Ideal Compartmented Secret Sharing Scheme Based on the Chinese Remainder Theorem for Polynomial Rings

Alexandru-Valentin Başagă[1], Sorin Iftene[1]

Faculty of Computer Science
Alexandru Ioan Cuza University
Iasi 700483, Romania

Abstract

A secret sharing scheme starts with a secret and then derives from it certain shares (or shadows) which are distributed to users. The secret may be recovered only by certain predetermined groups. In case of compartmented secret sharing, the set of users is partitioned into compartments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold and the total number of participants is greater than or equal to a global threshold. In this paper we use the Chinese Remainder Theorem for Polynomial Rings in order to construct an ideal compartmented secret sharing scheme, inspired by the work from [20].

Keywords: secret sharing, compartmented access structure, Chinese remainder theorem

1 Introduction and Preliminaries

A secret sharing scheme starts with a *secret* and then derives from it certain *shares* (*shadows*) which are distributed to users. The secret may be recovered only by certain predetermined groups. The initial applications of secret sharing were safeguarding cryptographic keys and providing shared access to strategical resources. More recently, secret sharing schemes are used as building blocks in threshold cryptographic schemes or in some e-voting schemes. The reader is referred to [6] for excellent recent survey on secret sharing.

In the first secret sharing schemes only the number of the participants in the reconstruction phase was important for recovering the secret. Such schemes have been referred to as *threshold* secret sharing schemes. We mention Shamir's threshold secret sharing scheme [16] based on polynomial interpolation, Blakley's geometric threshold secret sharing scheme [3], Mignotte's threshold secret sharing scheme [12] and Asmuth-Bloom threshold secret sharing scheme [1], both based on the Chinese remainder theorem (CRT). The popularity of CRT-based secret sharing schemes has recently grown due to some interesting recent papers, as [20], [19], [8], [13] (see also [17] for an excellent recent survey on modular (CRT-based) secret sharing).

In case of *compartmented* secret sharing, the set of users is partitioned into compartments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold, and the total number of participants is greater than or equal to a global threshold.

The paper is organized as follows. The rest of this section is dedicated to the Chinese remainder theorem over polynomial rings. In Section 2, after a brief introduction to secret sharing, we present an ideal threshold secret sharing scheme based on the Chinese remainder theorem for polynomial rings from [13], which will be the base of our proposed ideal compartmented secret sharing scheme from Section 3 . The last section concludes the paper.

The Chinese remainder theorem has many applications in computer science (see [7] for a survey on this topic). We only mention its applications to the *RSA* decryption algorithm as proposed by Quisquater and

[1] E-mail: {alexandru.basaga,sorin.iftene}@info.uaic.ro

Couvreur [15], the discrete logarithm algorithm as proposed by Pohlig and Hellman [14], and the algorithm for recovering the secret in Mignotte's threshold secret sharing scheme [12] or in Asmuth-Bloom threshold secret sharing scheme [1].

We include next only the standard version of the Chinese remainder theorem for polynomial rings over finite fields:

Theorem 1.1 *Let $k \geq 2$, $m_1(x), \ldots, m_k(x)$ pairwisely coprime polynomials over a finite field, and $b_1(x), \ldots, b_k(x)$ some arbitrary polynomials over the same finite field. Then the system of equations*

$$\begin{cases} X(x) \equiv b_1(x) \ \texttt{mod}\ m_1(x) \\ \qquad \vdots \\ X(x) \equiv b_k(x) \ \texttt{mod}\ m_k(x) \end{cases}$$

has a unique solution of degree less than the sum of the degrees of $m_1(x), \ldots, m_k(x)$.

This solution can be obtained as

$$X(x) = (\sum_{i=1}^{k} c_i(x) \cdot s_i(x)) \ \texttt{mod}\ m_1(x) \cdots m_k(x),$$

where $c_i(x) = \frac{m_1(x) \cdots m_k(x)}{m_i(x)}$ and $s_i(x) = (c_i(x) \ \texttt{mod}\ m_i(x))^{-1} \cdot b_i(x) \ \texttt{mod}\ m_i(x)$, for all $1 \leq i \leq k$.

2 Threshold Secret Sharing Schemes Based on the Chinese Remainder Theorem

We present first some basic facts about secret sharing schemes. The reader is referred to [6] for a survey on this topic. Suppose we have n users labeled with the numbers $1, \ldots, n$ and consider a set of groups $\mathcal{A} \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. Informally, an *$\mathcal{A}$-secret sharing scheme* is a method of generating $(S, (I_1, \ldots, I_n))$ such that

- for any $A \in \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$, is "easy";
- for any $A \in \mathcal{P}(\{1, 2, \ldots, n\}) \setminus \mathcal{A}$, the problem of finding the element S, given the set $\{I_i \mid i \in A\}$, is intractable.

The set $\mathcal{A}$ will be referred to as the *authorized access structure* or simply as the *access structure*, S will be referred to as the *secret* and $I_1, \ldots, I_n$ will be referred to as the *shares* (or the *shadows*) of S. The elements of the set $\mathcal{A}$ will be referred to as the *authorized groups*.

In a *perfect* secret sharing scheme, the shares of any unauthorized group give no information (in information-theoretical sense) about the secret. Karnin, Greene, and Hellman [11] have proved, using the concept of entropy, that in any perfect threshold secret sharing scheme, the shares must be at least as long as the secret and, later on, Capocelli, De Santis, Gargano, and Vaccaro [5] have extended this result to the case of any perfect secret sharing scheme. In an *ideal* secret sharing scheme, the shares are as long as the secret.

A natural condition is that an access structure $\mathcal{A}$ is *monotone* ([2]), i.e.,

$$(\forall B \in \mathcal{P}(\{1, 2, \ldots, n\}))((\exists A \in \mathcal{A})(A \subseteq B) \Rightarrow B \in \mathcal{A}).$$

Any monotone access structure $\mathcal{A}$ is well specified by the set of the minimal authorized groups, i.e., the set $\mathcal{A}_{min} = \{A \in \mathcal{A} | (\forall B \in \mathcal{A} \setminus \{A\})(\neg B \subseteq A)\}$. Also, the unauthorized access structure $\overline{\mathcal{A}}$, $\overline{\mathcal{A}} = \mathcal{P}(\{1, 2, \ldots, n\}) \setminus \mathcal{A}$, is well specified by the set of the maximal unauthorized groups, i.e., the set $\overline{\mathcal{A}}_{max} = \{A \in \overline{\mathcal{A}} | (\forall B \in \overline{\mathcal{A}} \setminus \{A\})(\neg A \subseteq B)\}$.

An important particular class of secret sharing schemes is that of the *threshold* secret sharing schemes. In these schemes, only the cardinality of the sets of shares is important for recovering the secret. More exactly, if the required threshold is k, $2 \leq k \leq n$, the minimal access structure is $\mathcal{A}_{min} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid |A| = k\}$. In this case, an $\mathcal{A}$-secret sharing scheme will be referred to as an *(k, n)-threshold secret sharing scheme*.

2.1 The Polynomial Variant of the Asmuth-Bloom Scheme

Next we present the scheme of Ning et al. [13], which is in fact a polynomial variant of the Asmuth-Bloom Scheme. This variant uses sequences of pairwisely coprime polynomials $p_0(x) = x^{d_0}, p_1(x), \ldots, p_n(x)$ over a

finite field, of degrees $d_0, d_1, \ldots, d_n \geq 1$ such that:

$$d_0 \leq d_1 \leq d_2 \leq \cdots \leq d_n, \text{ and}$$

$$d_0 + \sum_{i=n-k+2}^{n} d_i \leq \sum_{i=1}^{k} d_i.$$

- The secret $S(x)$ is chosen as a random polynomial over the same finite field, of degree less than or equal to $d_0 - 1$;
- The shares $I_i(x)$ are chosen as $I_i(x) = (S(x) + \gamma(x) \cdot p_0(x)) \bmod p_i(x)$, for all $1 \leq i \leq n$, where $\gamma(x)$ is a random polynomial over the same finite field of degree less than or equal to $(\sum_{i=1}^{k} d_i) - d_0 - 1$ (thus, the degree of the polynomial $S(x) + \gamma(x) \cdot p_0(x)$ is less than $\sum_{i=1}^{k} d_i$) ;
- Given k distinct shares $I_{i_1}(x), \ldots, I_{i_k}(x)$, the secret $S(x)$ can be obtained as $S(x) = f(x) \bmod p_0(x)$, where $f(x)$ is obtained, using the polynomial variant of the Chinese remainder theorem, as the unique solution modulo $p_{i_1}(x) \cdots p_{i_k}(x)$ of the system

$$\begin{cases} X(x) \equiv I_{i_1}(x) \bmod p_{i_1}(x) \\ \quad \vdots \\ X(x) \equiv I_{i_k}(x) \bmod p_{i_k}(x) \end{cases}$$

The authors have proven in [13] that the above threshold secret sharing scheme is perfect and, by choosing $d_0 = d_1 = \cdots d_n$, the scheme also achieves idealness.

3 Ideal Compartmented Secret Sharing Based on the Polynomial Chinese Remainder Theorem

In case of compartmented secret sharing, the set of users is partitioned into compartments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold, and the total number of participants is greater than or equal to a global threshold. The compartmented secret sharing has been discussed for the first time by Simmons in [18]. He has presented the example of an official action that requires that at least two U.S. members and at least two U.S.S.R. members be simultaneously present for its initiation.

The compartmented access structures can be introduced as follows.

Definition 3.1 Let $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ be a partition of $C_0 = \{1, 2, \ldots, n\}$ and consider a sequence $\mathcal{K} = \{k_0, k_1, k_2, \ldots, k_m\}$, where $k_j \leq |C_j|$, for all $0 \leq j \leq m$, and $\sum_{j=1}^{m} k_j \leq k_0$. The $(\mathcal{C}, \mathcal{K})$-*compartmented access structure* is given by

$$\mathcal{A} = \{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \ | (\forall j = \overline{0, m})(|A \cap C_j| \geq k_j)\}.$$

In this case, an $\mathcal{A}$-secret sharing scheme will be referred to as a $(\mathcal{C}, \mathcal{K})$-*compartmented secret sharing scheme*. The sets $C_1, C_2, \ldots, C_m$ will be referred to as the *compartments* of the scheme, the values $k_1, k_2, \ldots, k_m$ as the *compartment thresholds* and k_0 as the *global threshold* of the scheme.

Brickell [4] proposed an elegant solution for the case $k_0 = \sum_{j=1}^{m} k_j$ by expressing the secret S as a combination of some compartment secrets $s_1, \ldots, s_m$ and using an $(k_j, |C_j|)$-threshold secret sharing scheme for obtaining the shares $\{I_i | i \in C_j\}$ corresponding to the compartment secret s_j, for all $1 \leq j \leq m$. In the reconstruction phase, if the number of participants from the j^{th} compartment is greater than or equal to k_j, for all $1 \leq j \leq m$, then all compartment secrets can be recovered and, thus, the secret S can be obtained (remark that in this case the compartmented access structure can be simplified to $\{A \in \mathcal{P}(\{1, 2, \ldots, n\}) \mid (\forall j = \overline{1, m})(|A \cap C_j| \geq k_j)\}$).

Ghodosi, Pieprzyk, and Safavi-Naini proposed an efficient scheme for the general case in [9].

Compartmented secret sharing based on the Chinese remainder theorem on integers has been discussed in [10] or [19], but these versions are not perfect or ideal. On our best knowledge, ideal compartmented secret sharing based on the Chinese remainder theorem on polynomials has not been yet discussed in the literature. In fact, Yang et al. have left this issue as an open problem in their paper on hierarchical secret sharing [20]. We combine the approach from [10] with their approach as it will be described next. We will consider only the compartmented case $\sum_{j=1}^{m} k_j < k_0$ (the case $\sum_{j=1}^{m} k_j = k_0$ is completely covered by Brickell's approach).

Let us assume that, for any $0 \leq j \leq m$, that $C_j = \{u_1^j, \ldots, u_{|C_j|}^j\}$. Let us remark that any user $1 \leq i \leq n$ belongs to C_0 (as u_i^0) and also to an another $C_{comp(i)}$, for an unique $1 \leq comp(i) \leq m$ (as $u_{pos(i)}^{comp(i)}$, where $1 \leq pos(i) \leq |C_{comp(i)}|$ denotes the unique order number of the user i in the unique compartment $C_{comp(i)}$ to which i belongs to). Thus, in case $j \geq 1$, $i = u_l^j$ is equivalent with $j = comp(i)$ and $l = pos(i)$ (i.e., we have also $i = u_{pos(i)}^{comp(i)}$).

- The dealer generates the secret $S(x)$ as a random polynomial over some finite field, of degree less than or equal to $d_0 - 1$, for an arbitrary $d_0 \geq 1$ and sets $p_0(x) = x^{d_0}$;
- For each $1 \leq j \leq m$, the dealer generates $S_j(x)$ as a random polynomial over the same finite field, also of degree less than or equal to $d_0 - 1$, and set $S_0(x) = S(x) - (\sum_{j=1}^{m} S_j(x))$ (let us remark that $S_0(x)$ has also the degree less than or equal to $d_0 - 1$);
- For each $0 \leq j \leq m$, the dealer generates a sequence of integers $d_{u_1^j}^j, \ldots d_{u_{|C_j|}^j}^j$ such that

$$d_0 \leq d_{u_1^j}^j \leq d_{u_2^j}^j \leq \cdots \leq d_{u_{|C_j|}^j}^j, \text{ and}$$

$$d_0 + \sum_{l=|C_j|-k_j+2}^{n} d_{u_l^j}^j \leq \sum_{l=1}^{k_j} d_{u_l^j}^j;$$

- Then, for each $0 \leq j \leq m$ and for each $u_l^j \in C_j$, the dealer generates some pairwisely coprime polynomials $p_{u_l^j}^j(x)$ of degree $d_{u_l^j}^j$ over the same field, all with the free coefficient different than 0 (thus, they will be all also coprime with the polynomial $p_0(x)$);
- For each $1 \leq j \leq m$ and for each $u_l^j \in C_j$, the dealer generates the share $I_{u_l^j}(x)$ as

$$I_{u_l^j}(x) = (S_j(x) + \gamma_j(x) \cdot p_0(x)) \bmod p_{u_l^j}^j(x),$$

  where $\gamma_j(x)$ is a random polynomial over the same finite field of degree less than or equal to $(\sum_{l=1}^{k_j} d_{u_l^j}^j) - d_0 - 1$ (thus, the degree of the polynomial $S_j(x) + \gamma_j(x) \cdot p_0(x)$ is less than $\sum_{l=1}^{k_j} d_{u_l^j}^j$), for all $1 \leq j \leq m$);
- The dealer also generates $\gamma_0(x)$, a random polynomial over the same finite field of degree less than or equal to $(\sum_{i=1}^{k_0} d_{u_i^0}^0) - d_0 - 1$ (thus, the degree of the polynomial $S_0(x) + \gamma_0(x) \cdot p_0(x)$ is less than $\sum_{i=1}^{k_0} d_{u_i^0}^0$), and computes

$$t_i(x) = (S_0(x) + \gamma_0(x) \cdot p_0(x)) \bmod p_{u_i^0}^0(x),$$

  for all $1 \leq i \leq n$;
- For any $1 \leq i \leq n$, the dealer publishes $pub_i(x) = (t_i(x) - I_i(x)) \bmod p_{u_i^0}^0(x)$;

In this point, some remarks are required for a better understanding. Each user $i = u_{pos(i)}^{comp(i)} = u_l^j$ receives a single share, $I_i(x) = I_{u_{pos(i)}^{comp(i)}}(x)$ (or, equivalently, $I_i(x) = (S_{comp(i)}(x) + \gamma_{comp(i)}(x) \cdot p_0(x)) \bmod p_i^{comp(i)}(x)$) and for each user i, an information is published, namely $pub_i(x) = (t_i(x) - I_i(x)) \bmod p_i^0(x)$ (where $t_i(x) = (S_0(x) + \gamma_0(x) \cdot p_0(x)) \bmod p_i^0(x)$), for all $1 \leq i \leq n$. The same approach of publishing some informations is used in [20].

For the reconstruction of the secret in the case of a (minimal) authorized set A, the next steps are required:

- For each $1 \leq j \leq m$, the polynomial $S_j(x)$ is recovered, using the polynomial variant of the Chinese remainder theorem, as $f_j(x) \bmod p_0(x)$, where $f_j(x)$ is the unique solution modulo $\prod_{i \in A_j} p_i^j(x)$ of the system

$$\left\{ X(x) \equiv I_i(x) \bmod p_i^j(x), i \in A_j \right.$$

  for an arbitrary set $A_j \subseteq (A \cap C_j)$ such that $|A_j| = k_j$ (such an A_j certainly exists because A is an authorized set);

- Then, the polynomial $S_0(x)$ is recovered, using the polynomial variant of the Chinese remainder theorem, as $f_0(x) \bmod p_0(x)$, where $f_0(x)$ is the unique solution modulo $\prod_{i \in A_0} p_i^0(x)$ of the system

$$\left\{ X(x) \equiv (I_i(x) + pub_i(x)) \bmod p_i^0(x), i \in A_0 \right.$$

  for an arbitrary set $A_0 \subseteq A$ such that $|A_0| = k_0$ (such an A_0 certainly exists because A is an authorized set);
- Finally, the secret $S(x)$ is recovered as $\sum_{j=0}^{m} S_j(x)$

The correctness of the scheme is obvious, resulting from the correctness of each threshold secret sharing scheme used as a building block.

The same argument can be used for proving the perfectness of the scheme. Ning et al. have proven that the polynomial variant of Asmuth-Bloom threshold secret sharing scheme is perfect in [13]. Our scheme is, in fact, a composition (an addition) of such perfect threshold schemes and, therefore, is perfect itself. A similar result to Theorem 3.3 from [20] can be easily formulated and proven.

For achieving idealness, we may choose to set all members of all the sequences $d^j_{u_1^j}, \ldots d^j_{u^j_{|C_j|}}$ equal to d_0. The same idea is used in [20] to achieve idealness in their hierarchical scheme.

Example 3.2 illustrates the proposed construction.

Example 3.2 (with artificial small parameters)

Let us consider $n = 6$, $C_0 = \{1,2,3,4,5,6\}$, $m = 2$, $C_1 = \{1,2,3\} = \{u_1^1, u_2^1, u_3^1\}$, $C_2 = \{4,5,6\} = \{u_1^2, u_2^2, u_3^2\}$, the compartment thresholds $k_1 = 2$, $k_2 = 2$ and the global threshold $k_0 = 5$.

The dealer chooses to use the polynomial ring over the finite field $\mathbb{Z}_7$ as domain. The dealer then generates the secret $S(x) = 2x^4 + 5x^3 + 4x^2 + 3x + 5 \in \mathbb{Z}_7[X]$ and as a result sets $d_0 = 5$ and $p_0(x) = x^5$. The following secrets are randomly generated, corresponding to each compartment:

$$S_1(x) = x^4 + 5x^3 + 4x^2 + x + 6$$

$$S_2(x) = 2x^4 + 6x^3 + 2x^2 + 5x + 6$$

from which $S_0(x)$ is determined:

$$S_0(x) = S(x) - \sum_{j=1}^{m} S_j(x) = 6x^4 + x^3 + 5x^2 + 4x$$

The dealer then sets $d^j_{u_l^j} = d_0 = 5$, for each $0 \le j \le 2$ and $u_l^j \in C_j$.

- For each $0 \le j \le 2$ and $u_l^j \in C_j$, the dealer generates the following polynomials $p^j_{u_l^j}$, pairwisely coprime for the same j and all coprime with $p_0(x) = x^5$:

$$\begin{vmatrix} p^1_{u_1^1}(x) = 4x^5 + 5x^4 + 4x^3 + 4x + 5 \\ p^1_{u_2^1}(x) = 3x^5 + 5x^4 + 4x^3 + 6x^2 + 6x + 2 \\ p^1_{u_3^1}(x) = x^5 + 4x^4 + 3x^3 + 2x^2 + 6x + 2 \\ p^2_{u_1^2}(x) = 3x^5 + x^4 + 5x^2 + 4x + 3 \\ p^2_{u_2^2}(x) = 2x^5 + 2x^4 + 5x^3 + 2x^2 + 3x + 6 \\ p^2_{u_3^2}(x) = 5x^5 + x^4 + 6x^3 + 5x^2 + 3x + 4 \end{vmatrix}$$

  as well as randomly generating $\gamma_1(x) = 3x^4 + 5x^3 + 2x^2 + 5x + 3$ and $\gamma_2(x) = x^4 + 4x + 3$.

Then, the dealer computes the shares and distributes $I_{u_i^j}(x)$:

$$\begin{cases} I_{u_1^1}(x) = 5x^4 + x^3 + 2x^2 + 5x + 5 \\ I_{u_2^1}(x) = 2x^4 + 4x^3 + 6x^2 + 4x \\ I_{u_3^1}(x) = 5x^4 + 5x^3 + 4x^2 + 2x + 5 \\ I_{u_1^2}(x) = 3x^4 + 4x^3 + 6x^2 + 2x + 5 \\ I_{u_2^2}(x) = x^4 + 2x^2 + 3 \\ I_{u_3^2}(x) = 4x^4 + 5x^3 + 2x + 2 \end{cases}$$

- Corresponding to the global part of the secret, $S_0(x)$, the dealer also generates the coprime pairwise sequence of polynomials, which are also coprime with $p_0(x)$:

$$\begin{cases} p^0_{u_1^0}(x) = x^5 + 2x^4 + 6x^3 + 2x^2 + 1 \\ p^0_{u_2^0}(x) = 2x^5 + 2x^4 + 5x^2 + 5x + 5 \\ p^0_{u_3^0}(x) = x^5 + 5x^4 + 5x^3 + 2x^2 + x + 3 \\ p^0_{u_4^0}(x) = 2x^5 + 2x^4 + 5x^3 + x + 1 \\ p^0_{u_5^0}(x) = x^5 + 4x^4 + 4x^3 + 3x^2 + 5 \\ p^0_{u_6^0}(x) = 4x^5 + 6x^4 + 4x^3 + 2x^2 + 3 \end{cases}$$

and randomly generates

$$\gamma_0(x) = 4x^{19} + x^{17} + x^{16} + x^{15} + 5x^{14} + 2x^{13} + 2x^{11} + 3x^{10} + 5x^9 + 5x^8 + 6x^7 + 3x^6 + 3x^5 + x^4 + 5x^2 + 3x + 4.$$

Finally, the dealer computes

$$\begin{cases} t_1(x) = x^4 + 5x^3 + 4x^2 + 2x + 2 \\ t_2(x) = x^4 + 4x^3 + 3x^2 + 5x + 2 \\ t_3(x) = x^4 + 3x^2 + 6x + 6 \\ t_4(x) = 4x^4 + 6x^3 + 5x^2 + 2x \\ t_5(x) = 4x^4 + x^2 + 3x + 4 \\ t_6(x) = 6x^4 + 6x^2 + 5x \end{cases}$$

and publishes the following:

$$\begin{cases} pub_1(x) = 3x^4 + 4x^3 + 2x^2 + 4x + 4 \\ pub_2(x) = 6x^4 + 4x^2 + x + 2 \\ pub_3(x) = 3x^4 + 2x^3 + 6x^2 + 4x + 1 \\ pub_4(x) = x^4 + 2x^3 + 6x^2 + 2 \\ pub_5(x) = 3x^4 + 6x^2 + 3x + 1 \\ pub_6(x) = 2x^4 + 2x^3 + 6x^2 + 3x + 5 \end{cases}$$

Let us assume the users from the authorized set $\{1, 2, 3, 4, 5\}$ want to reconstruct the secret. They put together their shares $I_1(x)$, $I_2(x)$, $I_3(x)$, $I_4(x)$ and $I_5(x)$, and solve gradually the systems

$$\begin{cases} X_0(x) \equiv (5x^4 + x^3 + 2x^2 + 5x + 5) + (3x^4 + 4x^3 + 2x^2 + 4x + 4) \bmod x^5 + 2x^4 + 6x^3 + 2x^2 + 1 \\ X_0(x) \equiv (2x^4 + 4x^3 + 6x^2 + 4x) + (6x^4 + 4x^2 + x + 2) \bmod 2x^5 + 2x^4 + 5x^2 + 5x + 5 \\ X_0(x) \equiv (5x^4 + 5x^3 + 4x^2 + 2x + 5) + (3x^4 + 2x^3 + 6x^2 + 4x + 1) \bmod x^5 + 5x^4 + 5x^3 + 2x^2 + x + 3 \\ X_0(x) \equiv (3x^4 + 4x^3 + 6x^2 + 2x + 5) + (x^4 + 2x^3 + 6x^2 + 2) \bmod 2x^5 + 2x^4 + 5x^3 + x + 1 \\ X_0(x) \equiv (x^4 + 2x^2 + 3) + (3x^4 + 6x^2 + 3x + 1) \bmod x^5 + 4x^4 + 4x^3 + 3x^2 + 5 \end{cases}$$

$$\begin{cases} X_1(x) \equiv 5x^4 + x^3 + 2x^2 + 5x + 5 \bmod 4x^5 + 5x^4 + 4x^3 + 4x + 5 \\ X_1(x) \equiv 2x^4 + 4x^3 + 6x^2 + 4x \bmod 3x^5 + 5x^4 + 4x^3 + 6x^2 + 6x + 2 \\ X_1(x) \equiv 5x^4 + 5x^3 + 4x^2 + 2x + 5 \bmod x^5 + 4x^4 + 3x^3 + 2x^2 + 6x + 2 \end{cases}$$

$$\begin{cases} X_2(x) \equiv 3x^4 + 4x^3 + 6x^2 + 2x + 5 \bmod 3x^5 + x^4 + 5x^2 + 4x + 3 \\ X_2(x) \equiv x^4 + 2x^2 + 3 \bmod 2x^5 + 2x^4 + 5x^3 + 2x^2 + 3x + 6 \end{cases}$$

They obtain the following solutions:

$$\begin{aligned} f_0(x) &= 4x^{24} + x^{23} + x^{21} + x^{20} + 5x^{19} + 2x^{18} + 2x^{16} + 3x^{15} + 5x^{14} + 5x^{13} + 6x^{12} + 3x^{11} + 3x^{10} + \\ &\quad x^9 + 5x^7 + 3x^6 + 4x^5 + 6x^4 + x^3 + 5x^2 + 4x \\ f_1(x) &= 3x^9 + 5x^8 + 2x^7 + 5x^6 + 3x^5 + x^4 + 5x^3 + 4x^2 + x + 6 \\ f_2(x) &= x^9 + 4x^6 + 3x^5 + 2x^4 + 6x^3 + 2x^2 + 5x + 6 \end{aligned}$$

Reducing these solutions modulo x^5, they obtain the secret parts, $S_0(x) = 6x^4 + x^3 + 5x^2 + 4x$, $S_1(x) = x^4 + 5x^3 + 4x^2 + x + 6$ and $S_2(x) = 2x^4 + 6x^3 + 2x^2 + 5x + 6$. The secret is then reconstructed successfully as $S(x) = \sum_{j=0}^{2} S_j(x) = 2x^4 + 5x^3 + 4x^2 + 3x + 5$.

We have to emphasize that this approach of publishing some information in order to achieve idealness is quite contrived. In the solution from [20], the dealer, for each user in j-th level, publishes $m - j$ informations. In our case, for each user, independently of what compartment they belong to, a single information is published. It is natural to try to minimize the amount of published information.

By careful tuning of some of the polynomials used in the schemes that act as building blocks, so that the global components of some shares coincide with the corresponding compartment ones, i.e., $t_i(x) = I_i(x)$, for some $i \in \{1, 2, \ldots, n\}$, the amount of information that needs to be published can be minimized. In this case For this, we can generate first the secret parts $S_1(x), \ldots, S_m(x)$, then the sequences $p^j_{u^j_l}(x)$ and $\gamma_j(x)$, for $1 \leq j \leq m$ and $u^j_l \in C_j$. We can thus compute $I_1(x), \ldots, I_n(x)$ and determine $S_0(x) = f_0(x) \bmod p_0(x)$, where $f_0(x)$ is the solution of the system of equations

$$\begin{cases} X(x) \equiv I_{i_1}(x) \bmod p_{i_1}^{comp(i_1)}(x) \\ \quad\quad \vdots \\ X(x) \equiv I_{i_k}(x) \bmod p_{i_{k_0}}^{comp(i_{k_0})}(x) \end{cases}$$

where $\{i_1, \ldots, i_{k_0}\}$ is an arbitrary authorized set of users.

However, it must be noted that in order for this system to have an unique solution modulo $p_{i_1}(x) \cdots p_{i_{k_0}}(x)$, the previous condition that the polynomials $p^j_{u^j_l}(x)$ must be pairwisely coprime for a given j now becomes that any two such polynomials are coprime, even if they are not related to the same compartment C_j. In other words, any $p^{j_1}_{i_1}(x)$ and $p^{j_2}_{i_2}(x)$, for $i_1, i_2 \in \{1, \ldots n\}$ and $j_1, j_2 \in \{1, \ldots m\}$, must be coprime. This condition does not affect the security of the scheme in any way, but such restrains on the parameters may affect the ease of construction. We choose $\{1, 2, \ldots, k_0\}$ as our set $\{i_1, \ldots, i_{k_0}\}$ from now on.

- For $i \in \{1, 2, \ldots, k_0\}$ used, we can consider $p^0_i(x) = p^{comp(i)}_{pos(i)}(x)$.
  We will choose $I_i(x) = t_i(x)$ and not publish anything.
- For $i \in \{k_0 + 1, \ldots, n\}$, we can generate the sequence $p^0_i(x)$, also pairwisely coprime with polynomials of the other sequences, and generate the random polynomial $\gamma_0(x)$.
  We will choose $t_i(x) = (S_0(x) + \gamma_0(x) \cdot p_0(x)) \bmod p^0_i(x)$ and $pub_i(x) = (t_i(x) - I_i(x)) \bmod p^0_i(x)$, for all $k_0 + 1 \leq i \leq n$.

Example 3.3 illustrates the reduction of the published information.

Example 3.3 (with artificial small parameters)

Let us reconsider Example 3.2, choosing the same secret parts:

$$S_1(x) = x^4 + 5x^3 + 4x^2 + x + 6$$
$$S_2(x) = 2x^4 + 6x^3 + 2x^2 + 5x + 6$$

However, due to the new condition of coprimality enforced upon the sequences $p_i^j(x)$, the dealer has to generate new polynomials:

$$\begin{vmatrix} p^1_{u^1_1}(x) = 2x^5 + 2x^4 + 4x^3 + 2x^2 + 3x + 5 \\ p^1_{u^1_2}(x) = 3x^5 + 3x^4 + 4x^3 + x^2 + 2x + 3 \\ p^1_{u^1_3}(x) = 5x^5 + 6x^3 + 2x + 1 \\ p^2_{u^2_1}(x) = x^5 + 6x^3 + 2x^2 + 6 \\ p^2_{u^2_2}(x) = 4x^5 + 4x^4 + 4x^3 + 5x^2 + 2x + 5 \\ p^2_{u^2_3}(x) = 3x^5 + 6x^4 + 5x^3 + 2x^2 + 4x + 6 \\ \gamma_1(x) = 6x^4 + 2x^3 + 3x^2 + 4 \\ \gamma_2(x) = 6x^4 + 6x^3 + x^2 + 6x + 5 \end{vmatrix}$$

Then, the dealer computes the shares and distributes $I_{u_i^j}(x)$:

$$\begin{vmatrix} I_{u^1_1}(x) = 2x^4 + x^3 + 4x^2 + 5x + 1 \\ I_{u^1_2}(x) = 4x^4 + 5x^3 + 5x^2 + 4x + 3 \\ I_{u^1_3}(x) = 3x^4 + x^3 + 3x^2 + 4 \\ I_{u^2_1}(x) = x^4 + 5x^3 + 2x^2 + 5x + 6 \\ I_{u^2_2}(x) = 6x^4 + 5x^3 + 3x^2 + 5x + 6 \\ I_{u^2_3}(x) = 4x^4 + 4x^3 + x^2 + 5x + 3 \end{vmatrix}$$

$S_0(x)$ can be computed as $S_0(x) = f_0(x) \bmod x^5$, where $f_0(x)$ is the solution to the following system:

$$\begin{cases} X(x) \equiv 2x^4 + x^3 + 4x^2 + 5x + 1 \bmod 2x^5 + 2x^4 + 4x^3 + 2x^2 + 3x + 5 \\ X(x) \equiv 4x^4 + 5x^3 + 5x^2 + 4x + 3 \bmod 3x^5 + 3x^4 + 4x^3 + x^2 + 2x + 3 \\ X(x) \equiv 3x^4 + x^3 + 3x^2 + 4 \bmod 5x^5 + 6x^3 + 2x + 1 \\ X(x) \equiv x^4 + 5x^3 + 2x^2 + 5x + 6 \bmod x^5 + 6x^3 + 2x^2 + 6 \\ X(x) \equiv 6x^4 + 5x^3 + 3x^2 + 5x + 6 \bmod 4x^5 + 4x^4 + 4x^3 + 5x^2 + 2x + 5 \end{cases}$$

As such, the dealer sets $S_0(x) = 6x^4 + 5x^3 + 3x^2 + 5x + 6$. The dealer generates the remaining necessary polynomials to compute $I_{u^2_3}(x)$ and $t_6(x)$:

$$\begin{vmatrix} p^0_{u^0_6}(x) = 2x^5 + 5x^3 + 5x^2 + 4 \\ \gamma_0(x) = 3x^{17} + 3x^{15} + 5x^{14} + 2x^{10} + 3x^6 + x^5 + x^4 + x + 1. \end{vmatrix}$$

$$\Rightarrow t_6(x) = (S_0(x) + \gamma_0(x) \cdot p_0(x)) \bmod p^0_{u^0_6}(x) = 6x^4 + 6x^3 + 4x^2 + 5x + 6$$

Finally, the secret will be $S(x) = S_0(x) + S_1(x) + S_2(x) = 2x^4 + 2x^3 + 2x^2 + 4x + 4$ and the only published information will be $pub_6(x) = 2x^4 + 2x^3 + 3x^2 + 3$.

This approach is equivalent to assuring that the corresponding public information $pub_i(x)$ is constant, e.g. 0, for $i \in \{1, 2, \ldots, k_0\}$, which means that no informations need to be published for these users. It would be interesting to see if this is possible for more users, even, ideally, for all users.

4 Conclusions

In this paper, we use ideal threshold secret sharing based on the polynomial variant of the Chinese remainder theorem in order to construct an ideal compartmented secret sharing scheme. The price of idealness is publishing some information as inspired from the work in [20]. We are concerned in reducing the amount of published

information, and we have succeeded for some cases. We shall investigate further improvements in this regard in our future work.

References

[1] Asmuth, C. A. and J. Bloom, *A modular approach to key safeguarding*, IEEE Transactions on Information Theory **IT-29** (1983), pp. 208–210.

[2] Benaloh, J. and J. Leichter, *Generalized secret sharing and monotone functions*, in: S. Goldwasser, editor, *Advanced in Cryptology-CRYPTO' 88*, Lecture Notes in Computer Science **403** (1989), pp. 27–35.

[3] Blakley, G. R., *Safeguarding cryptographic keys*, in: *National Computer Conference, 1979*, American Federation of Information Processing Societies Proceedings **48**, 1979, pp. 313–317.

[4] Brickell, E. F., *Some ideal secret sharing schemes.*, in: J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89*, Lecture Notes in Computer Science **434** (1990), pp. 468–475.

[5] Capocelli, R. M., A. D. Santis, L. Gargano and U. Vaccaro, *On the size of shares for secret sharing schemes*, Journal of Cryptology **6** (1993), pp. 157–167, (a preliminary version of this paper appeared in Advances in Cryptology - CRYPTO '91).

[6] Chattopadhyay, A. K., S. Saha, A. Nag and S. Nandi, *Secret sharing: A comprehensive survey, taxonomy and applications*, Comput. Sci. Rev. **51** (2024), p. 100608.

[7] Ding, C., D. Pei and A. Salomaa, "Chinese remainder theorem: applications in computing, coding, cryptography," World Scientific Publishing Co., Inc., 1996.

[8] Dragan, C. C. and F. L. Tiplea, *On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme*, Inf. Sci. **463–464** (2018), pp. 75–85.

[9] Ghodosi, H., J. Pieprzyk and R. Safavi-Naini, *Secret sharing in multilevel and compartmented groups.*, in: C. Boyd and E. Dawson, editors, *ACISP '98: Proceedings of the Third Australasian Conference on Information Security and Privacy*, Lecture Notes in Computer Science **1438** (1998), pp. 367–378.

[10] Iftene, S., *General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting*, in: C. Dima, M. Minea and F. L. Tiplea, editors, *Proceedings of the First Workshop in Information and Computer Security, ICS@SYNASC 2006, Timisoara, Romania, September 30, 2006*, Electronic Notes in Theoretical Computer Science **186** (2006), pp. 67–84.

[11] Karnin, E. D., J. W. Greene and M. E. Hellman, *On secret sharing systems*, IEEE Transactions on Information Theory **IT-29** (1983), pp. 35–41.

[12] Mignotte, M., *How to share a secret*, in: T. Beth, editor, *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982*, Lecture Notes in Computer Science **149** (1983), pp. 371–375.

[13] Ning, Y., F. Miao, W. Huang, K. Meng, Y. Xiong and X. Wang, *Constructing Ideal Secret Sharing Schemes Based on Chinese Remainder Theorem*, in: T. Peyrin and S. Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018* (2018), pp. 310–331.

[14] Pohlig, S. C. and M. E. Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Transactions on Information Theory **24** (1978), pp. 106–110.

[15] Quisquater, J.-J. and C. Couvreur, *Fast decipherment algorithm for the RSA public-key cryptosystem*, IEE Electronics Letters **18 (21)** (1982), pp. 905–907.

[16] Shamir, A., *How to share a secret*, Communications of the ACM **22** (1979), pp. 612–613.

[17] Shenets, N., *On modular (CRT-based) secret sharing*, J. Comput. Virol. Hacking Tech. **20** (2024), pp. 765–782.

[18] Simmons, G. J., *How to (really) share a secret.*, in: S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88*, Lecture Notes in Computer Science **403** (1990), pp. 390–448.

[19] Tiplea, F. L. and C. C. Dragan, *Asymptotically ideal Chinese remainder theorem -based secret sharing schemes for multilevel and compartmented access structures*, IET Inf. Secur. **15** (2021), pp. 282–296.

[20] Yang, J., S.-T. Xia, X. Wang, J. Yuan and F.-W. Fu, *A perfect ideal hierarchical secret sharing scheme based on the CRT for polynomial rings*, in: *2024 IEEE International Symposium on Information Theory (ISIT)*, 2024, pp. 321–326.