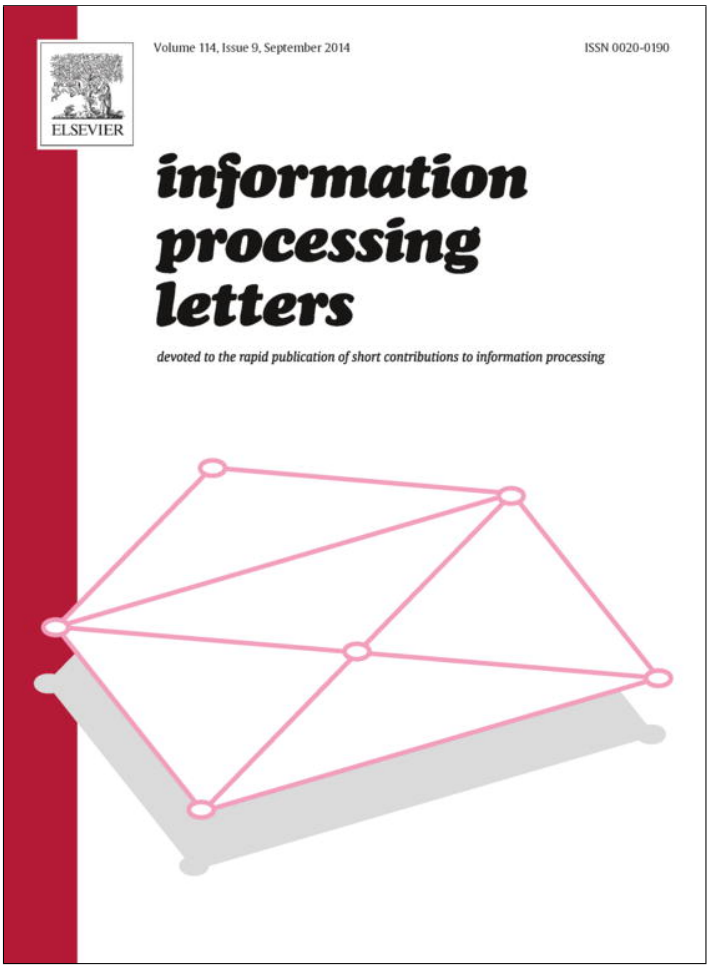

Information Processing Letters 114 (2014) 504–509

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Multilevel threshold secret sharing based on the Chinese Remainder Theorem

Lein Harn [a,*], Miao Fuyou [b]

[a] Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, United States
[b] School of Computer Science and Technology, University of Science & Technology of China, China

ARTICLE INFO

Article history:
Received 30 July 2013
Received in revised form 1 December 2013
Accepted 5 April 2014
Available online 16 April 2014
Communicated by S.M. Yiu

Keywords:
Multilevel secret sharing
Chinese Remainder Theorem
Asmuth–Bloom's secret sharing scheme
Threshold value
Multilevel secret sharing scheme
Cryptography

ABSTRACT

The (t,n) threshold secret sharing schemes (SSs) were introduced by Shamir and Blakley separately in 1979. Multilevel threshold secret sharing (MTSS) is a generalization of classical threshold SS, and it has been studied extensively in the literature. In an MTSS, shareholders are classified into different security subsets. The threshold value of a higher-level subset is smaller than the threshold value of a lower-level subset. Shareholders in each subset can recover the secret if the number of shares available is equal to or more than a threshold value. Furthermore, the share of a shareholder in a higher-level subset can be used as a share in the lower-level subset to recover the secret. Chinese Remainder Theorem (CRT) is one of popular tools used for designing SSs. For example, the Mignotte's scheme and Asmuth–Bloom's scheme are two classical (t,n) threshold SSs based on the CRT. So far, there was no CRT-based MTSS in the literature. In this paper, we propose the first MTSS based on the CRT. In our proposed scheme, one unique feature is that each shareholder needs to keep only one private share. Our proposed scheme is based on the Asmuth–Bloom's SS which is unconditionally secure.

1. Introduction

In a secret sharing scheme (SS), a dealer divides a secret s into n shares and shared among a set of n *shareholders*, $U=\{U_1,U_2,\ldots,U_n\}$, in such a way that any authorized subset can reconstruct the secret s; whereas any un-authorized subset cannot recover the secret s. The (t,n) threshold secret sharing schemes were introduced by Shamir [1] and Blakley [2] separately in 1979. A (t,n) threshold secret sharing scheme allows any t or more than t shareholders to reconstruct the secret s; while any fewer than t shareholders cannot reconstruct the secret s. In Shamir's (t,n) threshold SS, a dealer generates n shares based on a $t-1$ degree polynomial. Secret reconstruction is based on the Lagrange interpolating polynomial of any t private shares. Shamir's (t,n) SS is unconditionally secure. There are other types of SSs. For example, Blakley's scheme [1] is based on the geometry, Mignotte's scheme [3] and Asmuth–Bloom's scheme [4] are based on the Chinese Remainder Theorem (CRT).

Multilevel threshold secret sharing (MTSS) is a generalization of classical threshold SS, and it has been studied extensively in the literature [5–10]. In an MTSS, all shareholders play different roles; while in a classical threshold SS, all shareholders play the same role. Simmons [9] considered a setting where all shareholders are partitioned into different levels, $L_1,L_2,\ldots,L_m$, and each level, L_i, is assigned with a threshold value t_i, for $i=1,2,\ldots,m$. Note that throughout this paper, the notations, L_i and L_j, where $i<j$, indicate that the level L_i is higher than the level L_j. In an MTSS scheme, when there are at least t_i shareholders belonging to levels higher than or equal to the level L_i, this subset of shareholders can reconstruct the secret. For example, we assume that thresholds are $t_1=2$ in level

* Corresponding author.

http://dx.doi.org/10.1016/j.ipl.2014.04.006
0020-0190/

L_1 and $t_2 = 3$ in level L_2. Then, two shareholders in L_1, or three shareholders in L_2 can reconstruct the secret. In addition, when there are one shareholder in L_1 and two shareholders in L_2, this combination of shareholders can also reconstruct the secret.

Brickell [6] proposed an ideal MTSS. However, his scheme is inefficient since the dealer is required to compute exponentially to ensure non-singular matrices. Ghodosi et al. [7] proposed an ideal MTSS scheme based on Shamir's threshold SS; but their schemes only work for small number of shareholders. Lin et al. [10] proposed an ideal MTSS based on the polynomial in 2009.

The CRT has been a popular tool used for designing SSs. For example, the Mignotte's scheme [3] and Asmuth–Bloom's scheme [4] are two classical (t, n) threshold SSs. Kaya et al. [11] 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 [12]. The security of their VSS is based on the RSA assumption [13]. In addition, in 2009, Sarkar et al. [14] have proposed a CRT-based RSA-threshold cryptography for a mobile ad hoc network (MANET) and in 2011, Lu et al. have proposed a secret key distributed storage scheme [15] based on CRT-VSS and trusted computing technology. Quisquater et al. [16] have shown that Asmuth–Bloom's SS [4] is asymptotically optimal both from an information theoretic and complexity theoretic viewpoint when the parameters satisfy a simplified relationship.

So far, there was no CRT-based MTSS in the literature. In this paper, we propose the first MTSS based on Asmuth–Bloom's scheme [4] which is unconditionally secure. One unique feature of our proposed scheme is that each shareholder needs to keep only one private share. This private share can also be used in the lower-level subsets to recover the secret.

The rest of this paper is organized as follows. In the next section, we introduce some preliminaries that include the definition of MTSS, the CRT, Mignotte's and Asmuth–Bloom schemes based on the CRT. In Section 3, we propose an MTSS based on a simple modification of Asmuth–Bloom scheme. In Section 4, we include the security analysis of our proposed scheme. Conclusion is given in Section 5.

2. Preliminaries

In this section, we introduce some preliminaries that are the fundamentals in our design including a definition of MTSS, the CRT, Mignotte's and Asmuth–Bloom schemes based on the CRT.

2.1. Definition of MTSS

Definition 1 *(Authorized set in a multilevel threshold secret sharing scheme).* Let $L_1, L_2, ..., L_m$, denote a partition of shareholders, $(U_1, U_2, ..., U_n)$, into multiple security levels, i.e., $U = (U_1, U_2, ..., U_n) = \bigcup_{j=1}^{m} L_j$. Let $T = (t_1, t_2, ..., t_m)$ denote a sequence of threshold values, where $1 \le t_j \le |L_1| + |L_2| + ... + |L_j|$ for $j = 1, 2, ..., m$, and $t_1 < t_2 < ... < t_m$. The authorized set (MA) of n shareholders in an (L, T) multilevel threshold secret sharing (MTSS) scheme is defined as

$$MA = \left\{ A \subseteq (U_1, U_2, ..., U_n) \;\middle|\; \exists i \in \{1, 2, ..., m\} \text{ and } \left| A \cap \bigcup_{j=1}^{i} L_j \right| \ge t_i \right\},$$

where $A = (U_{i_1}, U_{i_2}, ..., U_{i_t})$ and $U_{ik} \ne U_{ij}$ if $k \ne j$ for any subset $\{i_1, i_2, ..., i_t\}$ of $\{1, 2, ..., n\}$.

2.2. The Chinese Remainder Theorem (CRT) [17]

Given following system of equations as

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

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 $N = p_1 \cdot p \cdot ... \cdot p_t$, if all moduli are pairwise coprime (i.e., $\gcd(p_i, p_j) = 1$, for every $i \ne j$).

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 of $\frac{1}{4}$. The CRT can also be used in the SS. Each of the shares is represented in a congruence, and the solution of the system of congruences 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 a certain cardinality. In the next subsections, we will review two most well-known SSs based on the CRT.

2.3. Review of Mignotte's (t, n) SS

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

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

Remark 1. The numbers in the t-threshold range, $Z_{p_{n-t+2} \cdot ... \cdot p_n, p_1 \cdot p_2 \cdot ... \cdot p_t}$, are integers upper bounded by $p_1 \cdot p_2 \cdot ... \cdot p_t$, which is the smallest product of any t moduli, and lower bounded by $p_{n-t+2} \cdot p_{n-t+3} \cdot ... \cdot p_n$, which is the largest product of any $t-1$ moduli. The secret, s, selected 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 the upper bound, $p_1 \cdot p_2 \cdot \ldots \cdot p_t$), 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 the lower bound, $p_{n-t+2} \cdot \ldots \cdot p_n$). 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, $\{s_{i_1}, s_{i_2}, \ldots, s_{i_t}\}$, the secret s can be reconstructed by solving the following system of equations as

$$x = s_{i_1} \bmod p_{i_1};$$
$$x = s_{i_2} \bmod p_{i_2};$$
$$\vdots$$
$$x = s_{i_t} \bmod p_{i_t}.$$

Using the standard CRT, a unique solution x is given as $x = \sum_{r=1}^{t} \frac{N}{p_{i_r}} \cdot y_{i_r} \cdot s_{i_r} \bmod N$, where $N = p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_t}$, and $\frac{N}{p_{i_r}} \cdot y_{i_r} \bmod p_{i_r} = 1$.

In Mignotte's (t, n) threshold SS, information of the secret may be leaked if there are fewer than t shareholders participated in the secret reconstruction.

2.4. Review of Asmuth–Bloom (t, n) SS [4]

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 [4], 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 range, $Z_{p_1 \cdot p_2 \cdot \ldots \cdot p_t}$), 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, $\{s_{i_1}, s_{i_2}, \ldots, s_{i_t}\}$, the secret s can be reconstructed by solving the following system of equations as

$$x = s_{i_1} \bmod p_{i_1};$$
$$x = s_{i_2} \bmod p_{i_2};$$
$$\vdots$$
$$x = s_{i_t} \bmod p_{i_t}.$$

Using the standard CRT, a unique solution x is given as $x = \sum_{r=1}^{t} \frac{N}{p_{i_r}} \cdot y_{i_r} \cdot s_{i_r} \bmod N$, where $N = p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_t}$, and $\frac{N}{p_{i_r}} \cdot y_{i_r} \bmod p_{i_r} = 1$. Then, the secret s can be recovered by computing $s = x \bmod p_0$.

Asmuth–Bloom (t, n) SS does not leak useful information if there are fewer than t shareholders participating in the secret reconstruction [4].

3. Proposed scheme

In our proposed scheme, each shareholder has to keep only one share. We assume that shareholders are classified into m subsets, L_i, $i = 1, 2, \ldots, m$, where L_m is the lowest level of subsets and L_1 is the highest level of subsets. Each subset, L_i, has the threshold, t_i. Shares belonging to the subset, L_i, or any subset with higher security level than the subset, L_i, can be used to recover the secret, s, if the number of shares available is equal to or more than the threshold, t_i (i.e., $\geq t_i$). The threshold of a higher-level subset is always smaller than the threshold of a lower-level subset (i.e., $t_j > t_i$ if $i < j$). In the secret reconstruction by shares in the subset, L_i, and in any subset with higher security level, it needs to satisfy the following conditions: (a) the secret can be reconstructed if the number of shares is t_i or more than t_i, and (b) the secret cannot be reconstructed when the number of shares is fewer than t_i. The proposed scheme consists of two phases: shares generation and secret reconstruction.

Share generation: The dealer selects an integer p_0 initially. For each subset, L_i, having n_i shareholders, the dealer selects a sequence of pairwise coprime positive integers, $p_1^i < p_2^i < \ldots < p_{n_i}^i$, such that $p_0 \cdot p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+3}^i \cdot \ldots \cdot p_{n_i}^i < p_1^i \cdot p_2^i \cdot \ldots \cdot p_{t_i}^i$, and $\gcd(p_0, p_k^i) = 1$, $k = 1, 2, \ldots, n_i$, where p_k^i is the public information associated with shareholder, U_k^i, in the subset L_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_i, such that $p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+3}^i \cdot \ldots \cdot p_{n_i}^i < s + \alpha_i p_0 < p_1^i \cdot p_2^i \cdot \ldots \cdot p_{t_i}^i$. We want to point out that the value, $s + \alpha_i p_0$, needs to be in the t_i-threshold range, $Z_{p_{n_i-t_i+2}^i p_{n_i-t_i+3}^i \cdot \ldots \cdot p_{n_i}^i, p_1^i \cdot p_2^i \cdot \ldots \cdot p_{t_i}^i}$; otherwise, the value, $s + \alpha_i p_0$, can be obtained with fewer than t_i shares. Share for the shareholder, U_k^i, is generated as $s_k^i = s + \alpha_i p_0 \bmod p_k^i$. s_k^i is sent to shareholder, U_k^i, secretly.

Furthermore, in order to enable private share, s_k^i, of the shareholder, U_k^i, in L_i to be used as a share in L_j, the dealer needs to select a parameter, $p_{k,j}^i$, such that $p_{t_j}^j < p_{k,j}^i < p_{n_j-t_j+2}^j$. Then, the dealer computes $\Delta s_{k,j}^i$ such that $(s + \alpha_j p_0 - s_k^i) \bmod p_{k,j}^i = \Delta s_{k,j}^i$ (i.e., $s + \alpha_j p_0 - (s_k^i + \Delta s_{k,j}^i) = \beta_{k,j}^i p_{k,j}^i$). Note that the private share, s_k^i, needs to be modified into $s_k^i + \Delta s_{k,j}^i$ if it is used as a share in the lower security level, L_j, and is associated with the modulus, $p_{k,j}^i$. $(\Delta s_{k,j}^i, p_{k,j}^i)$ is the public information associated with shareholder, U_k^i, while participating in the secret reconstruction in the subset L_j. All selected $p_{k,j}^i$ should be relatively coprime to all other moduli. The value,

$p^i_{k,j}$, needs to be selected in the specified range, otherwise, either (a) the secret $s+\alpha_j p_0$ can be obtained with fewer than t_j shares, or (b) the secret $s+\alpha_j p_0$ cannot be obtained with t_j or more than t_j shares. Theorem 1 will prove this statement.

In summary, at the end of this phase, each shareholder, U^i_k, in the subset, L_i, will have one private share, s^i_k, and following public information, where p^i_k is the modulus used in the subset, L_i, and $(\Delta s^i_{k,j}, p^i_{k,j})$, for $j=i+1, i+2, \ldots, m$, are share modification and modulus used in other subsets (i.e., $i<j$). Furthermore, we want to point out the following trade-offs in our proposed scheme. That are, (a) each shareholder keeps only one share, and (b) there is public information associated with each shareholder, U^i_k, while participating in the secret reconstruction in other subset L_j.

Theorem 1. *If $p^j_{t_j} < p^i_{k,j} < p^j_{n_j-t_j+2}$, where $j>i$, the share s^i_k in L_i used as a share in L_j reconstructing the secret satisfies (a) the secret can be reconstructed when the number of shares is t_j or more than t_j, and (b) the secret cannot be reconstructed when the number is fewer than t_j.*

Proof. If $p^j_{t_j} < p^i_{k,j} < p^j_{n_j-t_j+2}$, the condition, $p^j_{t_j} < p^i_{k,j}$, ensures that the parameter, $p^i_{k,j}$, is larger than the largest modulus in the upper bound of the t_j-threshold range. In other words, it ensures that when the share is used as a share in the subset, L_j, the modulus associated with this share is no smaller than the largest modulus in the t_j-threshold range. Thus, this share and t_j-1 other shares in the subset, L_j, can recover the secret. On the other hand, the condition, $p^i_{k,j} < p^j_{n_j-t_j+2}$, ensures that the modulus, $p^i_{k,j}$, is smaller than the smallest modulus in the lower bound of the t_j-threshold range. In other words, it ensures that when the share is used as a share in the subset, L_j, the modulus associated with this share is no larger than the smallest modulus in the lower bound of the t_j-threshold range. Thus, this share and t_j-2 other shares in the subset, L_j, cannot recover the secret. In summary, with both conditions, it ensures that this share is equivalent to one share exactly in the lower-level subset.

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

(Case 1) Assume that there are 4 shareholders, U^j_r, $r=1,2,3,4$, in the subset, L_j, and one shareholder, U^i_5, in the subset, L_i, where $j>i$. In this case, the total number of shares in the subset, L_j, is 5. Thus, the share of shareholder, U^i_5, can be used as a share in the subset, L_j, to recover the secret. Let us examine this case. Since $p^j_5 < p^i_{5,j} < p^j_{n_j-3}$, the product of all moduli associated with these shareholders satisfies $p^j_1\cdot p^j_2\cdot p^j_3\cdot p^j_4\cdot p^i_{5,j} > p^j_1\cdot p^j_2\cdot p^j_3\cdot p^j_4\cdot p^j_5$. In other words, since the product of their moduli is larger than the upper bound of the t_j-threshold range, the secret can be recovered.

(Case 2) We assume that there are 3 shareholders, U^j_r, $r=1,2,3$, in the subset, L_j, and one shareholder, U^i_4, in the subset, L_i, where $j>i$. The total number of shares in the subset, L_j, is 4. Thus, the share of shareholder, U^i_4, cannot be used as a share in the subset, L_j, to recover the secret. Let us examine this case. Since $p^j_5 < p^i_{4,j} < p^j_{n_j-3}$, the product of all moduli of these shareholders satisfies $p^j_1\cdot p^j_2\cdot p^j_3\cdot p^i_{4,j} < p^j_{n_j-3}\cdot p^j_{n_j-2}\cdot p^j_{n_j-1}\cdot p^j_{n_j}$. In other words, since the product of their moduli is smaller than the lower bound of the t_j-threshold range, the secret cannot be recovered. □

Secret reconstruction: The secret can be recovered if the number of shares belonging to the subset, L_j, or any subset with higher security level than the subset, L_j, is equal to or more than the threshold, t_j (i.e., $\geq t_j$). A system of equations can be established based on all shares. Any share, s^i_k, of shareholder, U^i_k, belonging to a subset with a higher security level needs to be modified as $(s^i_k+\Delta s^i_{k,j})$, and $p^i_{k,j}$ is used as the modulus corresponding to the modified share, $(s^i_k+\Delta s^i_{k,j})$, of shareholder, U^i_k, in constructing the system of equations. Using the standard CRT, a unique solution $x=s+\alpha_j p_0$ can be obtained. Then, the secret s is recovered by computing $s=x \bmod p_0$.

Remark 2. During the secret reconstruction, there is no need of the dealer and no need to compute $\beta^i_{k,j}$ by shareholder, U^i_k. The relation, $s+\alpha_j p_0-(s^i_k+\Delta s^i_{k,j})=\beta^i_{k,j}p^i_{k,j}$ specified in the share generation ensures that the modified share, $s^i_k+\Delta s^i_{k,j}$ (i.e., $i<j$), of shareholder, U^i_k, can be used as a share in the subset L_j, and is associated with the modulus, $p^i_{k,j}$.

We use the following numerical example to illustrate our proposed scheme.

Example 1. In this example, we assume that shareholders are classified into 3 subsets, L_i, $i=1,2,3$, where L_3 is the lowest level of subsets and L_1 is the highest level of subsets. The thresholds of subsets are $t_1=2$, $t_2=3$ and $t_3=4$. Furthermore, the numbers of shareholders in subsets are $n_1=3$, $n_2=4$ and $n_3=5$. The share of a shareholder in the higher-level subset, L_i, can be used as a share in the lower-level subset, L_j, to recover the secret (i.e., $i<j$).

The dealer selects a secret, $s=102$, and $p_0=113$, initially. In the subset, L_1, the integers associated with shareholders, U^1_k, $k=1,2,3$, are $p^1_1=137$, $p^1_2=139$, and $p^1_3=250$. The t_1-threshold range is $(250, 19\,043)$. The dealer selects $\alpha_1=150$ and $s+\alpha_1 p_0=17\,052$ which is in the above range. The shares are $s^1_1=64$, $s^1_2=94$, and $s^1_3=52$.

In the subset, L_2, the integers associated with shareholders, U^2_k, $k=1,2,3,4$, are $p^2_1=293$, $p^2_2=307$, $p^2_3=313$, and $p^2_4=319$. The t_2-threshold range is $(99\,847, 28\,154\,663)$. The dealer selects $\alpha_2=6864$ and $s+\alpha_2 p_0=775\,734$ which is in the above range. The shares are $s^2_1=163$, $s^2_2=252$, $s^2_3=120$ and $s^2_4=245$.

In the subset, L_3, the integers associated with shareholders, U^3_k, $k=1,2,\ldots,7$, are $p^3_1=229$, $p^3_2=233$, $p^3_3=239$, $p^3_4=241$, $p^3_5=277$, $p^3_6=281$, and $p^2_7=283$. The t_3-threshold range is $(22\,027\,871, 3\,073\,309\,843)$. The dealer

selects $\alpha_3 = 194946$ and $s + \alpha_3 p_0 = 22029000$ which is in the above range. The shares are $s_1^3 = 116$, $s_2^3 = 15$, $s_3^3 = 131$, $s_4^3 = 154$, $s_5^3 = 21$, $s_6^3 = 5$, and $s_7^3 = 280$.

Shares of shareholders in the higher-level subset, L_i, for example U_3^1 in the subset, L_1, and U_3^2 and U_4^2 in the subset, L_2, can be used as shares in the subset, L_3. The dealer first selects moduli, $p_{3,3}^1 = 263$, $p_{3,3}^2 = 269$ and $p_{4,3}^2 = 251$ which satisfy $241 = p_4^3 < p_{1,3}^1, p_{1,3}^2, p_{4,3}^2 < p_5^3 = 277$ and are coprime to one another. Then, the dealer evaluates $\Delta s_{3,3}^1$, $\Delta s_{3,3}^2$ and $\Delta s_{4,3}^2$ accordingly, where $(\Delta s_{k,j}^i, p_{k,j}^i)$ is the public information associated with the shareholder, U_k^i, while participating in the subset L_j. Thus, the dealer evaluates $((s + \alpha_3 p_0 - s_3^1) \bmod p_{3,3}^1) = (22029000 - 52) \bmod 263 = 68$ and the public information associated with U_3^1 in the subset, L_3, is $(68, 263)$. In the same way, the public information associated with U_3^2 and U_4^2, $(\Delta s_{3,3}^2, p_{3,3}^2)$ and $(\Delta s_{4,3}^2, p_{4,3}^2)$, respectively, in the subset L_3, are computed as $(201, 269)$ and $(242, 251)$.

Now, let us consider following cases in reconstructing the secret.

(Case 1) Assume that U_3^1 in the subset L_1, U_4^2 in the subset L_2, and U_3^3 and U_6^3 in the subset L_3, work together to recover the secret. Since the total number of shares in the subset L_3 is 4, they can use their shares, $s_3^1 = 52$, $s_4^2 = 245$, $s_3^3 = 131$, $s_6^3 = 5$, and the public information, $(\Delta s_{3,3}^1, p) = (68, 263)$, $(\Delta s_{4,3}^2, p_{4,3}^2) = (242, 251)$, $p_3^3 = 239$, $p_6^3 = 281$, to compute the secret by solving the following system of equations as

$$
\begin{aligned}
x &= \left(s_3^1 + \Delta s_{3,3}^1\right) \bmod p_{3,3}^1;\\
x &= \left(s_4^2 + \Delta s_{4,3}^2\right) \bmod p_{4,3}^2;\\
x &= s_3^3 \bmod p_3^3;\\
x &= s_6^3 \bmod p_6^3.
\end{aligned}
$$

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

$$
\begin{aligned}
x &= \left(\frac{N}{p_{3,3}^1} \cdot y_{3,3}^1 \cdot \left(\left(s_3^1 + \Delta s_{3,3}^1\right) \bmod p_{3,3}^1\right)\right.\\
&\quad + \frac{N}{p_{4,3}^2} \cdot y_{4,3}^2 \cdot \left(\left(s_4^2 + \Delta s_{4,3}^2\right) \bmod p_{4,3}^2\right)\\
&\quad \left. + \frac{N}{p_3^3} \cdot y_3^3 \cdot s_3^3 + \frac{N}{p_6^3} \cdot y_6^3 \cdot s_6^3\right) \bmod N\\
&= \left(16856909 \cdot 218 \cdot \left((68 + 52) \bmod 263\right)\right.\\
&\quad + 17662817 \cdot 161 \cdot \left((242 + 245) \bmod 251\right)\\
&\quad + 18549653 \cdot 221 \cdot 131\\
&\quad \left. + 15777107 \cdot 170 \cdot 5\right) \bmod 4433367067\\
&= (440976739440 + 671116394732\\
&\quad + 537031004003\\
&\quad + 13410540950) \bmod 4433367067\\
&= 22029000.
\end{aligned}
$$

Then, the secret is obtained as $s = x \bmod p_0 = 22029000 \bmod 113 = 102$.

(Case 2) Assume that U_3^2 and U_4^2 in the subset L_2, and U_1^3 and U_2^3 in the subset L_3, work together to recover the secret. Since the total number of shares in the subset L_3 is 4, they are able to compute the secret by solving the following system of equations as

$$
\begin{aligned}
x &= \left(s_3^2 + \Delta s_{3,3}^2\right) \bmod p_{3,3}^2;\\
x &= \left(s_4^2 + \Delta s_{4,3}^2\right) \bmod p_{4,3}^2;\\
x &= s_1^3 \bmod p_1^3;\\
x &= s_2^3 \bmod p_2^3.
\end{aligned}
$$

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

$$
\begin{aligned}
x &= \left(\frac{N}{p_{3,3}^2} \cdot y_{3,3}^2 \cdot \left(\left(s_3^2 + \Delta s_{3,3}^2\right) \bmod p_{3,3}^2\right)\right.\\
&\quad + \frac{N}{p_{4,3}^2} \cdot y_{4,3}^2 \cdot \left(\left(s_4^2 + \Delta s_{4,3}^2\right) \bmod p_{4,3}^2\right)\\
&\quad \left. + \frac{N}{p_1^3} \cdot y_1^3 \cdot s_1^3 + \frac{N}{p_2^3} \cdot y_2^3 \cdot s_2^3\right) \bmod N\\
&= \left(13392607 \cdot 14 \cdot \left((120 + 201) \bmod 269\right)\right.\\
&\quad + 14353033 \cdot 123 \cdot \left((245 + 242) \bmod 251\right)\\
&\quad + 15731927 \cdot 97 \cdot 116\\
&\quad \left. + 15461851 \cdot 8 \cdot 15\right) \bmod 3602611283\\
&= (9749817896 + 416639841924 + 177015642604\\
&\quad + 1855422120) \bmod 3602611283\\
&= 22029000.
\end{aligned}
$$

Then, the secret is obtained as $s = x \bmod p_0 = 22029000 \bmod 113 = 102$.

(Case 3) Assume that U_3^1 in the subset L_1, U_4^2 in the subset L_2, and U_5^3 in the subset L_3, work together to recover the secret. Since the total number of shares in the subset L_3 is 3, in the following discussion, we show that they cannot use their shares, $s_3^1 = 52$, $s_4^2 = 245$, $s_5^3 = 21$, and the public information, $(\Delta s_{3,3}^1, p_{3,3}^1) = (68, 263)$, $(\Delta s_{4,3}^2 p_{4,3}^2) = (242, 251)$ and $p_5^3 = 277$, to obtain the secret. With their shares, they can form the following system of equations as

$$
\begin{aligned}
x &= \left(s_3^1 + \Delta s_{3,3}^1\right) \bmod p_{3,3}^1;\\
x &= \left(s_4^2 + \Delta s_{4,3}^2\right) \bmod p_{4,3}^2;\\
x &= s_5^3 \bmod p_5^3.
\end{aligned}
$$

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

$$
\begin{aligned}
x' &= \left(\frac{N'}{p_{3,3}^1} \cdot y_{3,3}^1 \cdot \left(\left(s_3^1 + \Delta s_{3,3}^1\right) \bmod p_{3,3}^1\right)\right.\\
&\quad + \frac{N'}{p_{4,3}^2} \cdot y_{4,3}^2 \cdot \left(\left(s_4^2 + \Delta s_{4,3}^2\right) \bmod p_{4,3}^2\right)\\
&\quad \left. + \frac{N'}{p_5^3} \cdot y_5^3 \cdot s_5^3\right) \bmod N'\\
&= (69527 \cdot 36 \cdot 120 + 72851 \cdot 107 \cdot 236
\end{aligned}
$$

$$+ 66\,013 \cdot 121 \cdot 21) \bmod 18\,285\,601$$
$$= 2\,307\,729\,125 \bmod 18\,285\,601$$
$$= 3\,743\,399.$$

Then, they obtain $s' = x' \bmod p_0 = 3\,743\,399 \bmod 113 = 48$ which is different from the secret.

4. Security analysis

Let us analyze the security in the secret reconstruction. First, since $s + \alpha_i p_0 \in Z_{p^i_{n_i-t_i+2} p^i_{n_i-t_i+3} \cdot \ldots \cdot p^i_{n_i} \cdot p^i_1 \cdot p^i_2 \cdot \ldots \cdot p^i_{t_i}}$, this condition can ensure that (a) the secret can be recovered if there are t_i or more than t_i shares; and (b) the secret cannot be obtained if there are fewer than t_i shareholders. With Theorem 1, we can conclude that (a) the secret can be recovered if the total number of available shares in the subsets, $\{L_1, L_2, \ldots, L_i\}$, is t_i or more than t_i, and (b) the secret cannot be recovered if the total number of shares in the subsets, $\{L_1, L_2, \ldots, L_i\}$, is less than t_i.

Just like the Asmuth–Bloom (t, n) SS [4], this proposed scheme is a unconditionally SS since the security does not depend any computational assumption. Let us assume that in our proposed secret reconstruction, there are $t_i - 1$ shareholders available and the product of their moduli is N'. Then, with their shares, shareholders can use CRT to obtain a value, $0 < x' < N'$, where $N' < p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+3} \cdot \ldots \cdot p^i_{n_i}$. This recovered value, x', is not the real secret; but has the following relation, $x = x' + \lambda N'$, with respect to the real secret value, $x = s + \alpha_i p_0$. By properly guessing λ, the secret may be obtained. However, there is only one real value out of $\frac{p^i_1 \cdot p^i_2 \cdot \ldots \cdot p^i_t - p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+3} \cdot \ldots \cdot p^i_{n_i}}{p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+3} \cdot \ldots \cdot p^i_{n_i}} > p_0 - 1$ possible values, where $p^i_1 \cdot p^i_2 \cdot \ldots \cdot p^i_t - p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+3} \cdot \ldots \cdot p^i_{n_i}$ is the length of the t_i-threshold range. Since the collection of possible values of λ is no less than the collection of possible values of the secret s, no useful information is leaked from the collection of shares.

The security of this secret reconstruction is the same as the Asmuth–Bloom's SS which is unconditionally secure.

5. Conclusion

We proposed the first MTSS based on the CRT. The security of our proposed scheme is the same as the Asmuth–Bloom's SS which is unconditionally secure. In our proposed scheme, shareholders are classified into different security subsets and each subset has different threshold. The secret can be recovered when there are enough number of shares available. In an MTSS, any share in the higher-level subset can be used as a share in the lower-level subset to recover the secret. One unique feature of our proposed MTSS is that each shareholder keeps only one private share.

References

[1] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[2] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of AFIPS'79 Nat. Computer Conf., vol. 48, AFIPS Press, 1979, pp. 313–317.

[3] M. Mignotte, How to share a secret, in: Proc. of the Workshop on Cryptography, Springer, Heidelberg, 1983, pp. 371–375.

[4] C.A. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Trans. Inf. Theory IT-29 (2) (1983) 208–210.

[5] E. Ballico, G. Boato, C. Fontanari, F. Granelli, Hierarchical secret sharing in ad hoc networks through birkhoff interpolation, in: Proc. the IEEE International Conference on Telecommunications and Networking, Springer-Verlag, 2006, pp. 157–164.

[6] E.F. Brickell, Some ideal secret sharing schemes, J. Comb. Math. Comb. Comput. 6 (1989) 105–113.

[7] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, Secret sharing in multilevel and compartmented groups, in: Proc. ACISP 1998, in: Lect. Notes Comput. Sci., vol. 1438, Springer-Verlag, 1998, pp. 367–378.

[8] Y. Zhang, Z. Liu, G. Huang, Sure interpolation and its application to hierarchical threshold secret sharing scheme, in: International Symposium on Computer Science and Computational Technology (ISCSCT'08), 2008, pp. 447–450.

[9] G.J. Simmons, How to (really) share a secret, in: Proc. CRYPTO 1988, in: Lect. Notes Comput. Sci., vol. 403, Springer-Verlag, 1988, pp. 390–448.

[10] C. Lin, L. Harn, D. Yea, Ideal hierarchical $(t; n)$ secret sharing schemes, in: Proceedings of the Fifth International Conference on Information Assurance and Security (IAS'09), Xi'an, China, Aug. 18–20, 2009.

[11] K. Kaya, A.A. Selcuk, A verifiable secret sharing scheme based on the Chinese Remainder Theorem, in: Advances in Cryptology – INDOCRYPT'08, in: Lect. Notes Comput. Sci., vol. 5365, 2008, pp. 414–425.

[12] F. Boudot, Efficient proofs that a committed number lies in an interval, in: Proc. of EUROCRYPT 2000, in: Lect. Notes Comput. Sci., vol. 1807, Springer-Verlag, 2000, pp. 431–444.

[13] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.

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

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

[16] M. Quisquater, B. Preneel, J. Vandewalle, On the security of the threshold scheme based on the Chinese remainder theorem, in: Public Key Cryptography, in: Lect. Notes Comput. Sci., vol. 2274, Springer-Verlag, 2002, pp. 199–210.

[17] H. Cohen, A Course in Computational Algebraic Number Theory, 4th ed., Grad. Texts Math., Springer–Verlag, 2000.