Front. Comput. Sci., 2022, 16(1): 161811
https://doi.org/10.1007/s11704-021-0483-9

RESEARCH ARTICLE

A simple construction of CRT-based ideal secret sharing scheme and its security extension based on common factor

Lei WU, Fuyou MIAO (✉), Keju MENG, Xu WANG

School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China

Abstract Secret sharing (SS) is part of the essential techniques in cryptography but still faces many challenges in efficiency and security. Currently, SS schemes based on the Chinese Remainder Theorem (CRT) are either low in the information rate or complicated in construction. To solve the above problems, 1) a simple construction of an ideal (t, n)-SS scheme is proposed based on CRT for a polynomial ring. Compared with Ning's scheme, it is much more efficient in generating n pairwise coprime modular polynomials during the scheme construction phase. Moreover, Shamir's scheme is also a special case of our scheme. To further improve the security, 2) a common-factor-based (t, n)-SS scheme is proposed in which all shareholders share a common polynomial factor. It enables both the verification of received shares and the establishment of a secure channel among shareholders during the reconstruction phase. As a result, the scheme is resistant to eavesdropping and modification attacks by outside adversaries.

Keywords ideal secret sharing, Chinese remainder theorem, coprime polynomial generation, common factor

1 Introduction

To safeguard cryptographic keys, Shamir [1] and Blakley [2] independently introduced (t, n)-threshold secret sharing ((t, n)-SS) in 1979. In a (t, n)-SS scheme, the dealer divides a secret into n pieces and allocates each piece to a shareholder. A group of t or more shareholders can reconstruct the secret, but $t - 1$ or fewer shareholders cannot recover the secret. Secret sharing schemes have been widely used in security protocols, e.g., threshold public key encryption [3], signature algorithm [4], and zero-knowledge proof [5]. (t, n)-SS schemes can be built by various mathematical tools. For example, Shamir's scheme is based on Lagrange interpolation polynomial, and Blakley's scheme is based on the hyperplane. In this paper, we focus on (t, n)-SS schemes based on the Chinese Remainder Theorem (CRT).

Mignotte [6] and Asmuth-Bloom [7] proposed the (t, n)-SS scheme based on CRT for integer ring $\mathbb{Z}$ in the 1980s. Since then, many CRT-based schemes [8–11] have been developed to meet different requirements in practice.

In 1990, Brickell [12] gave the notion of the ideal secret sharing (SS) scheme, which means a perfect SS scheme with the information rate $\rho = 1$. As the first CRT-based scheme, Mignotte's (t, n)-SS scheme [6] is not perfect in security and has an information rate $\rho < 1$. In contrast, Asmuth-Bloom's scheme [7] is perfect in security but is still not ideal. Besides, almost all other schemes based on Mignotte's or Asmuth-Bloom's schemes are not ideal either. In scheme construction, all (t, n)-SS schemes based on CRT for $\mathbb{Z}$ are complicated in picking a group of n pairwise coprime moduli, which is subject to a much rigorous condition. Hence, constructions of SS schemes based on CRT are more difficult compared with other schemes.

In 2018, Ning et al. [13] proposed an ideal SS scheme based on CRT for $\mathbb{F}_p[x]$, the polynomial ring over a finite field $\mathbb{F}_p$, and proved that Shamir's scheme is a special case of their scheme. In the scheme, generating coprime polynomials is the most time-consuming operation, which decides the efficiency of the distribution phase. The scheme generates pairwise coprime modular polynomials in two steps. At first, the dealer randomly chooses polynomials in $\mathbb{F}_p[x]$. Then the dealer checks their irreducibility to guarantee irreducible polynomials are chosen as pairwise moduli. However, it makes the scheme construction complicated and inefficient.

Therefore, one of our goals is to improve the efficiency of scheme construction by directly generating coprime polynomials without checking the irreducibility.

When considering attacks to SS schemes, most of the existing schemes face two types of attacks, message modification attack, and eavesdropping attack.

Message modification attack in SS schemes causes that shareholders receive incorrect shares in the distribution phase, and thus the secret cannot be reconstructed correctly in the reconstruction phase. Message authentication code (MAC) [14–16] is widely used to resist message modification attack.

Moreover, eavesdropping attack during the reconstruction phase may cause adversaries to reconstruct the secret illegally. Establishing secure channels is a sophisticated way to resist eavesdropping attack, which requires a secret key to be shared between two communication parties. The Diffie-Hellman key agreement protocol [17] was proposed in 1979 and widely

Received September 27, 2020; accepted January 20, 2021

E-mail: mfy@ustc.edu.cn

used to establish a secure channel between two parties. Besides, Barker et al. [18] proposed key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key establishment schemes. Hence, most SS schemes [19–21] often assume that a secure channel among shareholders has existed during reconstruction. To remove such an assumption, some researchers consider constructing SS schemes without pre-deployed secure channels between each pair of shareholders. In Zhao's scheme [22], each shareholder chooses his own shadow by himself, which makes the system does not need a secure channel. In [23], Harn et al. applied bivariate polynomials to establishing secure channels between any two shareholders. To thwart eavesdropping and modification attacks simultaneously, we use a common polynomial factor to enable message verification and private key agreement among shareholders.

Our contributions can be summarized as follows:

- **A simple ideal SS scheme based on CRT for $\mathbb{F}_p[x]$:**
  (1) The scheme is perfect in security and has the information rate $\rho = 1$, which is the highest.
  (2) The construction of the proposed scheme is simple which only takes $O(n)$ operations in $\mathbb{F}_p[x]$ to choose n pairwise coprime modular polynomials. It is more efficient than Ning's scheme, which takes $O(nd^3 \log d \log p)$ operations in $\mathbb{F}_p[x]$, where d is the degree of chosen polynomials.
- **A SS scheme based on common polynomial factor:**
  (1) The scheme can not only prevent message modification attack in the distribution phase and reconstruction phase but also thwart eavesdropping attack in the reconstruction phase. The probability of detecting message modification is $1 - \frac{1}{p^{d_g}}$, which approaches 1, where p is a large prime, and d_g is the degree of the verification polynomial.
  (2) The common polynomial factor enables the combiner and shareholders to share a secure channel in the reconstruction phase. Therefore, a pre-deployed secure channel is no longer required compared with most existing schemes.

The remainder of this paper is organized as follows. Section 2 contains some preliminaries and security models of the proposed schemes. The first scheme and its analyses are presented in Section 3. The second scheme and an example are included in Section 4. The detailed analysis of the second scheme is given in Section 5. Section 6 concludes our work.

2 Preliminaries

This section introduces some backgrounds of the proposed schemes.

2.1 Notation

Some frequently used notations are listed as below.

- $\mathbb{Z}$ denotes the ring of integers.
- $\mathbb{F}_p$ denotes the finite field with p elements, p prime.
- $\mathbb{F}_p[x]$ denotes the polynomial ring with indeterminate x over $\mathbb{F}_p$.
- $[n]$ denotes the set $\{1, 2, \ldots, n\}$.
- Both d_a and $\deg(a)$ denote the degree of a polynomial $a(x) \in F_p[x]$.
- Let
$$M = \begin{pmatrix} m_{11} & m_{12} & \ldots & m_{1f} \\ m_{21} & m_{22} & \ldots & m_{2f} \\ \vdots & \vdots & & \vdots \\ m_{e1} & m_{e2} & \ldots & m_{ef} \end{pmatrix},$$
be an array of size $m \times n$. Let $A = \{a_1, \ldots, a_r\} \subset [e]$ be a set of indices of rows of M and $B = \{b_1, \ldots, b_s\} \subset [f]$ be a set of indices of columns of M. Then $M(A, B)$ will denote the subarray indexed by indices of $A \times B$, i.e.,
$$M(A, B) = \begin{pmatrix} m_{a_1,b_1} & m_{a_1,b_2} & \ldots & m_{a_1,b_s} \\ m_{a_2,b_1} & m_{a_2,b_2} & \ldots & m_{a_2,b_s} \\ \vdots & \vdots & & \vdots \\ m_{a_r,b_1} & m_{a_r,b_2} & \ldots & m_{a_r,b_s} \end{pmatrix},$$
when $A = \{a\} \subset [e]$ or $B = \{b\} \subset [f]$ is singleton, the notation $M(A, B)$ will be simplified as $M(A, b)$ or $M(a, B)$.
- Let A be a finite set. $|A|$ and $\#A$ denotes the number of elements of A.

2.2 Secret sharing

There are three types of entities and two phases in the proposed SS schemes. The entities include a dealer, a combiner, and n shareholders. (1) *Dealer*. A secret sharing scheme is coordinated by a dealer who is trusted by all shareholders and splits the secret into n shares in the *distribution phase*. (2) *Shareholder*. Each shareholder receives its share from the dealer. Shareholders are called participants when they take part in the *reconstruction phase*. (3) *Combiner*. The combiner collects shares from shareholders and recovers the secret from collected shares in the *reconstruction phase*. For simplicity, we assume the combiner is one of the shareholders. The communication model is shown in Fig.1.

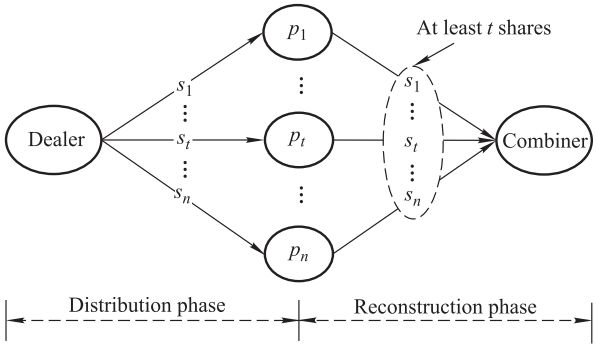

Fig. 1 Communication model

In a (t, n)-SS scheme, the dealer divides the secret into n shares, $\{s_i(x) \mid i \in [n]\}$, and then allocates each share, e.g., $s_i(x)$ to shareholder $\{P_i \mid i \in [n]\}$. A (t, n)-SS scheme has the following two properties. (1) The combiner can recover the secret after

collecting more than $t-1$ shares. (2) If fewer than t shares are available, the combiner cannot recover the secret.

Definition 1 ((t, n) Threshold Scheme) Let $S_0, S_1, \ldots, S_n$ be a series of finite sets. A (t, n) **threshold scheme** over $S_0, S_1, \ldots, S_n$ is an array M of m rows and $n+1$ columns verifying

1) (correctness) for any $A \subset [n]$ with $|A| \geqslant t$, for any rows $u, v \in [m]$ of the matrix, if $M(u, A) = M(v, A)$, then $M(u, 0) = M(v, 0)$; and
2) (perfectness) for any $B \subset [n]$ with $|B| \leqslant t-1$, for any tuple $T \in S_B$, for any keys $k_1, k_2 \in S_0$,

$$\#\{r \in m \mid M(r, B_0) = k_1 T\} = \#\{r \in m \mid M(r, B_0) = k_2 T\} > 0$$

where $B_0 = \{0\} \cup B$.

Definition 2 (Orthogonal array [24]) Let S be a set of s elements. An $N \times k$ array A with entries from S is said to be an orthogonal array with s levels, strength t, and index λ (for some t in the range $0 \leqslant t \leqslant k$), denoted as $\mathrm{OA}(N, k, s, t)$, if every $N \times t$ subarray of A contains each t-tuple based on S exactly λ times as a row. When $\lambda = 1$, it is customary to say that the orthogonal array has index unity.

Theorem 1 ([25]) Let M be an ideal (t, n)-SS scheme over S with $|S| = s$, then M is an $\mathrm{OA}(s^t, n+1, s, t)$. Conversely, if M is an $\mathrm{OA}(s^t, n+1, s, t)$, then M is an ideal (t, n)-SS scheme.

2.3 CRT for $\mathbb{F}_p[x]$

This subsection introduces the CRT for $\mathbb{F}_p[x]$, the ring of polynomials over the Finite Field $\mathbb{F}_p$.

Theorem 2 (Theorem 2 of [13]) Let $r_1(x), \ldots, r_n(x)$ be pairwise coprime polynomials in $\mathbb{F}_p[x]$. Given polynomials $f_1(x), \ldots, f_n(x) \in \mathbb{F}_p[x]$, the system

$$f(x) \equiv f_i(x) \bmod r_i(x) \text{ for all } i \in [n],$$

has the unique solution $f(x) \bmod (\prod_{i=1}^{n} r_i(x))$ as

$$f(x) = \sum_{i=1}^{n} f_i(x) M_i(x) M_i'(x) \bmod M(x),$$

where $M(x) = \prod_{i=1}^{n} r_i(x)$, $M_i(x) = \frac{M(x)}{r_i(x)}$ and $M_i(x)M_i'(x) \equiv 1 \bmod r_i(x)$.

3 A Simple construction of CRT-based ideal secret sharing scheme

In this section, an ideal (t, n)-SS scheme based on CRT is first proposed, which features a simple construction. Then the correctness, efficiency, and security analysis of the proposed scheme are presented.

3.1 A simple construction of CRT-based ideal secret sharing scheme

To simplify the construction of CRT-based (t, n)-SS, we generate modular polynomials directly by adding different constant terms to the same polynomial. The efficiency of the scheme is much higher than Ning's scheme. The specific steps are as follows:

Scheme 1 ***Distribution phase:***

Step 1: The dealer chooses a d_r-degree polynomial $r(x)$ to generate the modular polynomials and a secret polynomial $f(x)$ whose degree is d_f ($d_f \leqslant td_r - 1$). Then $f(x)$ can be written as

$$f(x) = a_0 + \cdots + a_{d_r-1}x^{d_r-1} + a_{d_r}x^{d_r} + \cdots + a_{d_f}x^{d_f},$$

where $a_i \in \mathbb{F}_p$. The secret $s(x)$ can be written as

$$s(x) = a_0 + a_1 x + \cdots + a_{d_r-1}x^{d_r-1}.$$

Step 2: The dealer generates each share, e.g., $s_i(x)$ for shareholder $\{P_i \mid i \in [n]\}$. The share of P_i is $s_i(x) = f(x) \bmod r_i(x)$, where $r_i(x) = r(x) + ID_i$ with $ID_i \in \mathbb{F}_p$ means the identification of P_i.

Reconstruction phase:

After collecting m ($m \geqslant t$) shares, e.g., $\{s_i \mid i \in [m]\}$ ($t \leqslant m \leqslant n$), the combiner can reconstruct the secret polynomial by calculating

$$f(x) = \sum_{i=1}^{m} s_i(x) M_i(x) M_i'(x) \bmod M(x),$$

where $M(x) = \prod_{i=1}^{m} r_i(x)$, $M_i(x) = \frac{M(x)}{r_i(x)}$ and $M_i(x)M_i'(x) \equiv 1 \bmod r_i(x)$. The secret is the first d_r terms in polynomial $f(x)$.

Scheme 1 can be simply shown in Fig. 2.

3.2 Correctness of Scheme 1

To prove Scheme 1 is correct, we need to prove t or more shareholders can reconstruct the secret while $t-1$ or fewer cannot reconstruct the secret.

Lemma 1 Polynomials in the form of $r(x) + i$ and $r(x) + j$ are pairwise coprime to each other, where $r(x)$ is a polynomial with $\deg(r) \geqslant 1$ in $\mathbb{F}_p[x]$ and $i, j \in \mathbb{F}_p, i \neq j$.

Proof Let $r(x)$ be a random polynomial in $\mathbb{F}_p[x]$, and assume i and j are different in $\mathbb{F}_p$. Clearly, $(i-j)^{-1}((r(x)+i)-(r(x)+j)) = 1$, therefore $r(x) + i$ and $r(x) + j$ are coprime. □

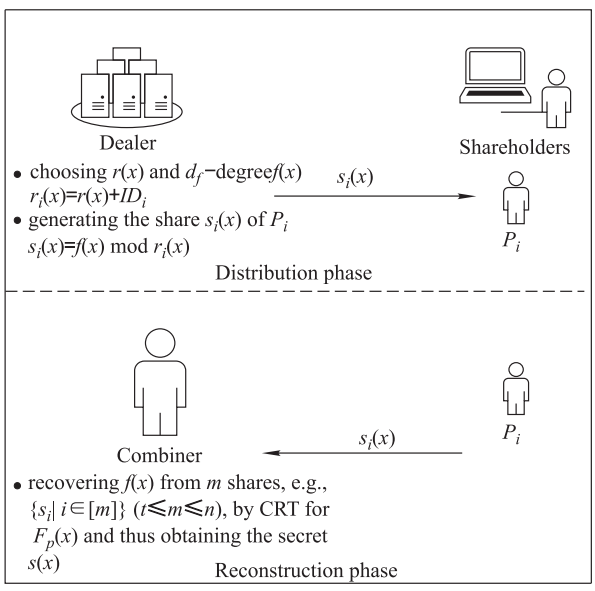

Fig. 2 CRT-based SS scheme

Proposition 1 More than $t-1$ shares can reconstruct the secret in Scheme 1.

Proof Without loss of generality, suppose shareholders $\{P_1, P_2, \ldots, P_m\}$ $(m \leqslant n)$ want to recover the secret, where $s_i(x)$ is the share of P_i and $r_i(x) = r(x) + ID_i$. Since the moduli $r_i(x)$ are pairwise coprime according to Lemma 1, then we have the CRT congruence system

$$\begin{cases} f_1(x) \equiv s_1(x) \bmod r_1(x), \\ f_1(x) \equiv s_2(x) \bmod r_2(x), \\ \quad \cdots\cdots\cdots\cdots \\ f_1(x) \equiv s_m(x) \bmod r_m(x). \end{cases} \tag{1}$$

Let $M(x) = \prod_{i=1}^{m} r_i(x)$. According to the Theorem 2, the system has the unique solution with degree $\deg(f_1) < \deg(M)$. Therefore, $f_1(x)$ can be recovered with degree $\deg(f_1) < \deg(M)$ and satisfies system (1). Since $f(x)$ with degree $\deg(f) \leqslant td_r - 1 < \deg(M)$ also satisfies the system, $f_1(x) = f(x)$ follows. In this case the secret $s(x)$ can be further obtained by $s(x) = f_1(x) \bmod x^{d_r}$. □

Proposition 2 Fewer than t shares cannot reconstruct the secret in Scheme 1.

Proof Assume that there are $t-1$ shareholders participating in the reconstruction phase in the worst case. Since this scheme is ideal, the combiner cannot get any additional information about the secret. The concrete proof will be shown in Section 3.4. □

According to Proposition 1 and Proposition 2, the correctness of Scheme 1 has been proved.

3.3 Efficiency comparison

In Ning's method, the most time-consuming part is to choose pairwise coprime modular polynomials by Algorithm 1 and Algorithm 2.

The method is selecting polynomials of specified degrees randomly in $\mathbb{F}_p[x]$, then checking the irreducibility of the chosen polynomials. The dealer chooses n irreducible polynomials as modular polynomials, which are automatically pairwise coprime to each other. This algorithm to choose n irreducible modular polynomials of degree d in $\mathbb{F}_p[x]$ has the time complexity $O(nd^3 \log d \log p)$.

Algorithm 1 Algorithm for irreducible polynomial testing [13]

INPUT: $f(x) \in \mathbb{F}_p[x]$ of degree $d > 0$
OUTPUT: whether $f(x)$ is irreducible or not
  $h = x \bmod f$;
  for each $k \in [1, \lfloor d/2 \rfloor]$ **do**
    $h = h^p \bmod f$;
    if $gcd(h - x, f) \neq 1$ **then**
      return false;
  end if
end for
return true;

Algorithm 2 Generation algorithm of random irreducible polynomial [13]

INPUT: the given degree d
OUTPUT: an irreducible polynomial of degree d
  repeat
    choose a polynomial f of degree d at random;
    test whether f is irreducible using Algorithm 1;
until *f is irreducible;*
return f;

Algorithm 3 Generating n pairwise coprime polynomials

INPUT: the given degree d and $\{ID_i \in \mathbb{F}_p \mid i \in [n]\}$
OUTPUT: n pairwise coprime polynomials $\{r_i(x) \in \mathbb{F}_p[x] \mid i \in [n]\}$ of degree d
  choose a polynomial $r(x)$ of degree d at random;
  for each $i \in [n]$ **do**
    $r_i(x) = r(x) + ID_i$;
end for
return $r_i(x)$;

In Scheme 1, the method to choose pairwise coprime polynomials is Algorithm 3, which has time complexity $O(n)$. The chosen polynomials are automatically coprime, according to Lemma 1. Clearly, our method is simpler and more efficient. Since our Scheme 1 is an improvement to Ning's scheme, both schemes are the generalization of Shamir's scheme according to [13].

3.4 Security analysis

In this part, we show that Scheme 1 is an ideal (t, n)-SS scheme as in Definition 1. To this end, by Theorem 1, it suffices to show that the distribution table of Scheme 1 is an orthogonal array of strength t and index unity as in Definition 2.

Clearly, there are $k \triangleq p^{td_r}$ polynomials of degree at most $td_r - 1$ over $\mathbb{F}_p$. Label them as

$$\left\{ f(x) \in \mathbb{F}_p[x] \;\middle|\; \deg(f) \leqslant td_r - 1 \right\} = \{f_1(x), f_2(x), \ldots, f_k(x)\}.$$

Table 1 lists all distribution rules of Scheme 1. It consists of k rows and $n+1$ columns. For each $1 \leqslant j \leqslant k$, the jth row is of the form

$$(f_j(x) \bmod x^{d_r}, f_j(x) \bmod r_1(x), \ldots, f_j(x) \bmod r_n(x)).$$

By Theorem 1, we need to show Table 1 is an OA of strength t and index 1.

Proposition 3 Denote Table 1 by M. For any t columns $i_1, i_2, \ldots, i_t$ of M, any t-tuple $(s_{i_1}(x), s_{i_2}(x), \ldots, s_{i_t}(x))$ of $\mathbb{F}_p[x]/r_{i_1}(x) \times \mathbb{F}_p[x]/r_{i_2}(x) \times \cdots \times \mathbb{F}_p[x]/r_{i_t}(x)$ must appear in M at the corresponding columns.

Proof Consider the following system of congruence

$$\begin{cases} X(x) \equiv s_{i_1}(x) \bmod r_{i_1}(x), \\ X(x) \equiv s_{i_2}(x) \bmod r_{i_2}(x), \\ \quad \cdots\cdots\cdots\cdots \\ X(x) \equiv s_{i_t}(x) \bmod r_{i_t}(x). \end{cases} \tag{2}$$

Table 1 Distribution table of Scheme 1

$s(x)$	$f(x) \bmod r_1(x)$	…	$f(x) \bmod r_n(x)$
$s_1(x)$	$s_{1_1}(x)$	…	$s_{1_n}(x)$
$s_2(x)$	$s_{2_1}(x)$	…	$s_{2_n}(x)$
⋮	⋮		⋮
$s_k(x)$	$s_{k_1}x$	…	$s_{k_n}x$

By Theorem 2, system (2) has a solution $g(x) \in \mathbb{F}_p[x]$ of degree at most $td_r - 1$. Suppose $g(x)$ is labeled as the jth polynomial as above. Then the tuple $(s_{i_1}(x), s_{i_2}(x), \ldots, s_{i_t}(x))$ appears in the corresponding columns of the jth row of M. □

Proposition 4 Denoted Table 1 by M. Then M is an OA of strength t and index unity.

Proof Fix any t columns of M, by Proposition 6, any t tuple will appear. Since the number of all such t tuples is p^{td_r}, which coincides with the number of rows of M, we conclude that any t tuple appears exactly once. Otherwise, if some t tuple appears more than two times, then the number of rows of M will be strictly larger than p^{td_r}, a contradiction. □

4 Common-factor-based secret sharing scheme

In this part, we propose a (t, n)-SS scheme based on a common polynomial factor that can resist eavesdropping attack and message modification. Then we use a concrete example to further demonstrate the scheme better.

4.1 Construction of common-factor-based secret sharing scheme

It is a (t, n)-SS with two functions of security which are both based on a common polynomial factor. On one hand, this scheme resists message modification attack during the distribution phase and reconstruction phase by verification enabled by the common polynomial factor. On the other hand, it also prevents the eavesdropping attack in the reconstruction phase by establishing a secure channel among the combiner and shareholders through the common polynomial factor. The specific steps are as follows:

The dealer needs to choose three polynomials in the distribution phase. They are the secret polynomial $f(x)$, the modular polynomial $r(x)$, and the verifying polynomial $g(x)$. To express this scheme more clearly, we assume the degree of $g(x)$ is $d_g = 2$. Of course, the degree of $g(x)$ can also be other value but needs to satisfy $d_g = d_f - td_r + 1$, where t is the number of shareholders participating in the reconstruction phase.

Scheme 2

Distribution phase

Step 1: Generating coprime modular polynomials The dealer randomly chooses a d_r-degree $r(x)$ and a secret $(td_r + 1)$-degree polynomial $f(x) = a_0 + \cdots + a_{d_r-1}x^{d_r-1} + a_{d_r}x^{d_r} + \cdots + a_{td_r+1}x^{td_r+1}$ in $\mathbb{F}_p[x]$. The secret $s(x)$ is the first d_r terms of $f(x)$, i.e.,

$$s(x) = a_0 + a_1 x + \cdots + a_{d_r-1}x^{d_r-1}.$$

For all shareholders $\{P_i \mid i \in [n]\}$, the dealer computes

$$r_i(x) = r(x) + ID_i,\ i \in [n],$$

as the modular polynomial of P_i with $ID_i \in \mathbb{F}_p$. It picks a 2-degree polynomial $g(x)$ coprime to each $r_i(x)$. The dealer makes each $r_i(x)$ and $g(x)$ public while keeps $f(x)$ and $s(x)$ private.

To make $g(x)$ coprime to each $r_i(x)$, the dealer picks a quadratic non-residue q in $\mathbb{F}_p$ and constructs

$$g(x) = x^2 - q.$$

Clearly, $g(x)$ is irreducible in $\mathbb{F}_p[x]$.

Step 2: Distributing shares The dealer calculates $m_i(x)$ as the share for shareholder P_i by

$$m_i(x) = f(x) \bmod (r_i(x) \cdot g(x)),\ i \in [n].$$

Let

$$f(x) \bmod g(x) = ax + b.$$

The dealer chooses a one-way hash function $H(\cdot)$ and calculates the verification message

$$h = H(a) \oplus H(b),$$

where $\oplus$ denotes bitwise XOR. The dealer publishes h and $H(\cdot)$ among all shareholders.

Step 3: Verifying shares Each shareholder P_i checks the share by calculating

$$g_i(x) = m_i(x) \bmod g(x).$$

If $g_i(x) = a'x + b'$ and $H(a') \oplus H(b') = h$, it means the share is not tempered during the distribution phase.

Reconstruction phase

Assume m shareholders, e.g., $\{P_i \mid i \in [m]\}$ $(t \leqslant m \leqslant n)$, need to recover the secret, they send shares to the combiner $P_c, c \in [m]$ through a secure channel and the secret can be reconstructed by the combiner as follows.

Step 1: Sending shares via a shared secure channel Each shareholder $P_i, i \in [m]$, calculates $k(x) = m_i(x) \bmod g(x) = a'x + b'$ and $k = H(a'\|b')$, where $a'\|b'$ means concatenation of a and b. Since the combiner is one of the shareholders, k is then served as the symmetric key for establishing the secure channel among the combiner P_c and shareholders. Each shareholder, e.g., P_i sends $Enc_k(m_i(x))$ to P_c, where $Enc_k(\cdot)$ represents some symmetric encryption algorithm and k is the encryption key.

Step 2: Verifying shares Let $Dec_k(\cdot)$ be the corresponding symmetric decryption algorithm with decryption key k. The combiner P_c decrypts $Enc_k(m_i(x))$ by $Dec_k(\cdot)$ and obtains $m_i(x), i \in [m]$. Hence, P_c can calculate the verifying message $g_i(x)$ and $s_i(x)$ of P_i by

$$g_i(x) = Dec_k(Enc_k(m_i)) \bmod g(x), \text{ and}$$
$$s_i(x) = Dec_k(Enc_k(m_i)) \bmod r_i(x).$$

Let $g_i(x) = a'x + b'$, if $H(a') \oplus H(b')$ is equal to the published h, it means the share $m_i(x)$ is not tempered.

Step 3: Recovering the secret After collecting m $(t \leqslant m \leqslant n)$ shares, the combiner P_c reconstructs the secret polynomial $f(x)$ by

$$f(x) = \sum_{i=1}^{m+1} s_i(x)M_i(x)M_i'(x) \bmod M(x),$$

where $r_{m+1}(x) = g(x)$, $s_{m+1}(x) = m_c(x) \bmod g(x)$, $M(x) = \prod_{i=1}^{m+1} r_i(x)$, $M_i(x) = \frac{M(x)}{r_i(x)}$, and $M_i(x)M_i'(x) \equiv 1 \bmod r_i(x)$. Finally, the secret can be figured out as the first d_r terms of $f(x)$.

Scheme 2 is shown in Fig.3.

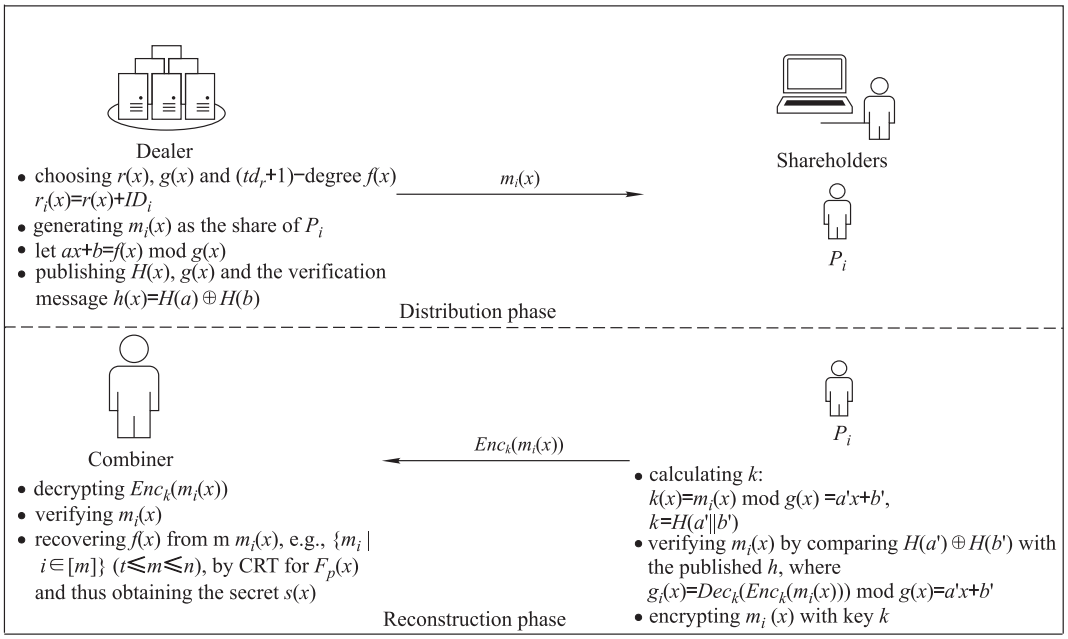

Fig. 3 Common-factor-based SS Scheme

4.2 An example of Scheme 2

In this part, an example of $(3, 4)$-SS scheme based on CRT for $\mathbb{F}_{17}[x]$ is presented to demonstrate Scheme 2.

In the distribution phase, the dealer selects public $r(x) = x^2 \in \mathbb{F}_{17}[x]$, secret polynomial $f(x) = x^5 + 7x^4 + 10x^3 + 6x^2 + 14x + 15 \in \mathbb{F}_{17}[x]$ and thus the secret is $s(x) = 14x + 15$. Moreover, The dealer chooses the polynomial $g(x) = x^2 - 4 \in \mathbb{F}_{17}[x]$ and MD5 as the one-way hash function $H(\cdot)$ to generate the verification information.

Then the dealer computes $f(x)$ mod $g(x) = 2x + 15$ and thus the published verification information

$$\begin{aligned} H(2) \oplus H(15) &= 9d4c2f636f067f89 \oplus f062936a96d3c8bd \\ &= 6d2ebc09f9d5b734. \end{aligned}$$

As a result, the key for establishing the secure channel is

$$H(2\|15) = H(215) = 26a953a8cd9526fc.$$

The dealer publishes the hash function *MD5*, $g(x) = x^2 - 4$ and the verification information $6d2ebc09f9d5b734$. The information of every shareholder is shown in Table 2. In addition, all the shareholders have the same verification information $6d2ebc09f9d5b734$, and the same key $26a953a8cd9526fc$.

If the combiner collects three or more correct shares, it can reconstruct the secret. Suppose shareholders P_3, P_5 and P_7 with identification $3, 5$ and 7 respectively, need to recover the secret and P_3 is the combiner. Thus, P_5 and P_7 need to send their encrypted share $Enc_k(m_i(x))$ to P_3 in a secure channel with $k = 26a953a8cd9526fc$. The combiner P_3 uses the same key to decrypt these shares. Then P_3 verifies shares and calculates $s_i(x)$ of each shareholder. If there is no modification in the transmission, P_3 calculates $s_3(x) = m_3(x)$ mod $r_3(x) = 10x + 9$, $s_5(x) = m_5(x)$ mod $r_5(x) = 6x + 7$, $s_7(x) = m_7(x)$ mod $r_7(x) = 10x + 10$ and $s_{t+1}(x) = s_4(x) = m_c(x)$ mod $g(x) = m_3(x)$ mod $g(x) = 2x + 15$, $r_{t+1}(x) = r_4(x) = g(x) = x^2 - 4$. In this case, the combiner P_3 can computing $f(x)$ as

$$\begin{aligned} f(x) = {} & (s_3(x)m_5(x)m_7(x)g(x)(m_5(x)m_7(x)g(x))^{-1} \bmod m_3(x)) \\ & + (s_5(x)m_3(x)m_7(x)g(x)(m_3(x)m_7(x)g(x))^{-1} \bmod m_5(x)) \\ & + (s_7(x)m_3(x)m_5(x)g(x)(m_3(x)m_5(x)g(x))^{-1} \bmod m_7(x)) \\ & + (s_4(x)m_3(x)m_5(x)m_7(x)(m_3(x)m_5(x)m_7(x))^{-1} \bmod g(x)) \\ & \bmod (m_3(x)m_5(x)m_7(x)g(x)) \\ = {} & x^5 + 7x^4 + 10x^3 + 6x^2 + 14x + 15, \end{aligned}$$

and finally recover the secret as $s(x) = f(x)$ mod $x^{d_r} = 14x+15$.

Table 2 Information of shareholders

i	ID	$r_i(x)$	$m_i(x)$	$s_i(x)$
1	3	$x^2 + 3$	$11x^3 + 13x^2 + 9x + 14$	$10x + 9$
2	5	$x^2 + 5$	$9x^3 + 16x^2 + 2$	$6x + 7$
3	7	$x^2 + 7$	$7x^3 + 2x^2 + 8x + 7$	$10x + 10$
4	12	$x^2 + 12$	$2x^3 + x^2 + 11x + 11$	$4x + 16$

5 Analysis of common-factor-based secret sharing

In this part, we analyze the correctness and security of Scheme 2.

5.1 Correctness of Scheme 2

Proposition 5 The degree of $g(x)$ needs to satisfy $d_g = d_f - td_r + 1$.

Proof In Scheme 2, at least t shareholders can reconstruct a polynomial $f(x)$ of degree $d_f = td_r + d_g - 1$ according to Theorem 2. Therefore, for t shareholders to reconstruct $f(x)$, the degree of $g(x)$ needs to satisfy $d_g = d_f - td_r + 1$. □

Proposition 6 More than $t - 1$ shareholders can reconstruct the secret in Scheme 2.

Proof If the combiner P_c gets m $(t \leqslant m \leqslant n)$, messages P_c

will get the system of congruences (3),

$$\begin{cases} f_3(x) \equiv m_1(x) \bmod (r_1(x)g(x)), \\ f_3(x) \equiv m_2(x) \bmod (r_2(x)g(x)), \\ \quad \cdots\cdots\cdots\cdots \\ f_3(x) \equiv m_m(x) \bmod (r_m(x)g(x)), \end{cases} \tag{3}$$

which yields the system of congruences (4) because $g(x)$ is coprime to each $r_i(x)$,

$$\begin{cases} f_3(x) \equiv m_1(x) \bmod r_1(x), \\ \quad \cdots\cdots\cdots\cdots \\ f_3(x) \equiv m_m(x) \bmod r_m(x), \\ f_3(x) \equiv m_c(x) \bmod g(x), \end{cases} \tag{4}$$

i.e.,

$$\begin{cases} f_3(x) \equiv s_1(x) \bmod r_1(x), \\ \quad \cdots\cdots\cdots\cdots \\ f_3(x) \equiv s_m(x) \bmod r_m(x), \\ f_3(x) \equiv m_c(x) \bmod g(x). \end{cases} \tag{5}$$

According to Theorem 2, system (5) determines $f_3(x)$ as

$$f_3(x) = \sum_{i=1}^{m+1} s_i(x)M_i(x)M_i'(x) \bmod M(x),$$

where $r_{m+1}(x) = g(x)$, $s_{m+1}(x) = m_c(x) \bmod g(x)$, $M(x) = \prod_{i=1}^{t+1} r_i(x)$, $M_i(x) = \frac{M(x)}{r_i(x)}$, and $M_i(x)M_i'(x) \equiv 1 \bmod r_i(x)$.

Now that $f_3(x)$ is the unique solution with degree $\deg(f_3) < \deg(M)$ and $f(x)$ is also a solution with degree $\deg(f) < \deg(M)$, it follows $f(x) = f_3(x)$ and thus the secret $s(x)$ can be obtained from $f_3(x)$ finally. □

Proposition 7 Fewer than t shareholders cannot reconstruct the secret in Scheme 2.

Proof Consider the worst case in which the combiner P_c gets $t-1$ shares, e.g., $\{m_1, m_2, \ldots, m_{t-1}\}$, P_c can establishes the system (6),

$$\begin{cases} f_4(x) \equiv m_1(x) \bmod (r_1(x)g(x)), \\ f_4(x) \equiv m_2(x) \bmod (r_2(x)g(x)), \\ \quad \cdots\cdots\cdots\cdots \\ f_4(x) \equiv m_{t-1}(x) \bmod (r_t(x)g(x)). \end{cases} \tag{6}$$

Since $g(x)$ is coprime to each $r_i(x)$, system (6) is equivalent to system (7),

$$\begin{cases} f_4(x) \equiv s_1(x) \bmod r_1(x), \\ \quad \cdots\cdots\cdots\cdots \\ f_4(x) \equiv s_{t-1}(x) \bmod r_{t-1}(x), \\ f_4(x) \equiv s_c(x) \bmod g(x). \end{cases} \tag{7}$$

According to Theorem 2, P_c can only determine a polynomial $f_4(x) \bmod (g(x)\prod_{i=1}^{t-1} r_i(x))$ with degree $td_r + d_g - d_r - 1$. Note that $f(x)$ has the degree $td_r + d_g - 1$ and satisfies

$$f(x) \equiv f_4(x) \bmod (g(x)\prod_{i=1}^{t-1} r_i(x)), \tag{8}$$

i.e.,

$$f(x) = f_4(x) + k(x)(g(x)\prod_{i=1}^{t-1} r_i(x)), \tag{9}$$

for some $k(x) \in \mathbb{F}_p[x]$ with degree $d_k \leqslant (d_r - 1)$. Clearly, there are p^{d_r} possible $k(x)$ satisfying Eq. (9), that is, the probability for $t-1$ shareholders to obtain $f(x)$ (and thus $s(x)$) is $1/p^{d_r}$, which is the same as the probability to directly guess the secret $s(x)$ without any share. Therefore, the SS scheme is perfect in security. □

According to Propositions 5–7, Scheme 2 is correct.

5.2 Security model

Scheme 2 is a (t, n)-SS scheme with two security functions based on a common polynomial factor. It is assumed that

(1) the dealer and all shareholders are honest;

(2) communications in the distribution phase are based on pre-deployed secure channels, which means each share is securely allocated to the corresponding shareholder.

(3) an Outsider is an adversary who has no valid share. It may listen to the channels (eavesdropping attack) or modify messages (modification attack) through these channels among the dealer, combiner, and shareholders. Eavesdropping attack aims to obtain shares and thus recover the secret while modification attack aims to prevent shareholders from recovering correct secret.

5.3 Resistance to attacks

Resistance to eavesdropping attack: An Outsider O may listen to the channel and get a message $\mathcal{M}_A$ transmitted in this channel.

The general method to resist to eavesdropping attack is transmitting information via a secure channel. In this case, O can only get the ciphertext instead of the plaintext.

According to the security model of Scheme 2, there exists a pre-deployed secure channel in the distribution phase, and thus shares can be securely distributed to each shareholder in this phase. Although an attacker can listen to the channel, the attacker can only get an encrypted message $\mathcal{M}_A$. Therefore, Scheme 2 is resistant to eavesdropping attack in the distribution phase.

In the reconstruction phase, there does not exist a pre-deployed secure channel. Instead, each shareholder, e.g., P_i can obtain the same polynomial $k(x)$ by computing $k(x) = m_i(x) \bmod g(x)$ with its share $m_i(x)$. Consequently, they are allowed to derive the shared key k from $k(x)$ and establish a secure channel with k among them. Therefore, Scheme 2 is resistant to eavesdropping attack in the reconstruction phase.

Resistance to message modification attack: An Outsider O listens to a secure channel and changes a message $\mathcal{M}_A$ to $\mathcal{M}_B$ through the channel. In this case, the receiver gets the modified $\mathcal{M}_B$, instead of the original message $\mathcal{M}_A$.

Shareholders guarantees by verification message that a received share is not tampered with. After receiving the share $m_i(x)$ from the dealer, a shareholder P_i calculates the verification message with $v(x) = m_i(x) \bmod g(x) = f(x) \bmod g(x) = a'x + b'$. Moreover, each shareholder is able to calculate the same $v(x)$ if the received message is not modified. Comparing

$H(a') \oplus H(b')$ with published h can realize the verification of each share $m_i(x)$. Thus, the dealer only needs to publish a single hash value, h, rather than n verification values to n shareholders.

The adversary cannot figure out the key from intercepted message $\mathcal{M}_A$ or published value h.

For the first case, O cannot get the key k from $\mathcal{M}_A$, which is the message encrypted by the key k if the used cryptographic algorithm $Enc_k(.)$ and $Dec_k(.)$ are secure enough.

For the second case, let consider the probability of O deriving k from $h = H(a) \oplus H(b)$.

According to the properties of one way hash functions, it is hard to invert $H(M)$ to obtain M. That is,

$$Pr[H^{-1}(H(M)) = M] = \delta,$$

where δ is negligible. It means a, b and thus $k = H(a\|b)$ cannot be obtained even if $H(a)$ and $H(b)$ are available from $h = H(a) \oplus H(b)$.

Therefore, O cannot get k from either $\mathcal{M}_A$ or $h = H(a) \oplus H(b)$.

The probability of modified message $\mathcal{M}_B$ passing the verification depends on p. We know that $\mathcal{M}_A$ has the form $Enc_k(f(x) \bmod r_i(x)g(x))$ before transmission. We assume that $\mathcal{M}_A$ is modified into $\mathcal{M}_B$ by an adversary during transmission and the modified message $m_i'(x) = Dec_k(\mathcal{M}_B)$, is a polynomial of degree $\deg(m_i') \leqslant d_r - 1$ uniformly distributed within $\mathbb{F}_p[x]$. We have $Dec_k(\mathcal{M}_B) \bmod g(x)$ uniformly distributed in $\mathbb{F}_p[x]$ with degree less than d_g.

In this case, we have

$$Pr[Dec_k(\mathcal{M}_B) \bmod g(x) = m_i(x) \bmod g(x)] = \frac{1}{p^{d_g}}.$$

Therefore, the possibility of the modified message $\mathcal{M}_B$ passing verification is $\frac{1}{p^{d_g}}$, which approaches 0 if p is large enough. In other words, the probability of detecting message modification is $1 - \frac{1}{p^{d_g}}$, which is almost 100%.

In conclusion, Scheme 2 is resistant to message modification. The security of it depends on the large p.

6 Conclusions

We propose two (t, n)-SS schemes based on the properties of CRT for the polynomial ring over a finite field.

In Scheme 1, we present a simpler construction of an ideal (t, n)-SS scheme based on CRT for $\mathbb{F}_p[x]$. It takes only $O(n)$ operations in choosing pairwise coprime polynomials. Compared with the construction of Ning's scheme, generating coprime polynomials, the most time-consuming part, takes $O(nd^3 \log d \log p)$ operations, where n is the number of shareholders, d is the degree of polynomials.

Scheme 2, based on a common polynomial factor, is a security extension of Scheme 1. In the scheme, no pre-deployed secure channel is required during the reconstruction phase, because it is easy to establish a symmetric secure channel between the combiner and shareholders through the common polynomial factor. Besides, the common factor can also be used to realize message verification, which makes sure received messages are correct. Analyses show Scheme 2 can both resist eavesdropping attack and message modification efficiently.

Acknowledgements This work was supported by National Key R&D Project 2018YFB2100300 and the National Natural Science Foundation of China (Grant No. 61520106007).

References

1. Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612–613
2. Blakley G R. Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference. 1979, 313–317
3. Zhang X, Xu C, Zhang W, Li W. Threshold public key encryption scheme resilient against continual leakage without random oracles. Frontiers of Computer Science, 2013, 7(6): 955–968
4. Zhang Y, He D, Zhang M, Choo K K. A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. Frontiers of Computer Science, 2020, 14(3): 1–4
5. Roy P. A homomorphism based zero knowledge proof of authentication for chinese remainder theorem based secret sharing. In: Proceedings of Annual Convention of the Computer Society of India. 2018, 562–572
6. Mignotte M. How to share a secret. In: Proceedings of Workshop on Cryptography. 1982, 371–375
7. Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 1983, 29(2): 208–210
8. Tiplea F L, Dragan C C. Asymptotically ideal CRT-based secret sharing schemes for multilevel and compartmented access structures. IACR Cryptology ePrint Archive, 2018, 2018: 933
9. Shyu S J, Chen Y R. Threshold secret image sharing by Chinese remainder theorem. In: Proceedings of IEEE Asia-Pacific Services Computing Conference. 2008, 1332–1337
10. Yan X, Lu Y, Liu L, Wan S, Ding W, Liu H. Chinese remainder theorem-based secret image sharing for (k, n) threshold. In: Proceedings of International Conference on Cloud Computing and Security. 2017, 433–440
11. Meng K, Miao F, Yu Y, Lu C. A universal secret sharing scheme with general access structure based on CRT. In: Proceedings of the 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference on Big Data Science And Engineering. 2018, 142–148
12. Brickell E F. Some ideal secret sharing schemes. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. 1989, 468–475
13. Ning Y, Miao F, Huang W, Meng K, Xiong Y, Wang X. Constructing ideal secret sharing schemes based on chinese remainder theorem. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. 2018, 310–331
14. Mahmood K, Chaudhry S A, Naqvi H, Shon T, Ahmad H F. A lightweight message authentication scheme for Smart Grid communications in power sector. Computers & Electrical Engineering, 2016, 52: 114–124
15. Gopal V, Brandt J W. Keyed-hash message authentication code processors, methods, systems, and instructions. U.S. Patent 10, 313, 129. 2019–6–4
16. Alomair B S. Residue message authentication code. U.S. Patent 10, 243, 744. 2019–3–26
17. Diffie W, Hellman M. New directions in cryptography. IEEE transactions on Information Theory, 1976, 22(6): 644–654
18. Barker E, Chen L, Keller S, Roginsky A, Vassilev A, Pavis R. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. National Institute of Standards and Technology, 2017
19. Li P, Liu Z, Yang C N. A construction method of (t, k, n)-essential secret image sharing scheme. Signal Processing: Image Communication, 2018, 65: 210–220
20. Chen H, Chang C C. A novel secret sharing scheme based upon euler's theorem. Security and Communication Networks, 2019, 2019: 2387358
21. Kawachi A, Okamoto Y, Tanaka K, Yasunaga K. General constructions of rational secret sharing with expected constant-round reconstruction. The

Computer Journal, 2017, 60(5): 711–728
22. Zhao J, Zhang J, Zhao R. A practical verifiable multi-secret sharing scheme. Computer Standards & Interfaces, 2007, 29(1): 138–141
23. Harn L, Hsu C F. (t, n) multi-secret sharing scheme based on bivariate polynomial. Wireless Personal Communications, 2017, 95(2): 1495–1504
24. Hedayat A S, Sloane N J A, Stufken J. Orthogonal Arrays: Theory and Applications. Springer Science & Business Media, 2012
25. Pieprzyk J, Zhang X M. Characterisations of ideal threshold schemes. Discrete Mathematics and Theoretical Computer Science, 2004, 6(2): 471–482

Lei Wu is a master student studying in the School of Computer Science and Technology in University of Science and Technology of China, China. She received bachelor's degree in information security from Hefei University of Technology, China in 2018. Her research interests include secret sharing and Internet of Things.

Fuyou Miao received the PhD degree in computer science from University of Science and Technology of China, China, where he is an associate professor currently with the School of Computer Science and Technology. His research interests include information security, information coding key management in WSN, and network security.

Keju Meng is a PhD student studying in the School of Computer Science and Technology, University of Science and Technology of China, China. He received bachelor's degree from Dalian Universiry of Technology, China in 2016. Now, his research interests include Internet of things, network security and secret sharing.

Xu Wang received her bachelor's degree from China University of Geosciences, China in 2019. After that, she has been studying for a master's degree at the University of Science and Technology of China, China. Her main research interests are secret sharing and coding.