Research Article

Unordered Multisecret Sharing Based on Generalized Chinese Remainder Theorem

Xiaoping Li,¹ Hefeng Chen,² Yanjun Liu,³ and Chin-Chen Chang^{3,4}

¹*School of Mathematical Science, University of Electronic Science and Technology of China, Chengdu 611731, China*

²*Computer Engineering College, Jimei University, Xiamen 361021, China*

³*Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan*

⁴*School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China*

Correspondence should be addressed to Chin-Chen Chang; alan3c@gmail.com

Received 24 November 2019; Revised 30 March 2020; Accepted 22 June 2020; Published 14 July 2020

Academic Editor: Kuo-Hui Yeh

Copyright © 2020 Xiaoping Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Multisecret sharing schemes have been widely used in the area of information security, such as cloud storage, group authentication, and secure parallel communications. One of the issues for these schemes is to share and recover multisecret from their shareholders. However, the existing works consider the recovery of multisecret only when the correspondences between the secrets and their shares are definite. In this paper, we propose a multisecret sharing scheme to share and recover two secrets among the participants based on the generalized Chinese Remainder Theorem (GCRT), where the multisecret and their shares are unordered. To overcome the leakage of information, we propose an improved scheme including the improved sharing phase and the recovery phase. The improved scheme has not only a more secure performance but also a lower computation complexity. The conditions for recovery failure and success are also explored.

1. Introduction

Secret sharing plays a critical role in numerous applications, such as in threshold cryptography, access control, cloud computing, data hiding, and digital watermarking [1–3]. In a secret-sharing scheme (SS), a dealer divides a secret into several pieces and then shares them among the shareholders. In 1979, Shamir and Blakley independently introduced the threshold schemes based on the interpolating polynomial in [4] and the linear projective geometry in [5], respectively. For a (t, n) SS with threshold t , a secret s is divided into n pieces to be sheared among n shareholders by a dealer. It shows that the secret can be recovered by any no less than t shares, while the recovery failure with fewer than t shares. Besides this kind of SS scheme, there are many other types, such as Mignotte's scheme [6], the Chinese Remainder Theorem- (CRT-) based Asmuth-Bloom scheme [7] and its generalizations [8, 9], and ramp secret-sharing scheme [10, 11].

Naturally, a secret-sharing scheme can be generalized to the case of multiple secrets, i.e., multisecret sharing [12, 13]. Several schemes for multisecret sharing have been proposed in [14–22]. According to the way of recovering, the existing works can be grouped into two categories. One is to recover multisecret in a stage-by-stage way, the other is to recover multisecret simultaneously. In [15], a one-way function-based multistage secret-sharing scheme was proposed to share multisecret. The authors presented a public shift scheme to obtain the true pieces and then used the proper one-way function to reconstruct the secrets stage-by-stage in a predetermined order. For this scheme, it needs a large number of public values. An improved method was proposed in [16], where a less number of public values is needed. In fact, the scheme presented in [15] is actually of one-time use. To overcome this drawback, a one-way hash function-based multiuse threshold secret-sharing scheme was proposed in [17]. In [18], a multistage multisecret-sharing scheme and a multilevel multisecret-sharing scheme are

proposed, which are based on Mignotte's sequence and Asmuth's Bloom sequence, respectively. For the second category of the recovery method, multisecret is recovered simultaneously by a bivariate function [19–21]. One of the disadvantages is that the required function is hard to get, although the computational load can be reduced by optimizing some existing algorithms. In a word, this approach is inconvenient in practical applications.

All the above works consider the case when the correspondences between multisecret and elements in each share are definite. When the correspondences between multisecret and elements in each share are unclear, we say that the shares are unordered. Sharing and recovering multisecret are more challenging when the shares are unordered. For this type of sharing scheme, it is more safe since multisecret cannot be recovered directly from the given unordered shares. It is a generalization of single case and has a wide application in the scenarios of keeping some sensitive and important information, such as passwords of opening bank safes or launching missile [23, 24]. This paper gives a novel scheme to share and recover multisecret from the unordered shares. Motivated by the works in [25–27], we propose a generalized CRT-based multisecret-sharing and recovering scheme. The proposed scheme is not a perfect SS since information can be leaked. To overcome this drawback, we propose an improved multisecret-sharing scheme. The improved scheme not only is more secure but also has a lower computation complexity.

The rest of the paper is organized as follows. In Section 2, we introduce the unordered multisecret-sharing problem and then briefly recall the basic idea of the generalized CRT. In Section 3, we present a generalized CRT-based multisecret-sharing scheme. In Section 4, we present the improved multisecret-sharing scheme. In Section 5, we conclude this paper.

2. Unordered Multisecret Sharing and the Generalized CRT

In this section, we first introduce the unordered multisecret-sharing problem considered in this paper. Then, we model the problem as the generalized CRT. Some existing results for the generalized CRT are also introduced.

2.1. Problem of Unordered Multisecret Sharing. Suppose that we have a set of two secrets $\{s_1, s_2\}$ and n shares $\{U_1, U_2, \dots, U_n\}$. For each share U_i , we have $U_i = \{r_{1,i}, r_{2,i}\}$ with modulus m_i , where $\{r_{1,i}, r_{2,i}\}$ are the remainders of $\{s_1, s_2\}$ modulo a positive integer m_i . Notice that the correspondences between the remainders in each share $\{r_{1,i}, r_{2,i}\}$ and their secrets $\{s_1, s_2\}$ are unknown. In other words, we cannot determine whether $r_{1,i}$ is the remainder of s_1 or s_2 modulo m_i . For the recovery phase, the problem is how to efficiently recover the two secrets $\{s_1, s_2\}$ from the given shareholders?

2.2. Model of the Unordered Multisecret Sharing. If multisecret is viewed as multiple unknown integers, then the

pieces of shares are the remainders of multiple integer modulo some given moduli, where the correspondences between multiple integers and the remainders are unknown. Consequently, the problem of recovering unordered multisecret sharing can be modeled as the generalized CRT that determines multiple integers from their residue sets.

Traditional CRT tells us that an unknown integer can be uniquely recovered from its remainder modulo several given moduli, if and only if the unknown integer is less than the least common multiple (lcm) of the given moduli [28]. One of the generalization is to recover two unknown integers $\{s_1, s_2\}$ from their remainders modulo several moduli. Different from the traditional CRT, the remainders of $\{s_1, s_2\}$ modulo a given modulus are two remainders in a same set, which is called the residue set. For example, the remainders of $\{26, 38\}$ modulo three moduli 5, 7, and 11 are the residue sets $\{1, 3\}$, $\{3, 5\}$, and $\{4, 5\}$, respectively. For this kind of generalized CRT, two integers $\{s_1, s_2\}$ should be simultaneously determined from their residue sets.

There are two differences between this kind of generalized CRT and the traditional CRT. One is that the correspondence between the integers $\{s_1, s_2\}$ and their remainders in the residue sets is unknown. As the above example shows, for the first residue set $\{1, 3\}$, it is not known whether 1 is the remainder of 26 or 38 modulo 5. The other difference is how large the two integers can be uniquely determined from their residue sets for the given moduli, which will be explained below. For the traditional CRT, the largest integer that can be uniquely determined from its remainders for some given moduli is the least common multiple of all the moduli. However, this conclusion may not be true for the generalized CRT. Consider the above example again. If the two integers are less than $\text{lcm}(5, 7, 11) = 385$, then we have four candidates: $\{26, 38\}$, $\{103, 346\}$, $\{136, 313\}$, and $\{213, 236\}$, where all of them have the same residue sets $\{1, 3\}$, $\{3, 5\}$, and $\{4, 5\}$ with moduli 5, 7, and 11, respectively. Hence, the two unknown integers $\{s_1, s_2\}$ cannot be uniquely determined from the given residue sets when the two integers are restricted in range of $(0, 385)$.

2.3. Model of the Unordered Multisecret Sharing. In order to uniquely determine the two integers from their residue sets for some given moduli, the concept of the dynamic range was introduced [25], where the dynamic range is a range that any multiple integers within it can be uniquely determined from their residue set modulo the given moduli. In [26], the largest dynamic range of the two integers for the given moduli was obtained. For convenience of description, we denote the remainder of x modulo y as $\langle x \rangle_y$.

For any given modulus set $\mathcal{M} = \{m_1, m_2, \dots, m_n\}$, the largest dynamic range $D(\mathcal{M})$ can be determined by the following results [26].

Proposition 1. If $\mathcal{M} = \{2, 2k + 1\}$ for some positive integers k , then

$$D(\mathcal{M}) = 2k + 2. \quad (1)$$

Proposition 2. Let n pairwise coprime integers be $2 \leq m_1 < m_2 < \dots < m_n$. If $m_{n-1} \geq 3$, then

$$D(\mathcal{M}) = \min_{I \subseteq \{1,2,\dots,n\}} \left\{ \prod_{i \in I} m_i + \prod_{i \in \bar{I}} m_i \right\}, \quad (2)$$

where $\bar{I}$ is the complement of I in $\{1, 2, \dots, n\}$.

As an example, we consider the largest dynamic range of the two modulus sets $\mathcal{M}_1 = \{2, 13\}$ and $\mathcal{M}_2 = \{11, 13, 17, 19\}$. According to Propositions 1 and 2, we have $D(\mathcal{M}_1) = 14$ and $D(\mathcal{M}_2) = 11 \times 19 + 13 \times 17 = 430$, respectively.

3. Unordered Multisecret-Sharing Scheme

In this section, we propose two algorithms, i.e., the unordered multisecret generation phase and the recovery phase. Some results of the proposed scheme are also given.

3.1. Unordered Multisecret Generation. Suppose that the shareholders have the public information m_i , where m_i is pairwise coprime integer satisfying $2 \leq m_1 < m_2 < \dots < m_n$. Note that the scheme of multisecret sharing is trivial when $n \leq 2$, and we only consider $n \geq 3$ in this paper. Let t be a positive integer satisfying $t < n$. The generation of n shares from two unordered secrets $\{s_1, s_2\}$ contains two steps. First, determine the largest range of two secrets such that t shares or more than t shares can lead to a unique recovery of $\{s_1, s_2\}$. Second, obtain n shares $\{U_1, U_2, \dots, U_n\}$ by reducing $\{s_1, s_2\}$ modulo $m_1, m_2, \dots, m_n$, respectively. For convenience, we denote

$$\begin{aligned} \mathcal{M}_1 &= \{m_{n-t+2}, \dots, m_n\}, \\ \mathcal{M}_2 &= \{m_1, m_2, \dots, m_t\}. \end{aligned} \quad (3)$$

Define

$$i_0 = \min \left\{ i: \prod_{j=i}^n m_j < D(\mathcal{M}_2), \quad 1 \leq i \leq n \right\}. \quad (4)$$

It is not difficult to find that

$$n - i_0 + 1 < t. \quad (5)$$

If not, i.e., $n - i_0 + 1 \geq t$, then we have

$$D(\mathcal{M}_2) < \prod_{i=1}^t m_i \leq \prod_{j=1}^{n-i_0+1} m_j \leq \prod_{j=i_0}^n m_j, \quad (6)$$

by the definition of $D(\mathcal{M})$ in (2), which contradicts with (4). For convenience, we let

$$t_0 = n - i_0 + 1, \quad (7)$$

and let

$$D_L = \max \left\{ \prod_{j=i_0}^n m_j, D(\mathcal{M}_1) \right\}. \quad (8)$$

Then, two unordered secrets $\{s_1, s_2\}$ can be selected in the range of $(D_L, D(\mathcal{M}_2))$, i.e.,

$$D_L < s_i < D(\mathcal{M}_2), \quad i = 1, 2. \quad (9)$$

Consequently, shares $U_i = \{r_{1,i}, r_{2,i}\}$ can be obtained by

$$\{s_1, s_2\} \equiv \{r_{1,i}, r_{2,i}\} \pmod{m_i}, \quad i = 1, 2, \dots, n. \quad (10)$$

That is,

$$U_i = \{\langle s_1 \rangle_{m_i}, \langle s_2 \rangle_{m_i}\}, \quad i = 1, 2, \dots, n. \quad (11)$$

To sum up, we have the following unordered multisecret generation phase for the pairwise coprime integers $m_1, m_2, \dots, m_n$, which is shown in Table 1 below.

3.2. Unordered Multisecret Recovery. Now, we consider the problem of recovering the two secrets $\{s_1, s_2\}$ from the given l shares $U_{i_1}, U_{i_2}, \dots, U_{i_l}$, where $1 \leq i_j \leq n$ and $l > t$. Table 2 gives the generalized CRT-based algorithm to recover the two secrets.

Next theorem gives some results of the multisecret-sharing scheme discussed above.

Theorem 1. Let the two secrets $\{s_1, s_2\}$ be defined in (9), and let $U_{i_1}, U_{i_2}, \dots, U_{i_l}$ be l shares with the corresponding modulus set $\mathcal{M} = \{m_{i_1}, m_{i_2}, \dots, m_{i_l}\}$, where $1 \leq i_j \leq n$ for $j = 1, 2, \dots, l$. Then, we have the following results.

- (1) If $l \leq t_0$, then $\{s_1, s_2\}$ cannot be recovered, where t_0 is defined in (7).
- (2) If $t_0 < l < t$, then $\{s_1, s_2\}$ cannot be recovered in $(0, D(\mathcal{M}))$. Moreover, the two secrets cannot be uniquely recovered in $(0, \text{lcm}(\mathcal{M}))$, where $\text{lcm}(\mathcal{M}) \geq D(\mathcal{M}_2)$.
- (3) If $l \geq t$, then $\{s_1, s_2\}$ can be uniquely recovered.

Proof.

- (1) We consider the case when $l = t_0$. For any $t_0 = n - i_0 + 1$ shares $U_{i_1}, U_{i_2}, \dots, U_{i_{n-i_0+1}}$, we have the corresponding moduli $m_{i_1}, m_{i_2}, \dots, m_{i_{n-i_0+1}}$. According to the definition of i_0 in (4), we have

$$\prod_{j=1}^{n-i_0+1} m_{i_j} \leq \prod_{j=i_0}^n m_j. \quad (12)$$

Note that $\text{lcm}(\mathcal{M}) \leq \prod_{j=1}^{n-i_0+1} m_{i_j}$. It follows that

$$\text{lcm}(\mathcal{M}) \leq \prod_{j=i_0}^n m_j. \quad (13)$$

If $D(\mathcal{M}_1) \geq \prod_{j=i_0}^n m_j$, then we obtain from (8) that $D_L = D(\mathcal{M}_1)$. From (9) and (13), we have

$$\text{lcm}(\mathcal{M}) \leq D(\mathcal{M}_1) = D_L < s_i, \quad i = 1, 2. \quad (14)$$

If $D(\mathcal{M}_1) < \prod_{j=i_0}^n m_j$, then we obtain from (8) that $D_L = \prod_{j=i_0}^n m_j$. From (9) and (13), we have

TABLE 1: Generalized CRT-based unordered multisecret-sharing algorithm.

Unordered multisecret-sharing algorithm
Step 1. Determine $\mathcal{M}_1$ and compute $D(\mathcal{M}_2)$ by (3) and (2), respectively
Step 2. Determine i_0 by (4)
Step 3. Determine D_L by (8)
Step 4. Select two unordered secrets $\{s_1, s_2\}$ satisfying (9)
Step 5. Obtain n shares $U_1, U_2, \dots, U_n$ by (10)

TABLE 2: Generalized CRT-based unordered multisecret recovery algorithm.

Unordered multisecret recovery algorithm
Step 1. For each share U_{i_j} , compute $q_{i_j} = \langle r_{1,i_j} + r_{2,i_j} \rangle_{m_{i_j}}, j = 1, 2, \dots, l$
Step 2. Compute $M = m_{i_1} m_{i_2} \dots m_{i_l}$, $M_{i_j} = M/m_{i_j}$, and $\overline{M}_{i_j}$ satisfying $\overline{M}_{i_j} M_{i_j} \equiv 1 \pmod{m_{i_j}}$
Step 3. Compute $\xi_1 = \langle \sum_{j=1}^l \overline{M}_{i_j} M_{i_j} q_{i_j} \rangle_M$
Step 4. Let $k = \max\{0, \lceil \xi_1 - 2\sqrt{M} \rceil\}$, then compute $\xi_2 = \langle \sum_{j=1}^l \overline{M}_{i_j} M_{i_j} (r_{1,i_j} - k)(r_{2,i_j} - k) \rangle_M$
Step 5. Obtain the two secrets $\{s_1, s_2\}$ by solving $(x - k)^2 - (\xi_1 - 2k)(x - k) + \xi_2 = 0$

$$\text{lcm}(\mathcal{M}) \leq D_L < s_i, \quad i = 1, 2. \quad (15)$$

Thus, the two secrets $\{s_1, s_2\}$ cannot be reconstructed from t_0 shares. For the case of the less than t_0 shares, the proof is obvious and it is omitted here.

- (2) We consider the reconstruction of any $l = t - 1$ shares $U_{i_1}, U_{i_2}, \dots, U_{i_{t-1}}$ that is different from the shares $U_{n-t+2}, U_{n-t+3}, \dots, U_n$. For convenience, we denote $\mathcal{M}' = \{m_{i_1}, m_{i_2}, \dots, m_{i_{t-1}}\}$ and suppose

$$m_{i_1} < m_{i_2} < \dots < m_{i_{t-1}}, \quad (16)$$

without loss of generality. Recall that $m_1 < m_2 < \dots < m_n$. Hence, we have

$$m_{i_1} < m_{n-t+2}, \quad m_{i_2} < m_{n-t+3}, \dots, m_{i_{t-1}} < m_n, \quad (17)$$

and then

$$\min_{I \subseteq \{i_1, i_2, \dots, i_{t-1}\}} \left\{ \prod_{i \in I} m_i + \prod_{i \in \bar{I}} m_i \right\} < \min_{I \subseteq \{n-t+2, \dots, n\}} \left\{ \prod_{i \in I} m_i + \prod_{i \in \bar{I}} m_i \right\}. \quad (18)$$

According to (2), we have

$$D(\mathcal{M}') < D(\mathcal{M}_1). \quad (19)$$

By (8) and (9), we obtain

$$D(\mathcal{M}') < s_i, \quad i = 1, 2. \quad (20)$$

According to the generalized CRT, we know that $\{s_1, s_2\}$ cannot be recovered in the range of $(0, D(\mathcal{M}'))$ from their shares $U_{i_1}, U_{i_2}, \dots, U_{i_{t-1}}$. For the case of

$l < t - 1$, the conclusion also holds. Next, we consider the recovery of the two secrets in $(0, \text{lcm}(\mathcal{M}))$.

Let l shares be $U_{i_1} = \{r_{1,i_1}, r_{2,i_1}\}, \dots, U_{i_l} = \{r_{1,i_l}, r_{2,i_l}\}$. According to (11), we have

$$U_{i_l} = \left\{ \langle s_1 \rangle_{m_{i_l}}, \langle s_2 \rangle_{m_{i_l}} \right\}, \dots, U_{i_l} = \left\{ \langle s_1 \rangle_{m_{i_l}}, \langle s_2 \rangle_{m_{i_l}} \right\}. \quad (21)$$

Note that

$$s_i < D(\mathcal{M}_2) \leq \text{lcm}(\mathcal{M}), \quad i = 1, 2. \quad (22)$$

Hence, the two secrets s_1 and s_2 can be recovered separately by using the CRT when the remainders in the residue sets are properly ordered. More details can be seen in Remark 1 below.

- (3) We consider t shares $U_{i_1}, U_{i_2}, \dots, U_{i_t}$, where $1 \leq i_j \leq n$. Let $U_{i_1}, U_{i_2}, \dots, U_{i_t}$. Similar to the proof of (2) above, we can prove that the dynamic range $\mathcal{M}''$ satisfies

$$D(\mathcal{M}'') > D(\mathcal{M}_2) > s_i, \quad i = 1, 2. \quad (23)$$

Hence, $\{s_1, s_2\}$ can be uniquely reconstructed from their shares $U_{i_1}, U_{i_2}, \dots, U_{i_t}$ by the generalized CRT. For the case of more than t shares, the proof is obvious and it is omitted here. $\square$

Remark 1. Theorem 1 tells us that the two secrets cannot be recovered when the number of shares $l \leq t_0$, where t_0 is defined in (7). When $l > t$, the two secrets can be uniquely recovered by using the proposed generalized CRT. When $t_0 < l < t$, the two secrets cannot be successfully recovered. To be specific, the two secrets cannot be recovered in the range of $(0, D(\mathcal{M}))$ in this case. In addition, the two secrets cannot be uniquely recovered in $(0, \text{lcm}(\mathcal{M}))$ by using the CRT since the correspondences between the two secrets and the elements in each shareholder are unclear. It is clear that the remainder of s_1 or s_2 cannot be determined from any share U_{i_l} . To recover s_1 and s_2 , we have 2^{l-1} possible cases of remainders with moduli m_i : $\{\langle s_1 \rangle_{m_{i_1}}, \langle s_2 \rangle_{m_{i_2}}, \dots, \langle s_2 \rangle_{m_{i_l}}\}$ and $\{\langle s_2 \rangle_{m_{i_1}}, \langle s_1 \rangle_{m_{i_2}}, \dots, \langle s_1 \rangle_{m_{i_l}}\}; \dots, \{\langle s_1 \rangle_{m_{i_1}}, \langle s_1 \rangle_{m_{i_2}}, \dots, \langle s_1 \rangle_{m_{i_l}}\}$ and $\{\langle s_2 \rangle_{m_{i_1}}, \langle s_2 \rangle_{m_{i_2}}, \dots, \langle s_2 \rangle_{m_{i_l}}\}$.

According to the CRT, s_1 and s_2 can be recovered only from the last tuples in the range of $(0, \text{lcm}(\mathcal{M}))$.

Now, we consider the computational complexity of the proposed scheme. According to Algorithm 2, we know that the computational complexity of each shareholder is $O(1)$. For the proposed generalized CRT-based multisecret recovery algorithm, the computational complexity is $O(12l)$. For the CRT algorithm, the computational complexity is $O(2^{l-1})$ as discussed above.

Example 1. Let us consider a two secret-sharing and recovering process when moduli are $m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19$, and $m_5 = 20$. Set $t = 4$. By the definition of $\mathcal{M}_1$ and $\mathcal{M}_2$ in (3), we have $\mathcal{M}_1 = \{17, 19, 20\}$ and $\mathcal{M}_2 = \{11, 13, 17, 19\}$. By Proposition 2, we have $D(\mathcal{M}_1) = 343$ and $D(\mathcal{M}_2) = 430$. Since $m_4 m_5 = 380$, we have $i_0 = 4$ and then $D_L = 380$ by Step 2 in Table 1. Let two secrets be $\{s_1, s_2\} = \{398, 426\}$, which are in the range of $(380, 430)$. Then, we have five shares $U_1 = \{2, 8\}$, $U_2 = \{8, 10\}$, $U_3 = \{1, 7\}$, $U_4 = \{8, 18\}$, and $U_5 = \{6, 18\}$ with moduli $m_1, m_2, \dots, m_5$, respectively.

Now, we consider the recovery of two secrets from l shareholders. We have three cases below.

(1) $l \leq 2$.

Suppose that the two shares are U_{i_1} and U_{i_2} with $1 \leq i_1, i_2 \leq 5$. Clearly,

$$\text{lcm}(m_{i_1}, m_{i_2}) \leq m_4 m_5 < s_i, \quad i = 1, 2. \quad (24)$$

Hence, the two secrets $\{s_1, s_2\}$ cannot be recovered.

(2) $l = 3$.

Let U_{i_1}, U_{i_2} , and U_{i_3} be three shares, and let $\mathcal{M} = \{m_{i_1}, m_{i_2}, m_{i_3}\}$. In this case, the two secrets cannot be determined in $(0, D(\mathcal{M}))$ since $D(\mathcal{M}) < s_1$ and $D(\mathcal{M}) < s_2$. Moreover, the two secrets cannot be uniquely determined in $(0, \text{lcm}(\mathcal{M}))$. For example, given three shares U_1, U_2 , and U_3 , we have four candidates: $\{398, 426\}, \{959, 2296\}, \{970, 2285\}$, and $\{1531, 1724\}$. In other words, all these candidates have the same shares U_1, U_2 , and U_3 with moduli m_1, m_2 , and m_3 , respectively. Table 3 gives the illustration of recovering the two secrets for all cases, where $Z_n = \{0, 1, \dots, n-1\}$.

(3) $l \geq 4$.

In this case, the two secrets can be uniquely determined. Suppose that the shares are U_1, U_2, U_3 , and U_4 . Next, we recover $\{s_1, s_2\}$ by using the proposed generalized CRT algorithm.

Note that $M = m_1 m_2 m_3 m_4 = 46189$, $M_1 = 4199$, $\overline{M}_1 = 7$, $M_2 = 3553$, $\overline{M}_2 = 10$, $M_3 = 2717$, $\overline{M}_3 = 11$, $M_4 = 2431$, and $\overline{M}_4 = 18$. By Step 1 in Table 2, we have $q_1 = 10$, $q_2 = 5$, $q_3 = 8$, and $q_4 = 7$. According to Step 3, we have $\xi_1 = 824$. By Step 4, we have $k = 395$, and then $\xi_2 = 93$. By Step 5, we have the quadratic equation $x^2 - 824x + 169548 = 0$. By solving it, we can obtain the two secrets: $\{s_1, s_2\} = \{398, 426\}$.

From (11), we know that U_i are the remainders of two secrets $\{s_1, s_2\}$ modulo m_i . By Theorem 1, we know that the two secrets can be recovered after putting no less than t shares together without any other information. For example, in example 1, the two secrets can be recovered from any four shareholders directly by the generalized CRT. It is clear that each shareholder has partial information of the two secrets. In other words, the proposed multisecret-sharing scheme above is not a perfect SS. To overcome this drawback, we

propose an improved multisecret-sharing scheme in the following.

4. Improved Unordered Multisecret-Sharing Scheme

In this section, we give an improved generalized CRT-based unordered multisecret-sharing scheme, which includes the improved unordered multisecret generation phase and recovery phase. Some results of the proposed scheme are also given.

4.1. Improved Unordered Multisecret Generation Phase.

Firstly, select an integer p satisfying

$$(p, m_i) = 1, \quad i = 1, 2, \dots, m, \quad (25)$$

$$pD_L < D(\mathcal{M}_2), \quad (26)$$

where D_L is defined in (8). Then, the dealer transmits it secretly to secret combiner. Let two secrets be $\{s_1, s_2\}$ and satisfy

$$s_i < p, \quad i = 1, 2. \quad (27)$$

Consequently, select two positive integers α_i satisfying

$$s_i + \alpha_i p \in (D_L, D(\mathcal{M}_2)), \quad i = 1, 2. \quad (28)$$

Let

$$\{x_1, x_2\} = \{s_1 + \alpha_1 p, s_2 + \alpha_2 p\}. \quad (29)$$

Then, the shares $U_i = \{r_{1,i}, r_{2,i}\}$ can be generated by

$$\{x_1, x_2\} \equiv \{r_{1,i}, r_{2,i}\} \pmod{m_i}, \quad i = 1, 2, \dots, n. \quad (30)$$

That is,

$$U_i = \{\langle x_1 \rangle_{m_i}, \langle x_2 \rangle_{m_i}\}, \quad i = 1, 2, \dots, n. \quad (31)$$

According to (29), the shares can be rewritten as

$$U_i = \{\langle s_1 + \alpha_1 p \rangle_{m_i}, \langle s_2 + \alpha_2 p \rangle_{m_i}\}, \quad i = 1, 2, \dots, n. \quad (32)$$

Recall that the secrets of the first approach are leaked. For the improved approach, the obtained shares U_i are $\{\langle s_1 + \alpha_1 p \rangle_{m_i}, \langle s_2 + \alpha_2 p \rangle_{m_i}\}$ for $i = 1, 2, \dots, n$, which are different from the two secrets $\{s_1, s_2\}$. Hence, the secrets of each shareholder are not leaked.

In summary, we have the improved unordered multisecret-sharing algorithm for the pairwise coprime integers $m_1, m_2, \dots, m_n$, which is shown in Table 4 below.

4.2. Improved Unordered Multisecret Recovery Phase.

Given l shares $U_{i_1}, U_{i_2}, \dots, U_{i_l}$, where $1 \leq i_j \leq n$ and $l > t$, then the two secrets $\{s_1, s_2\}$ can be recovered by the generalized CRT-based algorithm, which is shown in Table 5 below.

It is not difficult to find that the proposed recovery algorithm has a computational complexity of $O(12l)$, which is much smaller than the searching algorithm that has a

TABLE 3: Recovery of two secrets using three shares.

Shares	$D(\mathcal{M})$	$\text{lcm}(\mathcal{M})$	Recovery in $D(\mathcal{M})$	Candidates in $Z_{\text{lcm}(\mathcal{M})}$
U_1, U_2, U_3	160	2431	$\emptyset$	$\{398, 426\}, \{959, 2296\}, \{970, 2285\}, \{1531, 1724\}$
U_1, U_2, U_4	162	2717	$\emptyset$	$\{8, 816\}, \{151, 673\}, \{255, 569\}, \{398, 426\}$
U_1, U_2, U_5	163	2860	$\emptyset$	$\{398, 426\}, \{959, 2296\}, \{970, 2285\}, \{1531, 1724\}$
U_1, U_3, U_4	206	3553	$\emptyset$	$\{398, 426\}, \{987, 3390\}, \{1718, 2659\}, \{2098, 2279\}$
U_1, U_3, U_5	207	3740	$\emptyset$	$\{398, 426\}, \{1146, 3418\}, \{1718, 2846\}, \{2098, 2466\}$
U_1, U_4, U_5	229	4180	$\emptyset$	$\{46, 778\}, \{398, 426\}, \{1718, 3286\}, \{2098, 2906\}$
U_2, U_3, U_4	240	4199	$\emptyset$	$\{75, 749\}, \{398, 426\}, \{1310, 3713\}, \{1633, 3390\}$
U_2, U_3, U_5	241	4420	$\emptyset$	$\{86, 738\}, \{398, 426\}, \{2166, 3078\}, \{2506, 2738\}$
U_2, U_4, U_5	267	4940	$\emptyset$	$\{398, 426\}, \{1386, 4378\}, \{2298, 3466\}, \{2478, 3286\}$
U_3, U_4, U_5	343	6460	$\emptyset$	$\{18, 806\}, \{398, 426\}, \{1718, 5566\}, \{2098, 5186\}$

computational complexity of $O(2^{l-1})$. Based on the above multisecret recovery phase, we have the following results.

Theorem 2. Let $\{s_1, s_2\}$ be two secrets satisfying (27), and let $U_{i_1}, U_{i_2}, \dots, U_{i_l}$ be l shares defined in (32), where $1 \leq i_j \leq n$ for $j = 1, 2, \dots, l$. Then, we have the following results.

- (1) If $l \leq t_0$, then $\{s_1, s_2\}$ cannot be reconstructed, where t_0 is defined in (7).
- (2) If $t_0 < l < t$, then $\{s_1, s_2\}$ cannot be uniquely determined.
- (3) If $l \geq t$, then $\{s_1, s_2\}$ can be uniquely reconstructed.

Proof.

- (1) By Theorem 1, we know that $\{x_1, x_2\} = \{s_1 + \alpha_1 p, s_2 + \alpha_2 p\}$ cannot be reconstructed in this case. Hence, the two secrets $\{s_1, s_2\}$ cannot be recovered.
- (2) In this case, $\{x_1, x_2\} = \{s_1 + \alpha_1 p, s_2 + \alpha_2 p\}$ cannot be determined in $(0, D(\mathcal{M}))$ and cannot be uniquely determined in $(0, \text{lcm}(\mathcal{M}))$. Hence, $\{s_1, s_2\}$ cannot be successfully recovered in $(0, p)$.
- (3) In this case, $\{x_1, x_2\} = \{s_1 + \alpha_1 p, s_2 + \alpha_2 p\}$ can be uniquely reconstructed. Consequently, the two secrets $\{s_1, s_2\}$ can be recovered by

$$\{s_1, s_2\} = \{\langle s_1 + \alpha_1 p \rangle_p, \langle s_2 + \alpha_2 p \rangle_p\}. \quad (33)$$

Example 2. Let us consider an example when moduli are $m_1 = 23, m_2 = 29, m_3 = 31$, and $m_4 = 37$.

Let $t = 3$. Then, we have $\mathcal{M}_1 = \{31, 37\}$ and $\mathcal{M}_2 = \{23, 29, 31\}$. By (2), we obtain $D(\mathcal{M}_1) = 68$ and $D(\mathcal{M}_2) = 698$. According to (4), we have $i_0 = 4$, and then $D_L = 68$ by (8). From (26), we obtain $p < 349/34$. Let $p = 10$. By Step 3, in Table 4, we select two secrets $\{s_1, s_2\} = \{5, 9\}$, which are satisfied with the condition in (27). By Step 4, we select $\alpha = 55$ and then obtain $\{x_1, x_2\} = \{555, 559\}$. By (30), we have four shares $U_1 = \{3, 7\}, U_2 = \{4, 8\}, U_3 = \{1, 28\}$, and $U_4 = \{0, 4\}$ with moduli m_1, m_2, m_3 , and m_4 , respectively.

Now, we consider the recovery of two secrets from l shareholders. We have three cases below.

TABLE 4: Improved unordered multisecret-sharing algorithm.

Improved unordered multisecret-sharing algorithm
Step 1. Determine $\mathcal{M}_1$ and compute $D(\mathcal{M}_2)$ by (3) and (2), respectively
Step 2. Determine p by (19) and (20)
Step 3. Select two unordered secrets $\{s_1, s_2\}$ satisfying (21)
Step 4. Determine α_i by (19) and (20)
Step 5. Obtain n shares $U_1, U_2, \dots, U_n$ by (26)

TABLE 5: Improved unordered multisecret recovery algorithm.

Improved unordered multisecret recovery algorithm
Step 1. For each share U_{i_j} , compute $q_{i_j} = \langle r_{1,i_j} + r_{2,i_j} \rangle_{m_{i_j}}, j = 1, 2, \dots, l$
Step 2. Compute $M = m_{i_1} m_{i_2} \dots m_{i_l}, M_{i_j} = M/m_{i_j}$, and $\bar{M}_{i_j}$ satisfying $\bar{M}_{i_j} M_{i_j} \equiv 1 \pmod{m_{i_j}}$
Step 3. Compute $\xi_1 = \langle \sum_{j=1}^l \bar{M}_{i_j} M_{i_j} q_{i_j} \rangle_M$
Step 4. Let $k = \max\{0, \lceil \xi_1 - 2\sqrt{M} \rceil\}$, then compute $\xi_2 = \langle \sum_{j=1}^l \bar{M}_{i_j} M_{i_j} (r_{1,i_j} - k)(r_{2,i_j} - k) \rangle_M$
Step 5. Obtain two solutions $\{x_1, x_2\}$ by solving $(x - k)^2 - (\xi_1 - 2k)(x - k) + \xi_2 = 0$
Step 6. Obtain the two secrets by $\{s_1, s_2\} = \{\langle x_1 \rangle_p, \langle x_2 \rangle_p\}$

- (1) $l = 1$.

Clearly, for any shares U_{i_j} , we have $\text{lcm}(m_{i_j}) < D_L < x_i$ for $1 \leq i_j \leq 4, i = 1, 2$. Hence, two integers $\{x_1, x_2\}$ cannot be successfully reconstructed and hence the two secrets $\{s_1, s_2\}$ cannot be recovered.

- (2) $l = 2$.

In this cases, the two integers $\{x_1, x_2\}$ cannot be reconstructed from the two shares U_{i_1}, U_{i_2} in $(0, D(\mathcal{M}))$ as $D(\mathcal{M}) < x_1$ and $D(\mathcal{M}) < x_2$. Moreover, $\{x_1, x_2\}$ cannot be uniquely determined in $(0, \text{lcm}(\mathcal{M}))$, where $\mathcal{M} = \{m_{i_1}, m_{i_2}\}$. Hence, $\{s_1, s_2\}$ cannot be successfully recovered in $(0, p)$. For example, given two shares U_1, U_2 , we have two candidates: $\{2, 5\}, \{5, 9\}$. In other words, all these candidates have the same shares. Table 6 gives all the cases of the reconstruction, where $p = 10$.

TABLE 6: Recovery of two secrets using two shares.

Shares	$D(\mathcal{M})$	$\text{lcm}(\mathcal{M})$	Recovery in $D(\mathcal{M})$	Candidates in $Z_{\text{lcm}(\mathcal{M})}$	Candidates of $\{s_1, s_2\}$
U_1, U_2	52	667	$\emptyset$	$\{95, 352\}, \{555, 599\}$	$\{2, 5\}, \{5, 9\}$
U_1, U_3	54	713	$\emptyset$	$\{187, 214\}, \{555, 599\}$	$\{4, 7\}, \{5, 9\}$
U_1, U_4	60	851	$\emptyset$	$\{444, 670\}, \{555, 599\}$	$\{0, 4\}, \{5, 9\}$
U_2, U_3	60	899	$\emptyset$	$\{497, 617\}, \{555, 599\}$	$\{7, 7\}, \{5, 9\}$
U_2, U_4	66	1073	$\emptyset$	$\{4, 37\}, \{555, 599\}$	$\{4, 7\}, \{5, 9\}$
U_3, U_4	68	1147	$\emptyset$	$\{152, 962\}, \{555, 599\}$	$\{2\}, \{5, 9\}$

(3) $l \geq 3$.

In this case, the two secrets can be uniquely recovered. Suppose that the shares are U_1, U_3 , and U_4 . By the proposed generalized CRT, we have $\{x_1, x_2\} = \{555, 559\}$ and then $\{s_1, s_2\} = \{\langle 555 \rangle_{10}, \langle 559 \rangle_{10}\} = \{5, 9\}$.

5. Conclusions

In this paper, we consider the problem of recovering unordered multisecret from some shares with unordered remainders. The main difference between this work and the previous ones is that the correspondence between the remainders in each share and the secrets is unknown in our work, while it is definite in previous works. A generalized CRT-based unordered multisecret-sharing scheme and recovery algorithm are proposed. The conditions for recovery failure and success are also explored. Furthermore, for making a perfect SS such that the secrets will not be leaked, an improved sharing and recovery approach is proposed.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research was funded in part by the National Natural Science Foundation of China (no. 61701086), Fundamental Research Funds for the Central Universities (no. ZYGX2016KYQD143), Natural Science Foundation of Fujian Province (nos. 2017J01761 and 2018J01537), and Project of Ministry of Science and Technology of Taiwan (no. MOST 106-2221-E-035-013-MY3).

References

- [1] M. Naor and A. Wool, "Access control and signatures via quorum secret sharing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 9, no. 9, pp. 909–922, 1998.
- [2] M. Stadler, "Publicly verifiable secret sharing," in *Advances in Cryptology—EUROCRYPT'96*, pp. 190–199, Springer, Berlin, Germany, International Conference on the Theory and Applications of Cryptographic Techniques, 1996.
- [3] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7195–7206, 2016.
- [4] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [5] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of AFIPS'79 National Computer Conference*, vol. 48, pp. 313–317, New York, NY, USA, June 1979.
- [6] M. Mignotte, "How to share a secret," in *Proceedings of the Workshop on Cryptography*, pp. 371–375, Paris, France, April 1983.
- [7] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.
- [8] Y. Liu, L. Harn, and C. C. Chang, "An authenticated group key distribution mechanism using theory of numbers," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 3502–3512, 2014.
- [9] Y. Liu, L. Harn, and C.-C. Chang, "A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets," *International Journal of Communication Systems*, vol. 28, no. 7, pp. 1282–1292, 2015.
- [10] G. R. Blakley and C. Meadows, "Security of ramp schemes," *Advance in Cryptology-CRYPTO*, Springer, vol. 196, pp. 242–268, Berlin, Germany, 1985.
- [11] X. Gong, P. Hu, K. W. Shum, and C. W. Sung, "A Zigzag-decodable ramp secret sharing scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1906–1916, 2018.
- [12] C. Blundo, A. Santis, and U. Vaccaro, "Efficient sharing of many secrets," in *Proceedings of the Annual Symposium on Theoretical Aspects of Computer Science*, vol. 665, pp. 692–703, Lecture Notes in Computer Science, Munich, Germany, March 1993.
- [13] C. Blundo, A. De Santis, G. Di Crescenzo, A. G. Gaggia, and U. Vaccaro, "Multi-secret sharing schemes," in *Advances in Cryptology—CRYPTO'94*, vol. 839, pp. 150–163, Springer, Berlin, Germany, Proceedings of the Advance in Cryptology-RYPTO, 1994.
- [14] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe, "On sharing many secrets," in *Proceedings of the 4th International Conferences on the Theory and Applications of Cryptology-ASIA-CRYPT'94*, pp. 42–54, Wollongong, Australia, November 1994.
- [15] J. He and E. Dawson, "Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1994.
- [16] L. Harn, "Comment: multistage secret sharing based on one-way function," *Electronics Letters*, vol. 31, no. 4, p. 262, 1995.
- [17] H. Piharam and T. Eghlidis, "An efficient lattice based multistage secret sharing scheme," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 2–8, 2015.
- [18] A. N. Tentu, V. C. Venkaiah, and V. K. Prasad, "CRT based multi-secret sharing schemes: revisited," *International Journal of Security and Networks*, vol. 13, no. 1, pp. 1–9, 2018.

- [19] H. Y. Chien, J.-K. Jan, and Y.-M. Tseng, "A practical (t, n) multi-secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer*, vol. 83, no. 12, pp. 2762–2765, 2000.
- [20] C.-C. Yang, T.-Y. Chang, and M.-S. Hwang, "A (t, n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.
- [21] L.-J. Pang and Y.-M. Wang, "A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing," *Applied Mathematics and Computation*, vol. 167, no. 2, pp. 840–848, 2005.
- [22] Y. J. Geng, X. H. Fan, and H. Fan, "A new multi-secret sharing scheme with multi-policy," in *Proceedings of the 9th International Conference on Advanced Communication Technology*, vol. 3, pp. 1515–1517, Okamoto, Kobe, Japan, February 2007.
- [23] D. Chen, W. Lu, W. Xing, and N. Wang, "An efficient verifiable threshold multi-secret sharing scheme with different stages," *IEEE Access*, vol. 7, pp. 107104–107110, 2019.
- [24] Y. Zhang, C. Xu, H. Li, K. Yang, N. Cheng, and X. S. Shen, "PROTECT: efficient password-based threshold single-sign-on authentication for mobile users against perpetual leakage," *IEEE Transactions on Mobile Computing*, 2020, In press.
- [25] H. Liao and X.-G. Xia, "A sharpened dynamic range of a generalized Chinese remainder theorem for multiple integers," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 428–433, 2007.
- [26] W. Wang, X. Li, X.-G. Xia, and W. Wang, "The largest dynamic range of a generalized Chinese remainder theorem for two integers," *IEEE Signal Processing Letters*, vol. 22, no. 2, pp. 254–258, 2015.
- [27] X. Li, X.-G. Xia, W. Wang, and W. Wang, "A robust generalized Chinese remainder theorem for two integers," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7491–7504, 2016.
- [28] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, Boston, MA, USA, 6th edition, 2015.