, in [8, 13], the modulus is larger than the modulus computed in our scheme.

Share generation: Share for the shareholder, U_i^j, is generated as $s_i^j = s + \alpha p_0 \bmod p_i^j$. s_i^j is sent to shareholder, U_i^j, secretly.

Secret reconstruction: Given any subset of distinct shares having overall weight *t* or larger than *t*, the secret value, $x = s + \alpha p_0$, can be reconstructed by using the standard CRT. Then, the secret s can be recovered by computing $s = x \bmod p_0$.

4 Performance and Security Analysis

The most time-consuming computational effort of our proposed scheme is in parameters selection performed by the dealer. This computation only needs once during set up. Share generation and secret reconstruction follow the standard Asmuth-Bloom (t,n) SS [1].

In comparing with existing WSSs based on the CRT, we have only found two papers, [8, 13], in the literature. Both schemes are based on the Mignotte's scheme [18] which information of the secret may be leaked if there are fewer than *t* shareholders participated in the secret reconstruction, but our proposed scheme is based on the Asmuth-Bloom (t,n) SS [1] which does not leak useful information if there are fewer than t shareholders participating in the secret reconstruction [1]. Furthermore, in [8], the dealer needs to find out all minimal subsets of authorized access structure and then determines the modulus of each shareholder accordingly. It is a time-consuming process. In [13], the modulus associated with each shareholder is proportional to the weight of share. But, in our proposed scheme, the modulus associated with each shareholder having a larger weight (i.e., $weight > 1$), is determined by the moduli associated with shareholders having the minimal weight (i.e., $weight = 1$). Therefore, the size of moduli in our proposed scheme is smaller than the moduli in [8, 13]. In addition, since the size of each share of shareholder is proportional to the size of his/her modulus, the private share of shareholders in our proposed scheme is also smaller than the size of shares in [8, 13].

Let us analyze the security of the proposed WSS. Since $s + \alpha p_0 \in Z_{p^1_{n-t+2} p^1_{n-t+3} \cdot \ldots \cdot p^1_n, p^1_1 \cdot p^1_2 \cdot \ldots \cdot p^1_t}$, this can prevent fewer than t shareholders with each share having weight one to recover the secret. Furthermore, with Theorem 1, we can conclude that (a) the secret can be recovered if the overall weight of shares is t or larger than t, and (b) the secret cannot be recovered if the overall weight of shares is smaller than t.

Since our proposed scheme follows Asmuth-Bloom (t, n) SS [1] to generate shares and reconstruct the secret, the security our scheme is the same as the Asmuth-Bloom SS. Asmuth and Bloom showed that the entropy of the secret decreases "not too much" when $t-1$ shares are known. Goldreich et al.[18] showed that any set of $t-2$ shares gives no information on the secret using the zero-knowledge theory provided that the parameters on the system satisfy a natural condition (i.e., the primes p_i's have to be consecutive). Quisquater et al. [17] introduced the concept of an asymptotically perfect and an asymptotically ideal scheme which are natural relaxations of perfect and ideal schemes. They also prove that the (t, n) SS based on the CRT with consecutive primes is asymptotically perfect. In other words, any $t-1$ shares give no information on the secret.

5 Conclusion

We proposed a WSS based on the CRT. The security of our proposed scheme is the same as the Asmuth-Bloom's SS. In our proposed scheme, the modulus associated with all shareholders having weights larger than the minimal weight is determined by the moduli associated with shareholders having the minimal weight. In comparing with other WSSs based on the CRT, the moduli in our proposed scheme are smaller than the moduli in other existing WSSs.

References

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

[2] A. Beimel, T. Tassa, and E. Weinreb, "Characterizing ideal weighted threshold secret sharing," *Theory of Cryptography, Second Theory of Cryptography Conference*, LNCS 3378, pp. 600-619, Cambridge, MA, USA, Springer-Verlag, Feb. 10-12, 2005

[3] Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret secret," in *Crypto '86*, LNCS 263, pp. 251-260,
Springer-Verlag, 1987.

[4] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of AFIPS'79 National Computer Conference*, vol. 48, pp. 313-317, AFIPS Press, 1979.

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

[6] Y. Guo and Y. Zhao, "High-efficient quantum secret sharing based on the Chinese remainder theorem via the orbital angular momentum entanglement analysis," *Quantum Information Processing*, vol. 12, no. 2, pp. 1125-1139, 2013.

[7] L. Harn, F. Miao, and C. C. Chang, "Verifiable secret sharing based on the Chinese remainder theorem," *Security and Communication Networks*, will be published in 2013.

[8] S. Iftene and I. Boureanu, "Weighted threshold secret sharing based on the Chinese remainder theorem," Scientific Annals of the "Al. I. Cuza" University of Iasi, Computer Science Section, XVI, pp. 161-172, 2005.

[9] S. Iftene, *Secret Sharing Schemes with Applications in Security Protocols*, Technical Report, University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science, 2007.

[10] K. Kaya and A. A. Selcuk, "A verifiable secret sharing scheme based on the Chinese Remainder Theorem," in *Advances in Cryptology – Indocrypt '08*, LNCS 5365, pp. 414-425, Springer-Verlag , 2008.

[11] Y. Liu, L. Harn, and C. C. Chang, "An authenticated group key distribution mechanism using theory of numbers," *International Journal of Communication Systems*, will be published in 2013.

[12] Q. Lu, Y. Xiong, W. Huang, X. Gong, and F. Miao, "A distributed ECC-DSS authentication scheme based on CRT-VSS and trusted computing in MANET," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 656-665, 2012.

[13] F. Maino, E. Bertino, Elisa, Y. Sui, K. Wang and F. Li, "A new approach to weighted multi-secret Sharing," in *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, Aug. 4, 2011

[14] Mignotte, “How to share a secret,” in *Cryptography-Proceedings of the Workshop on Cryptography*, LNCS 149, pp. 371-375, Springer-Verlag, 1983.

[15] P. Morillo, C. Padró, G. Sáez, and J. L. Villar, “In Weighted threshold secret sharing schemes,” *Information Processing Letters*, vol. 70, pp. 211-216, 1999.

[16] L. Qiong, W. Zhifang, N. Xiamu, and S. Shenghe, “A non-interactive modular verifiable secret sharing scheme,” in *Proceedings of ICCCAS 2005: International Conference on Communications, Circuits and Systems*, pp. 84-87, IEEE, Los Alamitos, 2005.

[17] M. Quisquater, B. Preneel, and J. Vandewalle, “On the security of the threshold scheme based on the Chinese remainder theorem,” *Public Key Cryptography*, LNCS 2274, pp. 199-210, Springer-Verlag, 2002.

[18] O. Goldreich, D. Ron, and M. Sudan, “Chinese remaindering with errors,” in *Proceedings of the Thirty-first Annual ACM Symposium on the Theory of Computing*, pp. 225-234, New York, USA, 1999.

[19] S. Sarkar, B. Kisku, S. Misra, and M. S. Obaidat, “Chinese Remainder Theorem-based RSA-threshold cryptography in MANET using verifiable secret sharing scheme,” in *Proceedings of the WiMob 2009 - 5th IEEE International Conference on Wireless and Mobile Computing Networking and Communication*, pp. 258-262, 2009.

[20] A. Shamir, “How to share a secret,” *Commun. Assoc. Comp. Mach.*, vol. 22, no. 11, pp. 612-613, 1979.

Lein Harn received his BS degree in Electrical Engineering from the National Taiwan University in 1977. In 1980, he received his MS degree in Electrical Engineering from the State University of New York-Stony Brook and in 1984 he received his Ph. D. degree in Electrical Engineering from the University of Minnesota. Currently, he is a Full Professor at the Department of Computer Science Electrical Engineering, University of Missouri- Kansas City, USA. His research interests are cryptography, network security and wireless communication security. He has published number of papers on digital signature design and applications, wireless and network security.

Miao Fuyou received his Master degree in Computer Science and Technology from the China University of Mining Technology (Beijing) in 1999. In 2005, he received his Ph.D. degree in Computer Science from the University of Science & Technology of China. Currently, he is an associate professor at the School of Computer Science and Technology, University of Science & Technology of China. His research interests are applied cryptography, network security and mobile computing.