Hindawi
Security and Communication Networks
Volume 2019, Article ID 2387358, 7 pages
https://doi.org/10.1155/2019/2387358

Research Article

A Novel (t, n) Secret Sharing Scheme Based upon Euler's Theorem

Hefeng Chen[1] **and Chin-Chen Chang**[2]

[1] *Computer Engineering College, Jimei University, Xiamen 361021, China*
[2] *Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan*

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

Received 13 August 2018; Accepted 13 March 2019; Published 1 April 2019

Academic Editor: Salvatore D'Antonio

The (t, n) secret sharing scheme is used to protect the privacy of information by distribution. More specifically, a dealer splits a secret into n shares and distributes them privately to n participants, in such a way that any t or more participants can reconstruct the secret, but no group of fewer than t participants who cooperate can determine it. Many schemes in literature are based on the polynomial interpolation or the Chinese remainder theorem. In this paper, we propose a new solution to the system of congruences different from Chinese remainder theorem and propose a new scheme for (t, n) secret sharing; its secret reconstruction is based upon Euler's theorem. Furthermore, our generalized conclusion allows the dealer to refresh the shared secret without changing the original share of the participants.

1. Introduction

Secret sharing is used as one of basic cryptographic primitives in computer science including electronic voting [1], distributed cloud computing [2], key management [3], and data hiding [4]. The (t, n) secret sharing (SS) was first introduced by Shamir [5] based on the Lagrange interpolating polynomial and Blakley [6] based on the hyperplane geometry in 1979, independently. In 1983, Mignotte's scheme [7] and Asmuth-Bloom's scheme [8] were proposed based on the Chinese remainder theorem (CRT). A perfect (t, n) secret sharing scheme [5] has two properties: (1) Any t or more shares can recover the secret. (2) Any $t - 1$ or fewer shares reveal no information about the secret. The research on secret sharing has become the subject of many researchers; different types of secret sharing scheme have been designed to address different application requirements. For example, verifiable secret sharing [9, 10] allows the participants to verify the correctness of their share without leaking the confidentiality of both shares and the secret; weighted secret sharing [11] allows the participants with different privileges by holding the shares with different weights; multi-secret sharing [12] allows more than one secret to be shared. However, the major techniques used can still be categorized in the above three methods.

The CRT is to reconstruct a positive integer from its remainders modulo a series of integer moduli. It is widely used in the calculation of large integers, because it allows replacing a calculation for which one knows a bound on the size of the result by several similar computations on small integers. The CRT has many applications in various areas, like secret sharing [3, 4], the RSA decryption algorithm [13], the discrete logarithm algorithm [14], and the radio interferometric positioning system [15], etc.

The main contributions of our paper are summarized as follows:

(a) Using Euler's theorem to present a new method of the solution to the system of congruence

(b) First proposing a new type of secret sharing scheme based upon Euler's theorem

(c) Using Euler's theorem to present a new method of the solution to the system of congruence in the generalized CRT

(d) Proposing a refreshable secret sharing scheme to implement the secret refresh mechanism with the same shares.

Based on the equivalence between the conclusion of this paper and the CRT, our method is sufficient to be directly applied with the CRT-based scheme to achieve the same goal.

The rest of this paper is organized as follows. In Section 2, we describe some preliminaries on number theory and prove that the system of congruence has another solution form which is different from the CRT. In Section 3, we review the Asmuth-Bloom's scheme. In Section 4, we propose the secret sharing scheme based upon Euler's theorem. In Section 5, the security and performance analysis are given. In Section 6, we generalize the conclusion in Section 2 and propose a refreshable secret sharing scheme. In Section 7, we conclude the paper.

2. New Solution to the Congruence System

In this section, we describe the CRT and Euler's theorem firstly. Then we present another method to give the unique solution of the congruent system, by utilizing the properties of them.

The Chinese remainder theorem states that if the remainders of the Euclidean division of an integer x by several integers are known, then the remainder of the division of this integer x by the product of these integers can be uniquely determined, under the condition that the divisors are pairwise coprime.

Lemma 1 (Chinese remainder theorem (CRT) [16]). *Suppose $m_1, m_2, \cdots, m_n$ are pairwise relatively prime positive integers, and suppose $r_1, r_2, \cdots, r_n$ are integers. Then the system of n congruences $x \equiv r_i (\operatorname{mod} m_i)$ $(1 \leq i \leq n)$ has a unique solution modulo $M = \prod_{i=1}^{n} m_i$, which is given by*

$$x = \sum_{i=1}^{n} r_i M_i y_i \operatorname{mod} M, \quad (1)$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \operatorname{mod} m_i$ for $1 \leq i \leq n$.

Euler's theorem is a generalization of Fermat's little theorem and is further generalized by Carmichael's theorem [17].

Lemma 2 (Euler's theorem [17]). *If m and β are coprime positive integers, then*

$$\beta^{\varphi(m)} \equiv 1 (\operatorname{mod} m), \quad (2)$$

where $\varphi(m)$ called Euler's phi function is the number of positive integers less than m and relatively prime to m.

An efficient way to calculate Euler's phi function $\varphi(b)$ is the following Euler product formula [17]:

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right), \quad (3)$$

where the product is over the distinct prime numbers dividing m.

Now, we give another method of solving the systems of congruence and prove its correctness.

Theorem 3. *Suppose $m_1, m_2, \cdots, m_n$ are pairwise relatively prime positive integers (i.e., if $i \neq j$ then $\gcd(m_i, m_j) = 1$), and suppose $r_1, r_2, \cdots, r_n$ are integers. Then the system of n congruences*

$$\begin{aligned} x &\equiv r_1 \operatorname{mod} m_1 \\ x &\equiv r_2 \operatorname{mod} m_2 \\ &\vdots \\ x &\equiv r_n \operatorname{mod} m_n \end{aligned} \quad (4)$$

has a unique solution modulo $M = \prod_{i=1}^{n} m_i$, which is given by

$$x = \sum_{i=1}^{n} r_i (M_i)^{\varphi(m_i)} \operatorname{mod} M, \quad (5)$$

where $M_i = M/m_i$ for $1 \leq i \leq n$.

Proof. The Chinese remainder theorem shows that the function

$$\begin{aligned} \chi &: \mathbb{Z}_M \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \\ \chi(x) &= (r_1 \operatorname{mod} m_1, r_2 \operatorname{mod} m_2, \cdots, r_n \operatorname{mod} m_n) \end{aligned} \quad (6)$$

is a bijection.

Now, define a function $\rho : \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \longrightarrow \mathbb{Z}_M$ as follows:

$$\rho(r_1, r_2, \cdots, r_n) = \sum_{i=1}^{n} r_i (M_i)^{\varphi(m_i)} \operatorname{mod} M. \quad (7)$$

It amounts to show that the function $\rho = \chi^{-1}$.

Denote $x = \rho(r_1, r_2, \cdots, r_n)$, and let $1 \leq j \leq n$. Consider a term $r_i (M_i)^{\varphi(m_i)}$ in the above summation, reduced modulo m_j.

$m_1, m_2, \cdots, m_n$ are pairwise relatively prime positive integers, and $M_i = \prod_{1 \leq t \leq n, t \neq i} m_t$, for $1 \leq i \leq n$.

If $i = j$, it is obvious that $\gcd(M_i, m_i) = 1$; by Euler's theorem, we have

$$(M_i)^{\varphi(m_i)} \operatorname{mod} m_i = 1. \quad (8)$$

On the other hand, if $i \neq j$, because $m_j \mid M_i$, we have

$$(M_i)^{\varphi(m_i)} \operatorname{mod} m_j = 0. \quad (9)$$

Then

$$x \equiv \sum_{i=1}^{n} r_i (M_i)^{\varphi(m_i)} \operatorname{mod} m_j = r_j \operatorname{mod} m_j. \quad (10)$$

Since this is true for all j, $1 \leq j \leq n$, x is a solution to the system of congruences. □

Example 4. Suppose $n = 3$, $m_1 = 7$, $m_2 = 11$, and $m_3 = 13$. Then $M = 1001$, $\varphi(m_1) = 6$, $\varphi(m_2) = 10$, and $\varphi(m_3) = 12$. We compute $M_1 = 143$, $M_2 = 91$, and $M_3 = 77$, and then

$$\begin{aligned}(M_1)^{\varphi(m_1)} \bmod M &= 143^6 \bmod 1001 = 715,\\ (M_2)^{\varphi(m_2)} \bmod M &= 91^{10} \bmod 1001 = 364,\\ (M_3)^{\varphi(m_3)} \bmod M &= 77^{12} \bmod 1001 = 924.\end{aligned} \tag{11}$$

Then the function $\rho : \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13} \longrightarrow \mathbb{Z}_{1001}$ is

$$\rho(r_1, r_2, r_3) = (715r_1 + 364r_2 + 924r_3) \bmod 1001. \tag{12}$$

For example, if $x \equiv 5 \bmod 7$, $x \equiv 3 \bmod 11$, and $x \equiv 10 \bmod 13$, then this formula tells us that

$$\begin{aligned}x &= (715 \times 5 + 364 \times 3 + 924 \times 10) \bmod 1001\\ &= 13907 \bmod 1001 = 894.\end{aligned} \tag{13}$$

This can be verified by reducing 894 modulo 7, 11, and 13.

3. Review of Asmuth-Bloom's Secret Sharing

In 1983, Asmuth and Bloom [8] proposed a novel (t, n) SS, in which the shares are the congruence classes of the secret and the corresponding modulus is broadcasted as the participant's public key. The secret reconstruction is based on CRT.

3.1. Initialization. The $n + 1$ distinct positive integers $m_0, m_1, \cdots, m_n$ are chosen subject to the following conditions:

(1) $m_1 < m_2 < \cdots < m_n$

(2) $\gcd(m_i, m_j) = 1$ for $0 \le i \ne j \le n$

(3) $\prod_{i=1}^{t} m_i > m_0 \cdot \prod_{i=1}^{t-1} m_{n-t+i+1}$

3.2. Secret Generation. Suppose the shared secret is the integer $s \in [0, m_0)$. Let $s' = s + \alpha m_0$ where $\alpha \in \mathbb{Z}$ is subject to the condition $s' \in [0, m_1 \cdot m_2 \cdot \cdots \cdot m_t)$. Then let $s_i \equiv s' \bmod m_i$ $(i = 1, 2, \cdots, n)$ be the private shares.

3.3. Secret Reconstruction. If $s_{i_1}, s_{i_2}, \cdots, s_{i_t}$ are known, s' is obtained by

$$s' = \sum_{j=1}^{t} s_{i_j} N_{i_j} y_{i_j} \bmod N, \tag{14}$$

where $N = \prod_{j=1}^{t} m_{i_j}$, $N_{i_j} = N/m_{i_j}$, and $y_{i_j} = N_{i_j}^{-1} \bmod m_{i_j}$. Then the shared secret is

$$s = s' \bmod m_0. \tag{15}$$

3.4. Security Analysis. However, Harn et al. [18] pointed out that the value s' need be in the t-threshold range $(m_{n-t+2} \cdot m_{n-t+3} \cdot \cdots \cdot m_n, m_1 \cdot m_2 \cdot \cdots \cdot m_t)$; otherwise, it could be obtained by fewer than t participants. In the following, we give an example to illustrate this vulnerability.

Example 5. Consider Asmuth-Bloom's $(2, 4)$ secret sharing scheme.

We have a pairwise relatively prime integer set $\{5, 7, 11, 12, 13\}$. The shared secret s is 4. Let $s' = s + \alpha m_0 = 4 + 5 \times 18 = 94$. Then, four shares are generated as

$$\begin{aligned}(m_1, s_1) &= (7, 3),\\ (m_2, s_2) &= (11, 6),\\ (m_3, s_3) &= (12, 10),\\ (m_4, s_4) &= (13, 3).\end{aligned} \tag{16}$$

It is easy to recover the shared secret s by using two shares $(m_3, s_3) = (12, 10)$, $(m_4, s_4) = (13, 3)$ and the CRT, as shown below.

By Euclidean Algorithm, we get

$$\begin{aligned}y_3 &= 13^{-1} \bmod 12 = 1,\\ y_4 &= 12^{-1} \bmod 13 = 12,\end{aligned} \tag{17}$$

and then

$$\begin{aligned}s' &= (13 \times 1 \times 10 + 12 \times 12 \times 3) \bmod 156\\ &= 562 \bmod 156 = 94,\end{aligned} \tag{18}$$

and the secret $s = 94 \bmod 5 = 4$ is revealed.

Besides, Hwang and Chang [19] proposed a method to generate a pairwise relative prime integer set which satisfies the requirements of Asmuth-Bloom's and our schemes, and this specific integer set is not unique.

4. Proposed Secret Sharing Scheme

The traditional (t, n) secret sharing scheme is composed of a trusted dealer D and n participants $U_1, U_2, \cdots, U_n$. Our secret sharing scheme consists of three phases, that is, initialization phase, share generation phase, and secret reconstruction phase. In secret generation phase, we improve Asmuth-Bloom's scheme by considering the t-threshold range. We do the secret reconstruction by Euler's phi function, and the correctness is based upon Theorem 3 in Section 2.

4.1. Initialization. The dealer D chooses $n+1$ distinct positive integers $m_0, m_1, m_2, \cdots, m_n$ such that

(1) $m_1 < m_2 < \cdots < m_n$

(2) $\gcd(m_i, m_j) = 1$ for $0 \le i \ne j \le n$

(3) $\prod_{i=1}^{t} m_i > (m_0 + 1) \cdot \prod_{i=1}^{t-1} m_{n-t+i+1}$

The dealer D broadcasts the value m_0 and sends the value m_i to participant U_i as his/her public information, for $1 \le i \le n$.

4.2. Share Generation. Suppose the dealer D wants to share the secret $s \in \mathbb{Z}_{m_0}$.

The dealer D selects an integer $\alpha \in [\lceil \prod_{i=1}^{t-1} m_{n-i+1}/m_0 \rceil, \prod_{i=1}^{t} m_i/m_0 - 1)$; then let $s_i \equiv (s + \alpha m_0) \bmod m_i$ be the private share of the participant U_i, for $1 \le i \le n$.

4.3. Secret Reconstruction. If t participants pool their shares and corresponding modulus, $(s_{i_1}, m_{i_1}), (s_{i_2}, m_{i_2}), \cdots, (s_{i_t}, m_{i_t})$, the shared secret can be reconstructed as $s = s' \bmod m_0$, where

$$s' = \sum_{j=1}^{t} s_{i_j} \left(\prod_{1 \le k \le t, k \ne j} m_{i_k} \right)^{\varphi(m_{i_j})} \bmod \left(\prod_{1 \le k \le t} m_{i_j} \right). \qquad (19)$$

5. Security and Performance Analysis

In this section, we first give security analysis of the scheme proposed in Section 4 and then compare the performance of our proposed secret sharing with that of two types of classical secret sharing.

5.1. Security Analysis. Now we analyze the fact that our proposed (t, n) secret sharing is perfect, secure as follows.

Theorem 6. *Our proposed (t, n) secret sharing scheme described in Section 4 is perfect, that is, the following two properties are satisfied:*

(1) *If any t participants pool their shares, then they can determine the value of s.*

(2) *If any $t - 1$ participants pool their shares, then they can determine nothing about the value of s.*

Proof. Based on the conditions of our scheme,

$$s' = s + \alpha m_0, \qquad (20)$$

where $\lceil \prod_{i=1}^{t-1} m_{n-i+1}/m_0 \rceil \le \alpha < \prod_{i=1}^{t} m_i/m_0 - 1$ and $0 \le s < m_0$.

Let $M = \prod_{i=1}^{t} m_i$, we have

$$\begin{gathered} 0 + \left\lceil \frac{\prod_{i=1}^{t-1} m_{n-i+1}}{m_0} \right\rceil m_0 \le s + \alpha m_0 < m_0 + (M - m_0), \\ \prod_{i=1}^{t-1} m_{n-i+1} + 1 \le s' < M. \end{gathered} \qquad (21)$$

(1) If any t participants pool their shares $s_{i_1}, s_{i_2}, \cdots, s_{i_t}$, as described in Theorem 3, the system of t congruences

$$\begin{gathered} x \equiv s_{i_1} \bmod m_{i_1} \\ x \equiv s_{i_2} \bmod m_{i_2} \\ \vdots \\ x \equiv s_{i_t} \bmod m_{i_t} \end{gathered} \qquad (22)$$

has one unique solution as

$$x = \sum_{j=1}^{t} s_{i_j} \left(\frac{N}{m_{i_j}} \right)^{\varphi(m_{i_j})} \bmod N, \qquad (23)$$

where $N = \prod_{j=1}^{t} m_{i_j}$.

As $N \ge M$, this uniquely determines $s' = x$ and thus

$$s = s' \bmod m_0. \qquad (24)$$

(2) If only $t - 1$ participants pool their shares, $s_{l_1}, s_{l_1}, \cdots, s_{l_{t-1}}$, then all we have is $s^* = s' \bmod \overline{N}$, where $\overline{N} = \prod_{j=1}^{t-1} m_{l_j}$. The real secret $s' \in \{s^*, s^* + \overline{N}, \cdots, s^* + \lfloor M/\overline{N} - 1 \rfloor \overline{N}\}$; since $\gcd(\overline{N}, m_0) = 1$ and $M/\overline{N} > m_0$, the set of possible values is greater than that of possible secret. Hence, no useful information is compromised. □

Example 7. Consider the proposed $(2, 4)$ secret sharing scheme.

In initialization phase, the dealer D chooses 5 distinct positive integers, $m_0 = 5$, $m_1 = 7$, $m_2 = 11$, $m_3 = 12$, and $m_4 = 13$, which satisfies the conditions on initialization listed in Section 4.1. The minimum value $m_0 = 5$ is broadcasted. And m_i $(1 \le i \le 4)$ is sent as the public key of U_i.

In sharing phase, suppose the shared secret $s = 4$. Then dealer D selects an integer $\alpha = 18 \in [14, 183]$. So the private shares of U_1, U_2, U_3, and U_4, are generated as follows:

$$\begin{gathered} s_1 = 4 + 18 \times 5 \pmod 7 = 3, \\ s_2 = 4 + 18 \times 5 \pmod{11} = 6, \\ s_3 = 4 + 18 \times 5 \pmod{12} = 10, \\ s_4 = 4 + 18 \times 5 \pmod{13} = 3. \end{gathered} \qquad (25)$$

In reconstructing phase, suppose that U_3 and U_4 cooperate; by (19) we have

$$\begin{aligned} s' &= s_4 {m_3}^{\varphi(m_4)} + s_3 {m_4}^{\varphi(m_3)} \bmod (m_4 \cdot m_3) \\ &= 3 \times 12^{\varphi(13)} + 10 \times 13^{\varphi(12)} \bmod (13 \times 12) = 94, \end{aligned} \qquad (26)$$

and, then, the secret can be reconstructed as

$$s = s' \bmod m_0 = 94 \bmod 5 = 4. \qquad (27)$$

As in many literatures, we assume that all participants pool the real shares when they collaborate to recover the shared secret. To enhance the security, it can be combined with other cheater detection mechanisms to check the validity of the shares before recovery of the secret.

5.2. Performance Analysis. In this section, we analyze the computational cost of our proposed scheme and compare it with the other two classic secret sharing schemes, as summarized in Table 1. In Shamir's (t, n) scheme, the secret recovery using the usual polynomial interpolation requires $O(t \log^2 t)$ operations. In the Asmuth-Bloom's scheme, the modular

Table 1: Comparison of computational cost.

Scheme	Secret recovery
Shamir's scheme [5]	$O\left(t \log^2 t\right)$
Asmuth-Bloom's scheme [8]	$O(t)$
Our scheme	$O(t)$

method of secret recovery requires only $O(t)$ operations. In our scheme, the computation complexity of $(M_i)^{\varphi(m_i)} \bmod M$ requires at most $O(\log m_n)$ operations. However, this can be improved at the cost of storage room by keeping a table. Once the value of $(M_i)^{\varphi(m_i)} \bmod M \ (1 \le i \le n)$ is known, it requires only $O(t)$ operations to recover the secret.

6. Renewable Secret Sharing Scheme

The generalized Chinese remainder theorem (GCRT) [9, 10] is a variation of CRT with an additional integer k introduced as a common modulus. Inspired by GCRT, we have the following result.

Theorem 8. *Suppose $m_1, m_2, \cdots, m_n$ are pairwise relatively prime positive integers (i.e., if $i \ne j$ then $\gcd(m_i, m_j) = 1$), and $r_1, r_2, \cdots, r_n$ are integers. Suppose k is an integer satisfying $\max_{1 \le i \le n}\{r_i\} < k < \min_{1 \le i \le n}\{m_i\}$. Let $M = \prod_{i=1}^{n} m_i$. Then the system of n congruences*

$$\begin{aligned} \left\lfloor \frac{x}{m_1} \right\rfloor &\equiv r_1 \bmod k \\ \left\lfloor \frac{x}{m_2} \right\rfloor &\equiv r_2 \bmod k \\ &\vdots \\ \left\lfloor \frac{x}{m_n} \right\rfloor &\equiv r_n \bmod k \end{aligned} \qquad (28)$$

has a unique solution modulo kM, which is given by

$$x = \sum_{i=1}^{n} R_i k \left(M_i\right)^{\varphi(m_i)} \bmod kM, \qquad (29)$$

where $M_i = M/m_i$ and $R_i = \lceil r_i \cdot m_i/k \rceil$ for $1 \le i \le n$.

Proof. It amounts to showing that x in (28) is a solution to the system of congruences (19). The proof of uniqueness is similar to Theorem 3.

For $1 \le j \le n$, consider a term $R_i k (M_i)^{\varphi(m_i)}$ in the above summation, reduced modulo m_j.

If $i = j$, it is obvious that $\gcd(M_i, m_i) = 1$, by Euler's theorem; then we have $(M_i)^{\varphi(m_i)} \bmod m_i = 1$; i.e., there is an integerλ such that $(M_i)^{\varphi(m_i)} + \lambda m_i = 1$; then

$$k \left(M_i\right)^{\varphi(m_i)} \bmod k m_i = k, \qquad (30)$$

because $k(M_i)^{\varphi(m_i)} + k\lambda m_i = k$. On the other hand, if $i \ne j$, because $m_j \mid M_i$, we have

$$\left(M_i\right)^{\varphi(m_i)} \bmod m_j = 0, \qquad (31)$$

i.e., $R_i k (M_i)^{\varphi(m_i)} \bmod k m_j = 0$. Therefore,

$$\begin{aligned} \left\lfloor \frac{x}{m_j} \right\rfloor \bmod k &= \left\lfloor \frac{\sum_{i=1}^{n} R_i k \left(M_i\right)^{\varphi(m_i)}}{m_j} \right\rfloor \bmod k \\ &= \left\lfloor \frac{R_j k \left(M_j\right)^{\varphi(m_j)}}{m_j} \right\rfloor \bmod k, \end{aligned} \qquad (32)$$

because $R_i k (M_i)^{\varphi(m_i)}/m_j \bmod k = 0$ for $i \ne j$.

Since $k(M_i)^{\varphi(m_i)} \bmod k m_i = k$ and $k < m_i$, we have $k(M_i)^{\varphi(m_i)}/m_i \bmod k = k/m_i$.

If $r_j m_j$ is a multiple of k, then

$$R_j = \left\lceil r_j \cdot \frac{m_j}{k} \right\rceil = r_j \cdot \frac{m_j}{k}, \qquad (33)$$

and we have

$$\left\lfloor \frac{x}{m_j} \right\rfloor \bmod k = r_j \left(M_j\right)^{\varphi(m_j)} \bmod k = r_j. \qquad (34)$$

If $r_j m_j$ is not a multiple of k, then

$$\begin{aligned} \left\lfloor \frac{x}{m_j} \right\rfloor \bmod k &= \left\lfloor \frac{\lceil r_j \cdot m_j/k \rceil k \left(1 + \beta m_j\right)}{m_j} \right\rfloor \bmod k \\ &= \left\lfloor \frac{\lceil r_j \cdot m_j/k \rceil k}{m_j} \right\rfloor \bmod k \\ &= \left\lfloor r_j + \frac{\left(1 - \left(\left(r_j \cdot m_j \bmod k\right)/k\right)\right) k}{m_j} \right\rfloor \bmod k \\ &= r_j, \end{aligned} \qquad (35)$$

because $(1 - ((r_j \cdot m_j \bmod k)/k))k/m_j < 1$ and $r_j < k$. □

Although more computation is required, more flexible performance can be achieved. In the traditional secret sharing scheme, if we want to refresh the secret, the corresponding congruences system should be modified. However, based upon Theorem 8, we can refresh the shared secret without changing the share and the public information of the participants.

Compared with the previous scheme, the refreshable secret sharing scheme adds a secret refresh phase. In share generation phase, the dealer needs to broadcast an additional parameter as follows.

6.1. Initialization. The dealer D chooses $n+1$ distinct positive integers $m_0, m_1, \cdots, m_n$ such that

(1) $m_1 < m_2 < \cdots < m_n$

(2) $\gcd(m_i, m_j) = 1$ for $0 \le i \ne j \le n$

(3) $\prod_{i=1}^{t} m_i > (m_0 + 1) \cdot \prod_{i=1}^{t-1} m_{n-t+i+1}$

The dealer D broadcasts the value m_0 and sends the value m_i to participant U_i as his/her public information, for $1 \le i \le n$.

6.2. Share Generation. Suppose the dealer D wants to share the secret $s \in \mathbb{Z}_{m_0}$. The dealer D firstly selects and broadcasts an integer $k \in (0, \min_{1 \le i \le n}\{m_i\})$. Secondly, the dealer D chooses a random integer

$$\alpha \in \left[\left\lceil \frac{\prod_{i=1}^{t-1} m_{n-i+1}}{m_0} \right\rceil, \frac{\prod_{i=1}^{t} m_i}{m_0} - 1 \right), \tag{36}$$

then generating $s_i \equiv \lfloor s + \alpha m_0 / m_i \rfloor \bmod k$, which is the private share of the participant U_i, for $1 \le i \le n$.

6.3. Secret Refreshment. Suppose the dealer D wants to refresh the shared secret without changing the share and the public modulus of the participants which has been sent. The dealer D selects and broadcasts new integer $\widehat{k} \in (\max_{1 \le i \le n}\{r_i\}, \min_{1 \le i \le n}\{m_i\})$; then the secret $\widehat{s} = \widehat{s}' \bmod m_0$ can be shared by n participants with their original share and public modulus (s_i, m_i), where

$$\widehat{s}' = \sum_{i=1}^{n} \left\lceil r_i \cdot \frac{m_i}{\widehat{k}} \right\rceil \widehat{k} \left(M_i\right)^{\varphi(m_i)} \bmod \widehat{k} M. \tag{37}$$

6.4. Secret Reconstruction. If t participants pool their shares and public modulus, $(s_{i_1}, m_{i_1}), (s_{i_2}, m_{i_2}), \cdots, (s_{i_t}, m_{i_t})$, with the corresponding parameter k, the shared secret can be reconstructed as $s = s' \bmod m_0$, where

$$\begin{aligned} s' &\\ &= \sum_{j=1}^{t} \left\lceil \frac{r_{i_j} \cdot m_{i_j}}{k} \right\rceil k \left(\prod_{\substack{1 \le k \le t \\ k \ne j}} m_{i_k} \right)^{\varphi(m_{i_j})} \bmod \left(k \prod_{j=1}^{t} m_{i_j} \right). \end{aligned} \tag{38}$$

7. Conclusions

In this paper, we first show a new method to reconstruct the secret by the system of congruences utilizing Euler's theorem and propose a new type of perfect secret sharing scheme based on modular arithmetic. Furthermore, inspired by [20], we introduce an extra integer to help us to refresh the secret without changing the information the participant holds; only one public broadcasting parameter needs to be updated.

Data Availability

The relevant analysis data used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China (Grant No. 11804114) and the Natural Science Foundation of Fujian Province, China (Grant Nos. 2017J01761 and 2018J01537).

References

[1] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in E-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, pp. 67–84, 2007.

[2] H. Pilaram and T. Eghlidos, "An efficient lattice based multistage secret sharing scheme," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 2–8, 2017.

[3] C. Guo and C. Chang, "An authenticated group key distribution protocol based on the generalized Chinese remainder theorem," *International Journal of Communication Systems*, vol. 27, no. 1, pp. 126–134, 2014.

[4] P. Singh and B. Raman, "Reversible data hiding based on Shamir's secret sharing for color images over cloud," *Information Sciences*, vol. 422, pp. 77–97, 2018.

[5] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[6] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 AFIPS National Computer Conference*, vol. 48, pp. 313–317, New York, NY, USA, 1979.

[7] M. Mignotte, "How to share a secret," in *Proceedings of the Workshop on Cryptography, EUROCRYPT 1982: Cryptography*, pp. 371–375, Burg Feuerstein, Germany, 1982.

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

[9] B. Choc, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proceedings of the 26th Annual Symposium on Foundation of Computer Science (sfcs 1985)*, pp. 383–395, 1985.

[10] T. P. Pedersen, "Noninteractive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO '91*, vol. 576 of *Lecture Notes in Computer Science*, pp. 129–140, 1991.

[11] L. Harn and M. Fuyou, "Weighted secret sharing based on the Chinese remainder theorem," *International Journal of Network Security*, vol. 16, no. 6, pp. 420–426, 2014.

[12] L. Harn, "Secure secret reconstruction and multi-secret sharing schemes with unconditional security," *Security and Communication Networks*, vol. 7, no. 3, pp. 567–573, 2014.

[13] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 106–110, 1978.

[14] J. Quisquater and C. Couvreur, "Fast decipherment algorithm for RSA public-key cryptosystem," *IEEE Electronics Letters*, vol. 18, no. 21, pp. 905–907, 1982.

[15] X. Li, W. Wang, W. Zhang, and Y. Cao, "Phase-detection-based range estimation with robust Chinese remainder theorem," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10132–10137, 2016.

[16] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer Science & Business Media, 2013.

[17] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 3rd edition, 2005.

[18] L. Harn, C. Hsu, M. Zhang, T. He, and M. Zhang, "Realizing secret sharing with general access structure," *Information Sciences*, vol. 367-368, pp. 209–220, 2016.

[19] R. J. Hwang and C. C. Chang, "An improved threshold scheme based on modular arithmetic," *Journal of Information Science and Engineering*, vol. 15, pp. 691–699, 1999.

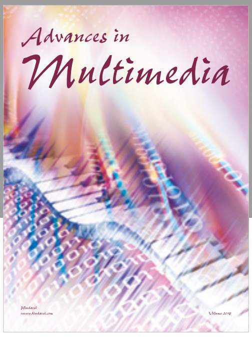
[20] Y. Liu and C. C. Chang, "An integratable verifiable secret sharing mechanism," *Journal of Network Security*, vol. 18, no. 4, pp. 617–624, 2016.

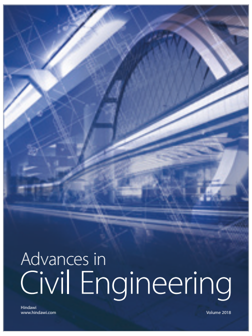
Journal of
Engineering

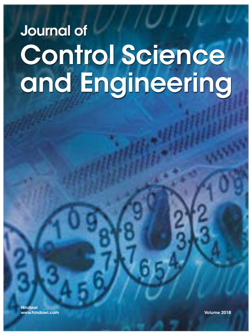
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

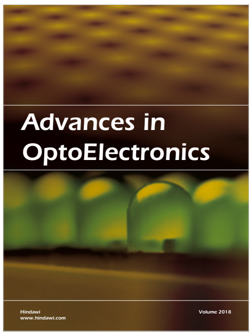

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

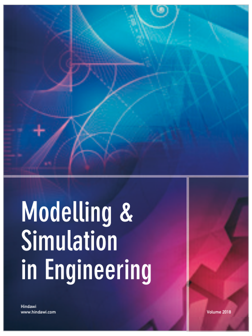
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

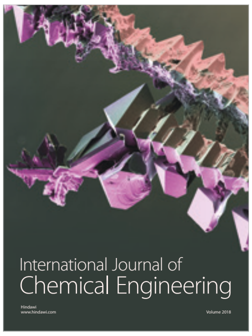

Advances in
OptoElectronics

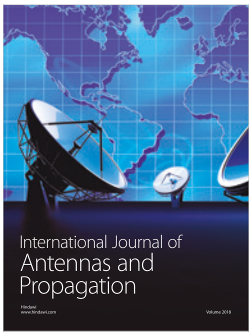
VLSI Design

International Journal of
Navigation and
Observation

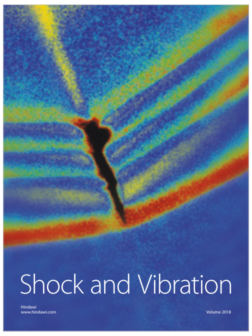

Modelling &
Simulation
in Engineering

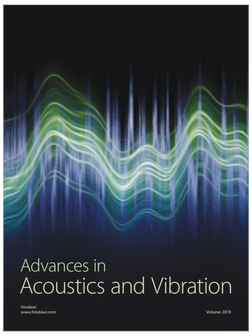
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration