Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

Mathematical Biosciences and Engineering, 16(3): 1280–1299
DOI: 10.3934/mbe.2019062
Received: 25 November 2018
Accepted: 18 January 2019
Published: 19 February 2019

Research article

A collaborative secret sharing scheme based on the Chinese Remainder Theorem

Xingxing Jia[1,*], Yixuan Song[1], Daoshun Wang[2,*], Daxin Nie[1] and Jinzhao Wu[3]

[1] School of Mathematics and Statistics, Lanzhou University, Lanzhou, Gansu 730000, China
[2] School of Computing, Tsinghua University, Beijing 100084, China
[3] School of Software, Guangxi University for Nationalities, Nanning, Guangxi 530006, China

* **Correspondence:** Email: jiaxx@lzu.edu.cn, daoshun@mail.tsinghua.edu.cn; Tel: +86-931-891-2483; Fax: +86-931-891-2481.

Abstract: Secret sharing (SS) can be used as an important group key management technique for distributed cloud storage and cloud computing. In a traditional threshold SS scheme, a secret is shared among a number of participants and each participant receives one share. In many real-world applications, some participants are involved in multiple SS schemes with group collaboration supports thus have more privileges than the others. To address this issue, we could assign multiple shares to such participants. However, this is not a bandwidth efficient solution. Therefore, a more sophisticated mechanism is required. In this paper, we propose an efficient collaborative secret sharing (CSS) scheme specially tailored for multi-privilege participants in group collaboration. The CSS scheme between two or among more SS schemes is constructed by rearranging multi-privilege participants in each participant set and then formulated into several independent SS schemes with multi-privilege shares that precludes information leakage. Our scheme is based on the Chinese Remainder Theorem with lower recovery complexity and it allows each multi-privilege participant to keep only one share. It can be formally proved that our scheme achieves asymptotically perfect security. The experimental results demonstrate that it is efficient to achieve group collaboration, and it has computational advantages, compared with the existing works in the literature.

Keywords: group collaboration; collaborative secret sharing; Chinese Remainder Theorem; secret sharing

1. Introduction

Online collaboration among multiple entities becomes a very popular application nowadays due to automatic data backup and cross-regional group collaboration requirements in cloud computing.

The collaborative and sharing nature of data storage in the cloud demands greater group collaborations [1, 2]. However, each participating entity would like to protect its privileges before outsourcing its data to the cloud servers. One feasible solution is to use secret sharing (SS) to enable group key management in the distributed fashion, so that the distrusting entities with conflicting interest can cooperate honestly and securely. In a (k, n)-SS scheme, the secret is shared among a number of participants. Due to the flexibility and convenience of cloud computing, the participants often need to participant in different SS sharing systems in different applications. If we just use the traditional SS scheme to design the management system, a participant joining in multiple management systems, called multi-privilege participant, will need to store multiple shares in each application, which is inconvenient. Consider the following scenario concerning data sharing.

With the development of big data and artificial intelligence (AI), data with multiple owners are often needed to be aggregated to accomplish an important task by using AI techniques. For example, the financial datas from cities A, B and C are running in a cooperated and distributed manner to analyze an economic development index as illustrated in Figure 1. The financial data, traffic data, population data of city A is used to analyze the urban construction planning. The financial data from city A is used in different group collaborative tasks. A convenient and secure data management system is the first consideration for such confidential data against untrusted cloud. This phenomenon has become more common in cloud data collaboration among different data owners. The data owner of city A must carry two shares to manage the data in different collaborative tasks. If a data owner is involved in a large number of data collaborative tasks, he or she needs to keep many shares, which can be a burden.

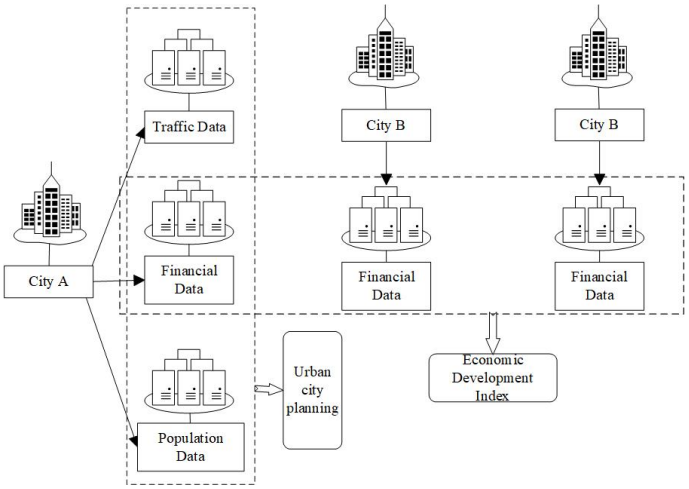

Figure 1. Data sharing scenario.

Therefore, it is desirable to have a SS scheme such that each multi-privilege participant needs to keep only one share in its related tasks. Not only it will be more convenient for the participants, but also the multiple key management systems can be made more practical. In this paper, we just propose such a scheme based on the Chinese Remainder Theorem (CRT).

The SS schemes were first introduced by Shamir [3] and Blakley [4] independently to share a secret among a group of n participants. It allows the secret to be reconstructed when more than the threshold k of these participants are working together, but less participants cannot recover the secret. Thanks to its high level of security protection and low computatonal requirements, SS schemes have

been used in various applications, such as human-verifiable authentication [5], group collaboration [6, 7], and secure multiparty computation [8]. Nowadays, with the popularity of cloud computing, SS schemes have emerged as an important technology for secure data storage in the cloud, secure group management [9–11], and reputation adjustment in social network [12, 13].

In a (k, n) SS scheme, the regular participant can obtain only one share. The multi-privilege participant who has more privileges will receive multiple shares, which is inconvenient. In cloud computing environments, group collaboration between two or more management systems is widely used in the era of shared economy [14]. Consider the following scenario regarding group collaboration: a participant joins in multiple reputation systems in the social network and she will have multiple reputation values using secret sharing schemes [12, 13, 15]. A collaborative reputation management system will allow this multi-privilege participant to share her reputation in different platforms. In general, the above scenarios can be described as a cryptographic model: a multiple secret sharing scheme is designed to share multiple secrets independently, while the participants and the secrets have the many-to-many relationships. Inspired by the practical problems arisen in the above scenarios, it is desirable to design a scheme to facilitate the group collaboration among different threshold secret sharing schemes so that each multi-privilege participant only needs to keep one share.

How to collaborate between threshold secret sharing schemes was first proposed by [16] to solve bank managers with multiple privileges problem. In their scheme, if u participants are involved in both schemes, each of these u multi-privilege participant keeps only one share by constructing polynomials with common solutions. Here we call the participants who are involved in multiple SS schemes as multi-privilege participants, and their shares are called multi-privilege shares. Each secret can be uniquely reconstructed by Lagrange interpolation, but it requires $O(k \log^2 k)$ operations. The collaborative visual cryptographic scheme was formulated as an integer linear programming problem that minimizes pixel expansion under the corresponding security and contrast constraints in [11]. Each multi-privilege participant takes one share and can reconstruct the secret together with the other participants when they belong to the designated qualified subsets family. The secret can be visually recovered without any computation but with lower quality. The scheme has strict constraints for the participant intersection [16]. The collaborative visual scheme will suffer from severe pixel expansion problem. Hence, it will become impractical when the participant intersections are complex [11]. Since a group collaboration in the cloud may involve flexible and complex computations, participant intersections are also complex. Therefore, it is desirable to construct a collaborative secret sharing (CSS) scheme to allow complex participant intersections and to recover the secret perfectly with lower computational complexity.

Another important mathematical model to address the threshold SS scheme is the Chinese Remainder Theorem (CRT), which requires only $O(k)$ operations in the secret reconstruction phase [17, 18]. The scheme in [18] is proved by [19–21, 24] having asymptotically perfect security and is practical due to its high efficiency and simple construction. The CRT has been extensively used in various SS schemes and has produced abundant research results. Shares in the (k, n) SS scheme based on the CRT form a redundant representation of the secret, which provides a number-theoretic construction of an "error-correcting code" in [21]. The threshold changeable secret sharing scheme in [22] is a lattice-based "error-correction" algorithm that can be seen as an application of the algorithm in 'Noisy Chinese Remaindering in the Lee Norm' [23]. It is accomplished based on CRT by adding noise to the shares. Intensive analysis of the security was presented in [24], and the prime sequence generation algorithm

for the Asmuth-Bloom scheme was proposed for the first time. A multi-level threshold scheme [25] was constructed by using the CRT. Harn et al. devised the general secret sharing scheme [26] based on the CRT with Boolean logic and integer linear/non-integer programming. Drăgan and Ţiplea proposed the distributive weighted threshold SS scheme [27], which has perfect zero-knowledge. In order to decrease the recovery complexity, we consider to use the CRT to construct the collaborative secret sharing scheme in this paper.

Inspired by the previous works in [16] and [18], we present a novel scheme to solve the collaboration problem based on CRT, which can reconstruct the secret with the same security as in scheme [18]. The computational complexity is only $O(k)$ in the secret reconstruction phase. Our method avoids high complexity, and restrictive participant intersections of [16], and the low recovery quality and extremely large pixel expansion of [11]. The compromise is that our scheme needs to publish n moduli as the public parameters comparable with one parameter in [11, 16]. The advantage of its single share and lower computation complexity make our approach ideal for high-through processing applications. It will provide an efficient outsourced computation platform which will facilitate the group collaboration among different secret-data owners. The proposed scheme can be used as a building block to handle different types of group collaborations.

In summary, the contributions of this paper are summarized as follows. A collaborative secret sharing scheme framework is proposed, in which the Chinese Remainder Theorem is used to lower the computational complexity. It can fully achieve the group collaboration functionality and security requirements. This contributes to a better performance than comparative state-of-the-art polynomial methods. Complex participant intersections are designed so that each multi-privilege participant just keeps one share even if multiple secrets are shared. Our approach to building CSS scheme may have some independent interests, and it may find applications in related cryptographic protocols.

The remainder of this paper is organized as follows. Section 2 gives the definition of SS scheme using entropy terms, the preliminaries of the CRT, the SS scheme based on the CRT [18]. Section 3 gives the definition of collaboration between two schemes and presents the algorithm design. Collaboration among three or more schemes is different from the collaboration between two schemes in terms of participant intersection and the presentation format, which is addressed in the same section. The correctness and security are analysed in Section 4, followed by the comparison of performance between the proposed scheme and the schemes in [16] and [11]. One example is presented to demonstrate the construction process. Finally, conclusions are drawn in Section 5.

2. Preliminaries

In this section, we review the key building blocks, including the definition of SS scheme, the Chinese Remainder Theorem and Asmuth-Bloom's scheme used in our scheme.

2.1. Definition of the SS scheme

SS scheme is an important key management technique by decomposing a secret into input shares. The (k, n) secret sharing scheme is the common used SS schemes, where n is the number of participants and $k(\leq n)$ is called threshold, which is pre-determined according to the security policy or the adversary model. The scheme has perfect security if participants not belonging to the access structure obtain no information about the secret. The access structure refers to the qualified subset holding at least k shares

which can recover the secret.

Let $\mathbb{P} = \{P_1, \cdots, P_n\}$ be a set of n participants, $S \subseteq \{0,1\}^x$ be a finite set of secrets, called the secret-domain, and R be a set of random strings. $H(\cdot)$ stands for the Shannon entropy and $H(\cdot|\cdot)$ denotes the conditional entropy. A secret sharing scheme over $\mathbb{P}$ is a mapping $\Pi : S \times R \to S_1 \times \cdots \times S_n$, where S_i is called the share-domain of P_i. Dealer shares a secret $s \in S$ among the participants according to Π by first sampling a random string $r \in R$, computing the shares $(S_1, \cdots, S_n)$, and then privately communicating each share S_i to P_i. For any subset $A \in \mathbb{P}$, S_A denotes the set of shares held by all participants in A. There are multiple forms of definitions for (k, n) SS scheme. From the information theory point of view, its definition is widely used to demonstrate its performance. In present study, we adopt the definition from [28].

Definition 2.1. *(Secret Sharing Scheme [28]). A (k, n) threshold secret sharing scheme over a participant set $\mathbb{P}$ is a secret sharing scheme $\Pi : S \times R \to S_1 \times \cdots \times S_n$ satisfying the following two conditions:*

1. *for all $A \subseteq \mathbb{P}$ and $|A| \geq k$, $H(S|S_A) = 0$;*
2. *for all $A \subseteq \mathbb{P}$ and $|A| < k$, $0 < H(S|S_A) \leq H(S)$.*

A scheme is called perfect if $H(S|S_A) = H(S)$ holds for all $A \subseteq \mathbb{P}$ and $|A| < k$. A scheme is called asymptotically perfect if for all $\epsilon > 0$, there exists $x_0 \geq 0$ such that for all $A \subseteq \mathbb{P}$ with $x \geq x_0$, we have that

$$\triangle H = |H(S) - H(S|S_A)| \leq \epsilon$$

holds for all $|A| < k$ (see the definition 4 in section 2 [20]).

2.2. Chinese Remainder Theorem

Theorem 1. *(Chinese Remainder Theorem [30]). If $p_1, p_2, \ldots, p_k$ are pairewise coprime positive integers, then the following equations of congruence*

$$\begin{cases} S \equiv S_1 \bmod p_1, \\ S \equiv S_2 \bmod p_2, \\ \cdots, \\ S \equiv S_k \bmod p_k, \end{cases} \tag{2.1}$$

have a unique solution

$$S \equiv \sum_{i=1}^{k} \frac{P}{p_i} S_i y_i \bmod P, \tag{2.2}$$

where $P = \prod_{i=1}^{k} p_i$, $\frac{P}{p_i} y_i \equiv 1 \bmod p_i$, and "$\equiv$" denotes the relation of congruence.

The CRT states that a positive integer S is uniquely specified by its remainder modulo k relatively prime integers p_1, p_2, $\cdots$, p_k, provided $S < \prod_{i=1}^{k} p_i$. The CRT has been used in RSA decryption to accelerate the decryption process [30]. It is also well known in communication applications as error-correction codes [30] and image encryption [31]. The CRT can also be used to design various SS

schemes [17, 18, 22, 25–27, 29]. The SS scheme based on CRT uses a special sequence of integers to guarantee the security and recovery of the secret. In our scheme, we use the CRT to design a CSS scheme, which can be seen as an extended application of CRT. In the next subsections, we will review the well-known SS scheme [18] based on the CRT.

2.3. Asmuth-Bloom's SS scheme based on the CRT

The SS schemes based on the CRT were designed by Mignotte [17] and Asmuth, Bloom [18], respectively. The SS scheme uses a special increasing sequence of pairwise coprime integers satisfying formula (2.3) to achieve asymptotically perfect security [18] and is widely used as the fundamental scheme to construct related SS schemes [22, 25–27]. The Asmuth-Bloom SS scheme is given in the following.

Distribution phase

1. Select relatively prime integers $p_0 < p_1 < \cdots < p_n$, where p_0 is a large secure prime, and the $n+1$ primes satisfy the following relationship

$$\prod_{i=1}^{k} p_i > p_0 \prod_{i=1}^{k-1} p_{n-i+1}. \tag{2.3}$$

2. The dealer selects a secret $s \in \mathbb{Z}_{p_0}$ and computes $S = s + \alpha \cdot p_0$, where α is a random positive integer satisfying the condition $\prod_{i=1}^{k-1} p_{n-i+1} < S < \prod_{i=1}^{k} p_i$ (This formula is enhanced in security by Harn and Fu in [25] from $0 < S < \prod_{i=1}^{k} p_i$ in [18]).
3. The share for participant i is $S_i \equiv S \bmod p_i$, $i \in \{1, 2, \ldots, n\}$.

Reconstruction phase

1. Let A be the participant set that reconstructs the sharing secret with k or more participants. The participants send their shares to the combiner secretly.
2. The combiner computes

$$S \equiv \sum_{i \in A} S_i P'_{A\setminus\{i\}} P_{A\setminus\{i\}} \bmod P_A$$

and obtains secret s by $s \equiv S \bmod p_0$. Set $P_A = \prod_{i \in A} p_i$ and $P_{A\setminus\{i\}} = \prod_{\substack{j \in A, \\ j \neq i}} p_j$. $P'_{A\setminus\{i\}}$ is the multiplicative inverse of $P_{A\setminus\{i\}}$ in $\mathbb{Z}_{p_i}$, which means that we have $P'_{A\setminus\{i\}} P_{A\setminus\{i\}} \equiv 1 \bmod p_i$.

3. Construction of the CSS scheme based on CRT

This section first presents the collaboration between two SS schemes in which each multi-privilege participant holds only one share. Then, the collaboration among more SS schemes is constructed. We assume each scheme is constructed by the trusted third party. We call it the dealer. Different dealers are honest to transfer the necessary information and will not collude with any participants. In this paper, we emphasize on the basic model construction.

3.1. Definition of the collaborative secret sharing scheme between two SS schemes

Assume two secrets s_1 and s_2 are concealed in a (k_1, n_1) scheme among participants in the set $\mathbb{P}_1 = \{P_1^1, \ldots, P_{n_1}^1\}$ and a (k_2, n_2) scheme among participant set $\mathbb{P}_2 = \{P_1^2, \ldots, P_{n_2}^2\}$ separately, where $k_1, n_1, k_2, n_2 \in \mathbb{Z}^+$. The multi-privilege participant set is denoted as $\mathrm{U} = \mathbb{P}_2 \bigcap \mathbb{P}_1 = \{P_1^{2,1}, \ldots, P_u^{2,1}\}$ with $|\mathrm{U}| = u$, the three values u, k_1 and k_2 are not equal. The collaborative scheme between two SS schemes is denoted as a $((k_1, n_1); (k_2, n_2))$-CSS scheme with U. In order to protect each shared secret against colluding attacks, we generally require $u < \min\{k_1, k_2\}$. It means that the recovery of each secret requires at least one internal participant who doesn't participant in any other SS scheme. A formal definition of the $((k_1, n_1); (k_2, n_2))$-CSS scheme with U is given below.

Definition 2 A (k_1, n_1)-SS scheme with participant set $\mathbb{P}_1 = \{P_1^1, \ldots, P_{n_1}^1\}$ to share a secret s_1 and a (k_2, n_2)-SS scheme with participant set $\mathbb{P}_2 = \{P_1^2, \ldots, P_{n_2}^2\}$ to share a secret s_2 constitute a $((k_1, n_1); (k_2, n_2))$-CSS scheme with U, where $\mathrm{U} = \mathbb{P}_2 \bigcap \mathbb{P}_1 = \{P_1^{2,1}, \ldots, P_u^{2,1}\}$ and $|\mathrm{U}| = u$ if the following two conditions are satisfied:

1. for all $A \subseteq \mathbb{P}_1$ and $|A| \geq k_1$, $H(s_1|S_A) = 0$; for all $A \subseteq \mathbb{P}_2$ and $|A| \geq k_2$, $H(s_2|S_A) = 0$;
2. for all $A \subseteq \mathbb{P}_1 \bigcup \mathbb{P}_2$ and $|A \bigcap \mathbb{P}_1| < k_1$, $0 < H(s_1|S_A) \leq H(s_1)$; for all $A \subseteq \mathbb{P}_1 \bigcup \mathbb{P}_2$ and $|A \bigcap \mathbb{P}_2| < k_2$, $0 < H(s_2|S_A) \leq H(s_2)$.

The first condition ensures that each secret can be revealed correctly by its authorized subsets. The second condition prevents unauthorized subsets from collusively revealing the secret. When the equality holds in the second condition, the $((k_1, n_1); (k_2, n_2))$-CSS scheme with U has perfect security. It is called asymptotically perfect if for all $\epsilon > 0$, there exists $x_0 \geq 0$ such that for all $A \subseteq \mathbb{P}_1 \bigcup \mathbb{P}_2$ with $x \geq x_0$, we have that

$$\triangle H = |H(s_i) - H(s_i|S_A)| \leq \epsilon$$

holds for all $|A \bigcap \mathbb{P}_i| < k_i$, $i \in \{1, 2\}$.

3.2. Construction method for a $((k_1, n_1); (k_2, n_2))$-CSS scheme with U

Since a $((k_1, n_1); (k_2, n_2))$-CSS scheme with U is a collaborative scheme, we assume that the (k_1, n_1) scheme is constructed first and then the multi-privilege shares are passed on to the dealer of the (k_2, n_2) scheme. Each (k_i, n_i) is an independent Asmuth-Bloom scheme, in addition to satisfying the collaborative conditions. The proposed $((k_1, n_1); (k_2, n_2))$-CSS scheme with U is presented in Scheme 1.

Scheme 1 The proposed $((k_1, n_1); (k_2, n_2))$-CSS scheme with U

Distribution phase

1. Dealer 1 chooses a large prime number p_0 and a sequence of pairwise coprime positive integers

$$p_0 < p_1 < p_2 < \cdots < p_{n_1}$$

such that $\prod_{i=1}^{k_1} p_i > p_0 \prod_{i=1}^{k_1-1} p_{n-i+1}$, where $\gcd(p_i, p_j) = 1$, $i \neq j$ for $i, j \in \{1, 2, \ldots, n_1\}$.

2. The dealer selects a secret s_1 and a random integer α_1, and computes the secret related value $S_1 = s_1 + \alpha_1 p_0$ such that $\prod_{i=1}^{k_1-1} p_{n-i+1} < S_1 < \prod_{i=1}^{k_1} p_i$.

3. Shares for the participants in $\mathbb{P}_1$ are generated by

$$S_{i,1} \equiv S_1 \bmod p_i$$

for $i \in \{1, 2, \ldots, n_1\}$ and are sent to them secretly. Dealer 1 chooses the u multi-privilege shares from the n_1 shares, assuming $s_{1,1}$, $s_{2,1}$, …, $s_{u,1}$ are chosen, and passes them to Dealer 2.

4. Dealer 2 selects a secure large prime number q_0 and a sequence of pairwise coprime positive integers

$$q_0 < q_1 < q_2 < \cdots < q_{n_2}$$

such that $\prod_{i=1}^{k_2} q_i > q_0 \prod_{i=1}^{k_2-1} q_{n-i+1}$ and $S_{i,1} < q_i$ for $i \in \{1, 2, \ldots, u\}$, where $\gcd(q_i, q_j) = 1$, $i \neq j$ for $i, j \in \{1, 2, \ldots, n_2\}$. Such process will maintain the validity of the multi-privilege shares.

5. Dealer 2 chooses the secret $s_2 \in \mathbb{Z}_{q_0}$. Here, we assume that the u multi-privilege shares are also the first u shares of the (k_2, n_2) SS scheme. The dealer selects a suitable random integer α_2 and computes the secret related value $S_2 = s_2 + \alpha_2 q_0$ such that $\prod_{i=1}^{k_2-1} q_{n-i+1} < S_2 < \prod_{i=1}^{k_2} q_i$. By combining the conditions of the multi-privilege shares, we can determine α_2 by:

$$\begin{cases} s_2 \equiv S_2 \bmod q_0, \\ S_{1,2}(= S_{1,1}) \equiv S_2 \bmod q_1, \\ \cdots, \\ S_{u,2}(= S_{u,1}) \equiv S_2 \bmod q_u. \end{cases} \tag{3.1}$$

The secret related value S_2 is derived by using (2.2) and then α_2 can be derived, which is specified in Remark 1.

6. The shares for the participants in $\mathbb{P}_2$ are generated as

$$S_{i,2} \equiv S_2 \bmod q_i$$

for $i = u + 1, 2, \ldots, n_2$, and are delivered secretly to them.

Reconstruction phase

1. Given any k_1 shares of $\mathbb{P}_1$, such as $S_{i_1,1}$, …, $S_{i_{k_1},1}$, we can find the secret related value S_1 according to the CRT by using (2.2) and compute the secret $s_1 \equiv S_1 \bmod p_0$.
2. Similarly, given any k_2 shares of $\mathbb{P}_2$, for example $S_{i_1,2}$, …, $S_{i_{k_2},2}$, the secret related value S_2 can be computed according to the CRT by using (2.2), and the secret is obtained by $s_2 \equiv S_2 \bmod q_0$.

Remark 1. *Step* 5 *of Scheme* 1 *is important for the CSS construction. It allows each multi-privilege participant to take only one share to participant multiple SS schemes. Here we show how to determine the secret related value* S_2. *A unique integer* $w \in \left(\prod_{i=0}^{u-1} q_{n-i+1}, \prod_{i=0}^{u} q_i \right]$ *can be determined from* (3.1) *according to the CRT by using* (2.2). *We rewrite it in the form* $w = s_2 + yq_0 \in \left(\prod_{i=0}^{u-1} q_{n-i+1}, \prod_{i=0}^{u} q_i \right]$ *and calculate the unique integer* y. *Then we randomly choose* x *such that* $S_2 = w + xq_0q_1 \ldots q_u \in$

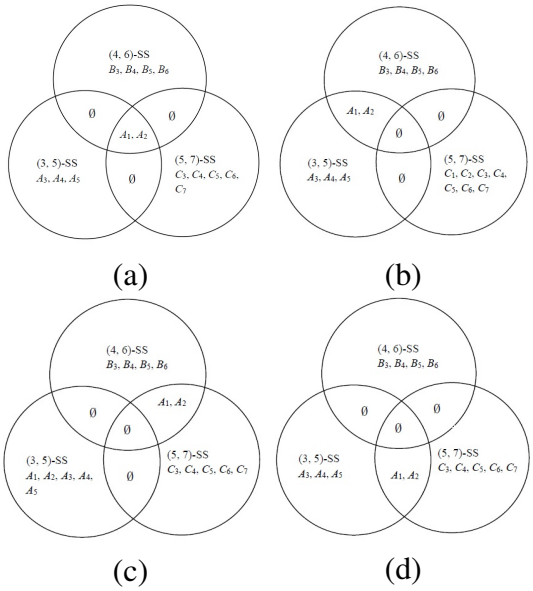

Figure 2. The multi-privilege participants appear.

$\left(\prod_{i=1}^{k_2-1} q_{n-i+1}, \prod_{i=1}^{k_2} q_i\right]$, *this leads to* $\alpha_2 = y + xq_1 \ldots q_u$ *since* $S_2 = s_2 + \alpha_2 q_0$. *Because* y *is uniquely determined and* x *has multiple random candidates by the above conditions,* α_2 *has the same random choices as* x.

In reality, Scheme 1 cannot be used when $u = k_1 = k_2$. In reality, $u = k_1 = k_2$ is not desirable from a security point of view since the u multi-privilege participants are not pure internal participants that they may collude to recover the secret without the authorization of the pure internal participants. It is safer if no more than u participants working together with at least one internal participant should be required to reconstruct the secret, i.e., $u < k_1$ and $u < k_2$.

3.3. Collaboration among multiple SS schemes: a $((k_1, n_1); \ldots; (k_l, n_l))$*-CSS scheme with U*

This subsection discusses cases where three or more threshold schemes collaborate with each other. Each dealer is in charge of one secret and distributes shares to related participants. The participant sets may overlap because the possibility of participants involving in multiple group collaboration is high. Under such circumstance, there may be common participants in any two schemes. The common participants means the multi-privilege participants. We now give an example for the collaboration among three SS schemes.

Example 1. *Consider three schemes, a* $(3, 5)$ *scheme to share* s_1*, a* $(4, 6)$ *scheme to protect* s_2 *and a* $(5, 7)$ *scheme for* s_3. *Their participants are denoted as* $A = \{A_1, A_2, A_3, A_4, A_5\}$, $B = \{B_1, B_2, B_3, B_4, B_5, B_6\}$ *and* $C = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7\}$, *respectively. The common participants may appear in different subsets of intersection of A and B and C. The basic intersections are shown in Figure 1 and depicted as four cases.*

Case 1: *The common participants occur in* $A \bigcap B \bigcap C$. A_1 *and* A_2 *are the common participants involved in all three schemes, i.e.,* $A_1 = B_1 = C_1$, $A_2 = B_2 = C_2$. *It is secure from the point of view*

of s_i, $i = 1, 2, 3$, since none of the other schemes or dealers can reveal the secret of s_i, $i = 1, 2, 3$. A diagram is given in Figure 2.(a).

Case 2: *The common participants occur in $A \bigcap B$. When A_1 and A_2 are in $A \bigcap B$, it is secure in terms of s_1 and s_2 (Figure 2.(b)).*

Case 3: *The common participants occur in $B \bigcap C$. When B_1 and B_2 are in $B \bigcap C$, it is secure in terms of s_2 and s_3 (Figure 2.(c)).*

Case 4: *The common participants occur in $C \bigcap A$. When A_1 and A_2 are in $C \bigcap A$, it is secure in terms of s_1 and s_3 (Figure 2.(d)).*

In fact, the common participants may occur in any combination of the above four cases. In different intersection cases, we need to consider different share intersections. This inspires us to propose a new method to define the participant set that the intersections can be seen clearly. For collaboration among l SS schemes, we define the participant set for each (k_i, n_i) scheme as $\mathbb{P}_i = \{p_1^i, \ldots, p_{n_i}^i\}$, and its access structure is $\Gamma_i = \{U \subseteq \mathbb{P}_i, |U| \geq k_i\}$ for $i \in \{1, 2, \ldots, l\}$. The shares are generated in order without repetition. We define the intersection in the following manner.

For the first scheme, (k_1, n_1)-SS scheme, the participants in $\mathbb{P}_1$ are defined as

$$\mathbb{P}_1 = \left\{P_1^1, \ldots, P_{n_1}^1\right\}. \tag{3.2}$$

Then, we define the second participant set $\mathbb{P}_2$. If it has common participants with the first participant set, their intersection is defined as $\mathrm{U}_{2,1} = \mathbb{P}_1 \bigcap \mathbb{P}_2 = \{P_1^{2,1}, \ldots, P_{u_{2,1}}^{2,1}\}$ with $|\mathrm{U}_{2,1}| = u_{2,1}$. Then, the second participants set is expressed as

$$\mathbb{P}_2 = \left\{P_1^{2,1}, \ldots, P_{u_{2,1}}^{2,1}, P_{u_{2,1}+1}^{2}, \ldots, P_{n_2}^{2}\right\}. \tag{3.3}$$

For the third participant set $\mathbb{P}_3$, if they have common participants with the first and the second participant sets, we denote them as $\mathrm{U}_{3,1} = \mathbb{P}_3 \bigcap \mathbb{P}_1 = \{P_1^{3,1}, \ldots, P_{u_{3,1}}^{3,1}\}$ with $|\mathrm{U}_{3,1}| = u_{3,1}$, and $\mathrm{U}_{3,2} = (\mathbb{P}_3 \bigcap \mathbb{P}_2) \setminus \mathrm{U}_{3,1} = \{P_1^{3,2}, \ldots, P_{u_{3,2}}^{3,2}\}$ with $|\mathrm{U}_{3,2}| = u_{3,2}$, meeting the requirement that $\mathrm{U}_{3,1} \bigcap \mathrm{U}_{3,2} = \varnothing$. Then, the third participant set can be defined as

$$\mathbb{P}_3 = \left\{P_1^{3,1}, \ldots, P_{u_{3,1}}^{3,1}, P_{u_{3,1}+1}^{3,2}, \ldots, P_{u_{3,1}+u_{3,2}}^{3,2}, P_{u_{3,1}+u_{3,2}+1}^{3}, \ldots, P_{n_3}^{3}\right\}. \tag{3.4}$$

The i-th participant set $\mathbb{P}_i$ is assumed to have $\mathrm{U}_{i,1} = \mathbb{P}_i \bigcap \mathbb{P}_1 = \{P_1^{i,1}, \ldots, P_{u_{i,1}}^{i,1}\}$ with $|\mathrm{U}_{i,1}| = u_{i,1}$, $\mathrm{U}_{i,2} = (\mathbb{P}_i \bigcap \mathbb{P}_2) \setminus \mathrm{U}_{i,1} = \{P_1^{i,2}, \ldots, P_{u_{i,2}}^{i,2}\}$ with $|\mathrm{U}_{i,2}| = u_{i,2}$ and $\mathrm{U}_{i,j} = (\mathbb{P}_i \bigcap \mathbb{P}_j) \setminus \left(\bigcup_{s=1}^{j-1} \mathrm{U}_{i,s}\right) = \{P_1^{i,j}, \ldots, P_{u_{i,j}}^{i,j}\}$ with $|\mathrm{U}_{i,j}| = u_{i,j}$ for $j \in \{3, \ldots, i-1\}$, meeting the requirement that $\mathrm{U}_{i,j} \bigcap \mathrm{U}_{i,k} = \varnothing$ for $j \neq k$ and $j, k \in \{3, \ldots, i-1\}$. Therefore,

$$\mathbb{P}_i = \left\{P_1^{i,1}, \ldots, P_{u_{i,1}}^{i,1}, P_{u_{i,1}+1}^{i,2}, \ldots, P_{u_{i,1}+u_{i,2}}^{i,2}, \ldots, P_{u_{i,1}+u_{i,2}+\cdots+u_{i,i-2}+1}^{i,i-1}, \ldots, P_{u_{i,1}+u_{i,2}+\cdots+u_{i,i-1}}^{i,i-1}, P_{u_{i,1}+u_{i,2}+\cdots+u_{i,i-1}+1}^{i}, \ldots, P_{n_3}^{i}\right\}.$$

The remaining $n-3$ participant sets are defined in the same manner as participant set $\mathbb{P}_i$. Let $\mathrm{U} = \bigcup_{i=1}^{l} \bigcup_{j=1}^{i-1} \mathrm{U}_{i,j}$. To maintain the security of each secret, the number of multi-privilege participants for

each (k_i, n_i) SS scheme in $\mathbb{P}_i$ should be less than k_i. Therefore,

$$\left|\left(\bigcup_{\substack{j=1,\\ j\neq i}}^{l}\mathbb{P}_j\right)\bigcap\mathbb{P}_i\right| < k_i \tag{3.5}$$

holds, so the leakage of secret information through the collusion of the multi-privilege participants can be precluded.

With the above notations, we now give a formal definition of the $((k_1, n_1); \ldots; (k_l, n_l))$-CSS scheme with U.

Definition 3 A l tuples of the (k_i, n_i) SS scheme with participant set $\mathbb{P}_i$ sharing a secret s_i, $i = 1, 2, \ldots, l$ with intersection U constitute a $((k_1, n_1); \ldots; (k_l, n_l))$-CSS scheme with U depicted as above if the following two conditions hold:

1. for all $A \subseteq \mathbb{P}_i$ and $|A| \geq k_i$, $H(s_i|A) = 0$ for $i = 1, \ldots, l$;
2. for all $A \subseteq \bigcup_{i=1}^{l}\mathbb{P}_i$ and $\left|A\bigcap(\bigcup_{j=1}^{l}\mathbb{P}_i)\right| < k_i$, $0 < H(s_i|S_A) \leq H(s_i)$ for $i = 1, \ldots, l$.

The first condition ensures that each secret can be revealed correctly by its authorized subsets. The second condition prevents the unauthorized subsets from collusively revealing the secret. When the "=" relation holds in the second condition, the $((k_1, n_1); \ldots; (k_l, n_l))$-CSS scheme has a perfect security. It is called asymptotically perfect if for all $\epsilon > 0$, there exists $x_0 \geq 0$ such that for all $A \subseteq \bigcup_{i=1}^{l}\mathbb{P}_i$ with $x \geq x_0$, we have that $\triangle H = |H(s_i) - H(s_i|S_A)| \leq \epsilon$ holds for all $\left|A\bigcap(\bigcup_{j=1}^{l}\mathbb{P}_i)\right| < k_i$ where $i = 1, \ldots, l$. We now present the construction scheme of a $((k_1, n_1); \ldots; (k_l, n_l))$-CSS with U.

Scheme 2 The proposed $((k_1, n_1); \ldots; (k_l, n_l))$-CSS with U

Distribution phase

1. Dealer 1 chooses a large prime number $p_{0,1}$ and a sequences of pairwise coprime positive integers,

$$p_{0,1} < p_{1,1} < p_{2,1} < \cdots < p_{n_1,1},$$

satisfying $\prod_{i=1}^{k_1} p_{i,1} > p_{0,1}\prod_{i=1}^{k_1-1} p_{n_1-i+1,1}$, $\gcd(p_{j,1}, p_{k,1}) = 1$, $j \neq k$ for $j, k \in \{1, 2, \ldots, n_1\}$. Dealer 1 selects a secret $s_1 \in \mathbb{Z}_{p_{0,1}}$ and a random integer α_1, and computes the secret related value $S_1 = s_1 + \alpha_1 p_{0,1}$ such that $S_1 \in (\phi^1_{k_1-1}, \phi^1_{k_1}]$. Here, we set $\prod_{j=1}^{k_i} p_{j,i} = \phi^i_{k_i}$ and $\prod_{j=1}^{k_i-1} p_{n_i-j+1,i} = \phi^i_{k_i-1}$ for $1 \leq i \leq l$. Shares for the participants in $\mathbb{P}_1$ are generated as

$$S_{j,1} \equiv s_1 + \alpha_1 p_{0,1} \bmod p_{j,1},$$

where $j \in \{1, 2, \ldots, n_1\}$. Dealer 1 picks the $u_{i,1}$ multi-privilege shares $\{S^{i,1}_1, \ldots, S^{i,1}_{u_{i,1}}\}$ and passes them to Dealer i.

2. Dealer 2 receives the $u_{2,1}$ multi-privilege shares $\{S^{2,1}_1, \ldots, S^{2,1}_{u_{2,1}}\}$ from $U_{2,1}$. Then, he/she chooses a large prime number $p_{0,2}$ and a sequence of pairwise coprime positive integers,

$$p_{0,2} < p_{1,2} < p_{2,2} < \cdots < p_{n_2,2},$$

satisfying $\prod_{i=1}^{k_2} p_{i,2} > p_{0,2} \prod_{i=1}^{k_2-1} p_{n_2-i+1}$ and $S_j^{2,1} < p_{j,2}$ for $1 \le j \le u_{2,1}$, where $\gcd(p_{j,2}, p_{k,2}) = 1$, $j \ne k$ for $j, k \in \{1, 2, \ldots, n_2\}$.

Dealer 2 selects a secret $s_2 \in \mathbb{Z}_{p_{0,2}}$ and a random integer α_2 and computes the secret related value $S_2 = s_2 + \alpha_2 p_{0,2}$ satisfying the condition $S_2 \in (\phi_{k_2-1}^2, \phi_{k_2}^2]$ and the following congruent equations:

$$\begin{cases} s_2 \equiv S_2 \bmod p_{0,2}, \\ S_{1,2} (= S_1^{2,1}) \equiv S_2 \bmod p_{1,2}, \\ \cdots, \\ S_{u_{2,1},2} (= S_{u_{2,1}}^{2,1}) \equiv S_2 \bmod p_{u_{2,1},2}. \end{cases} \tag{3.6}$$

Here, we assume that the multi-privilege participants in $\mathrm{U}_{2,1}$ are the first $u_{2,1}$ participants in $\mathbb{P}_2$. The integer α_2 can be determined according to Remark 1. The remaining $n_2 - u_{2,1}$ shares $S_{j,2}$ can be determined by using

$$S_{i,2} = S_2 \bmod p_{i,2}.$$

Dealer 2 distributes shares $S_{1,2}, S_{2,2}, \ldots, S_{n_2,2}$ to participants in $\mathbb{P}_2$ privately. Dealer 2 also sends multi-privilege shares $\{S_1^{i,2}, S_2^{i,2}, \ldots, S_{u_{i,2}}^{i,2}\}$ to Dealer i for $i \in \{3, \ldots, l\}$.

3. Dealer i receives shares $\{S_1^{i,j}, S_2^{i,j}, \ldots, S_{u_{i,j}}^{i,j}\}$ from dealer j, $j \in \{1, \ldots, i-1\}$, $i \in \{3, 4, \ldots, l\}$. Then, he/she chooses a large prime number $p_{0,i}$ and a sequence of pairwise coprime positive integers,

$$p_{0,i} < p_{1,i} < p_{2,i} < \cdots < p_{n_i,i},$$

satisfying $\prod_{j=1}^{k_i} p_{j,i} > p_{0,i} \prod_{j=1}^{k_i-1} p_{n_i-j+1}$ and with $S_k^{i,j} < p_{k,i}$ for $1 \le k \le u_{i,j}$, where $\gcd(p_{j,i}, p_{k,i}) = 1$, $j \ne k$ for $j, k \in \{1, 2, \ldots, n_i\}$. Dealer i selects a secret $s_i \in \mathbb{Z}_{p_{0,i}}$ and a random integer α_i, and computes the secret related value $S_i = s_i + \alpha_i p_{0,i}$ satisfying $S_i \in (\phi_{k_i-1}^i, \phi_{k_i}^i]$ and the following congruent equations:

$$\begin{cases} s_i = S_i \bmod p_{0,i}, \\ \left.\begin{array}{l} S_{i,1} (= S_1^{i,1}) \equiv S_i \bmod p_{1,i}, \\ \cdots, \\ S_{i,u_{i,1}} (= S_{u_{i,1}}^{i,1}) \equiv S_i \bmod p_{u_{i,1},i}, \end{array}\right\} \to \mathrm{U}_{i,1}, \\ \left.\begin{array}{l} S_{i,u_{i,1}+1} (= S_1^{i,2}) \equiv S_i \bmod p_{u_{i,1}+1,i}, \\ \cdots, \\ S_{i,u_{i,1}+u_{i,2}} (= S_{u_{i,2}}^{i,2}) \equiv S_i \bmod p_{u_{i,1}+u_{i,2},i}, \end{array}\right\} \to \mathrm{U}_{i,2}, \\ \left.\begin{array}{l} S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j-1}+1,i} (= S_1^{j,i}) \equiv S_i \\ \quad \bmod p_{u_{i,1}+u_{i,2}+\cdots+u_{i,j-1}+1,i}, \\ \cdots, \\ S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j},i} (= S_{u_{i,j}}^{i,j}) \equiv S_i \\ \quad \bmod p_{u_{i,1}+u_{i,2}+\cdots+u_{i,j},i}, \end{array}\right\} \to \mathrm{U}_{i,j}, \ 3 \le j \le i-1. \end{cases} \tag{3.7}$$

Here, we assume that the common participants in $\mathrm{U}_{i,j}$ appear in $\mathbb{P}_i$ in increasing order of i, j. The integer α_i can be determined according to Remark 2 below. Then, Dealer i computes the shares

for the remaining participants in set $\mathbb{P}_i$ by

$$S_{j,i} \equiv S_i \bmod p_{j,i},$$

for $u_i + 1 \le j \le n_i$. Let $u_i = u_{i,1} + u_{i,2} + \cdots + u_{i,i-1}$. Dealer i sends shares $S_{j,i}$ to participants in $\mathbb{P}_i$ and the multi-privilege shares $\{S_1^{j,i}, S_2^{j,i}, \ldots, S_{u_{j,i}}^{j,i}\}$ to Dealer j for $j = i+1, \ldots, l$.

Reconstruction phase

Given any k_i shares of $\mathbb{P}_i$, such as $S_{j_1,i}, \ldots, S_{j_{k_i},i}$, we can find the secret related value S_i according to the CRT by using (2.2) and compute the secret $s_i \equiv S_i \bmod p_{0,i}$, $i \in \{1, 2, \ldots, l\}$.

Remark 2. *Step 3 in Scheme 2 is the key point to construct the CSS scheme. It allows each multi-privilege participant to take one share to manage multiple secrets. The secret can be randomly chosen by each dealer. Here we show how to determine the secret related value S_i. The unique integer w_i can be evaluated from* (3.7) *according to the CRT by using* (2.2)*. Then, we can determine $\alpha_i = y_i + x_i p_{1,i} \ldots p_{u,i}$ according to*

$$\begin{aligned} S_i &= w_i + x_i p_{0,i} p_{1,i} \ldots p_{u_i,i} \in \left(\prod_{j=1}^{k_i - 1} p_{n-j+1,i}, \prod_{j=1}^{k_i} p_{j,i} \right], \\ w_i &= s_i + y_i p_{0,i} \in \left(\prod_{j=0}^{u_i - 1} p_{n-j+1,i}, \prod_{j=0}^{u_i} p_{j,i} \right]. \end{aligned}$$

Because y_i and w_i are uniquely determined from (3.7)*, and x has multiple random candidates under the above condition, the variable α_i has the same random choices as the variable x_i.*

4. Performance analysis

In this section, we analyse the performance of the proposed scheme in terms of security and correctness. The performance comparison with previous collaborative schemes is shown. The experiments demonstrate the construction process of CSS proposed scheme and verify the two characteristics.

4.1. Security and correctness

It is clear that the security of the proposed scheme is the same as that of the scheme in [18] because each single scheme in the CSS scheme satisfies the security condition (2.3). The shares of multi-privilege participants who are involved in multiple secrets have more tendency to be attacked. The regular participants have the same role and security as that they have in a single SS scheme. Therefore, we consider three possible attacks with respect to multi-privilege participants and illustrate them in the following.

- The multi-privilege participants cannot recover any secret independently because of (3.5).
- The multi-privilege participants' unity with the participants in Γ_i cannot recover the corresponding secret s_i if their number is less than its threshold k_i.
- The multi-privilege participants' unity with the participants in $\mathbb{P}_i$ cannot recover the secret $s_j (j \neq i)$ if their number is less than the related threshold. Furthermore, even if their number is not less than the related threshold, no knowledge about s_j will be leaked, because $|(\mathrm{U} \bigcup \mathbb{P}_i) \bigcap \mathbb{P}_j)| \le k_j - 1$.

It is easy to verify that the three styles of attack will not succeed in obtaining any useful knowledge because they all satisfy condition (3.5). The multi-privilege participants are unlikely to obtain secret information. The proposed CSS scheme is secure against $k-1$ colluding participants.

The key point of the construction of CSS scheme is that each secret is still chosen randomly by its dealer and is not affected by the generated multi-privilege shares. Conditions (3.1) and (3.7) can guarantee that the secret s can be chosen randomly and the secret related value S can be calculated to satisfy the security requirement of CSS. The reasons are illustrated in the Remark 1 and Remark 2. When the threshold of any single scheme is reached, the secret can be evaluated by solving congruent equations using the CRT. The correctness of the proposed scheme is clear. The correctness and security proofs are presented in Theorem 2.

Theorem 2. *The proposed CSS scheme based on the CRT is a asymptotically perfect* $((k_1, n_1); \ldots; (k_l, n_l))$*-CSS scheme with U.*

Proof. We need to prove its correctness and asymptotically perfect security.

Before we prove the asymptotically perfect security, the proposed scheme needs to be validated. We show that for all $A \subseteq \mathbb{P}_i$ and $|A| \geq k_i$, where $i \in \{1, 2, \ldots, l\}$, the secret can be recovered correctly from the shares in A. Assuming that $A = \{i_1, i_2, \cdots, i_{|A|}\}$, we collect their shares $S_{i_1,i}, S_{i_2,i}, \cdots, S_{i_{|A|},i}$ and have the following equations of congruence:

$$\begin{cases} S_i \equiv S_{i_1,i} \bmod p_{i_1,i}, \\ S_i \equiv S_{i_2,i} \bmod p_{i_2,i}, \\ \cdots, \\ S_i \equiv S_{i_{|A|},i} \bmod p_{i_{|A|},i}. \end{cases} \tag{4.1}$$

The moduli of the above congruent equations satisfy $\prod_{\substack{j\in A,\\ |A|\geq t_i}} p_{j,i} \geq \phi^i_{k_i}$. Because we know the secret related value $S_i \in (\phi^i_{k_i-1}, \phi^i_{k_i}]$, it can be uniquely determined from the above equations of congruence by using the CRT. Then, we compute $s_i = S_i \bmod p_0$ to obtain the secret s_i.

We prove its the asymptotically perfect security in the following. We show the security for the proposed scheme. The first two types of attack satisfy the condition of (3.5) and belong to the unauthorized subset of S_i. No useful information will be leaked. The third type attack fulfills the condition $|(\mathrm{U} \bigcup \mathbb{P}_i) \bigcap \mathbb{P}_j| < k_j$ and belongs to the unauthorized subset of S_j. Now we prove that the entropy loss of the secret derived from the the unauthorized share subset of S_j is negligible for $j \in \{1, 2, \ldots, l\}$.

Firstly, we derive the candidates of the secret related value by the shares of the unauthorized subset of S_j. Let $A \subseteq \mathbb{P}_j$ be the unauthorized subset of S_j. Its shares $S_{i_r,j}$, $i_r \in A$ with $|A| < t_j$, for the threshold t_j are collected and constitute the following congruent equations:

$$\begin{cases} S_j \equiv S_{i_1,j} \bmod p_{i_1,j}, \\ S_j \equiv S_{i_2,j} \bmod p_{i_2,j}, \\ \cdots, \\ S_j \equiv S_{i_{|A|},j} \bmod p_{i_{|A|},j}. \end{cases} \tag{4.2}$$

There is a unique solution $X \in (0, \prod_{i\in A} p_{i,j})$ for (4.2) according to Theorem 1. The candidates of the secret related value are $S_j = X + y \cdot \prod_{i\in A} p_{i,j}$ according to the CRT, where $y \in \{1, \ldots, C(A)\}$ with

$C(A) \triangleq \Big\lfloor \prod_{1\le i\le t_j} p_{i,j} / \prod_{i\in A} p_{i,j} \Big\rfloor$. Since $S_j \in \left(\phi^j_{k_j-1}, \phi^j_{k_j}\right]$ and $p_{0,j}\phi^j_{k_j-1} < \phi^j_{k_j}$, we can derive that

$$C(A) > p_{0,j} - 1, \tag{4.3}$$

from $\prod_{i\in A} p_{i,j} \le \phi^j_{k_j-1}$.

Secondly, we compute the conditional entropy of the secret by the known shares S_A from the unauthorized subset of S_j. The secret candidates can be derived by $s = S_j (\mathrm{mod}\, p_{0,j})$. The number of secret candidates is not reduced according to (4.3). Let $C(A) = p_{0,j}N + r$ with $0 \le r < p_{0,j}$. The $C(A)$ candidates of secret related value S_j are mapped to $p_{0,j}$ secret candidates. The secret candidates which will appear $N+1$ times and N times are denoted by $s^1 = \{s^j_1, s^j_2, \ldots, s^j_r\}$ and $s^0 = \{s_{r+1}, s_{r+2}, \ldots, s_{p_{0,j}}\}$, respectively. The two sets satisfy both $s^0 \bigcap s^1 = \emptyset$ and $s^0 \bigcap s^1 = \mathbb{Z}_{p_{0,j}}$. Given shares S_A, we compute the conditional entropy of the secret,

$$H(s|S_A) = -\sum_{i=1}^{r} p_i \log p_i - \sum_{i=r+1}^{p_{0,j}} p_i \log p_i = -r\frac{N+1}{C(A)} \log \frac{N+1}{C(A)} - (p_{0,j} - r)\frac{N}{C(A)} \log \frac{N}{C(A)}.$$

$H(s|S_A)$ can be lower bounded as

$$H(s|S_A) > r\frac{N+1}{C(A)} \log \frac{C(A)}{N+1} + (p_{0,j} - r)\frac{N}{C(A)} \log \frac{C(A)}{N+1} = \log \frac{N+1}{C(A)},$$

and upper bounded as

$$H(s|S_A) < -r\frac{N+1}{C(A)} \log \frac{N}{C(A)} - (p_{0,j} - r)\frac{N}{C(A)} \log \frac{N}{C(A)} = \log \frac{C(A)}{N}.$$

We obtain that $\log \frac{C(A)}{N+1} < H(s|S_A) < \log \frac{C(A)}{N}$.

Thirdly, we compute the loss of entropy of the secret $\triangle H$. The entropy of the secret satisfies $H(s) = \log p_{0,j}$ since $s \in_R \mathbb{Z}_{p_{0,j}}$.

$$\triangle H = |H(s) - H(s|S_A)| = \left| \log(1 \pm \frac{r}{C(A)}) \right| < \log \frac{p_{0,j}}{C(A)}. \tag{4.4}$$

By hypothesis, the prime $p_{i,j}$s are consecutive for $1 \le i \le n_j$. It follows that $p_{i+1,j} < p_i + p_i^{\frac{1}{2}+\frac{1}{21}}$ for p_i sufficiently large (See [32], p. 193). Because the primes $p_{i,j}$'s are consecutive, it holds that, for all sufficiently large $p_{0,j}$

$$C(A) + 1 \ge p^t_{0,j} \Big/ \Big(p^{t-1}_{0,j} + \sum_i a_i p_0^{b_i}\Big),$$

where $a_i \in \mathbb{R}^+$ and $0 < b_i < t-1$, for all i. For all sufficiently large prime $p_{0,j}$, it holds

$$\frac{p_{0,j}}{C(A)} \le p_{0,j}\Big(p^{t-1}_{0,j} + \sum_i a_i p_0^{b_i}\Big) \Big/ \Big(p^t_{0,j} - p^{t-1}_{0,j} - \sum_i a_i p_0^{b_i}\Big).$$

Applying the logarithm operator and using (4.4), we get

$$\triangle H = |H(s) - H(s|S_A)| \le \log p_{0,j}\Big(p^{t-1}_{0,j} + \sum_i a_i p_0^{b_i}\Big) \Big/ \Big(p^t_{0,j} - p^{t-1}_{0,j} - \sum_i a_i p_0^{b_i}\Big).$$

The upper bound converges to 0 when $p_{0,j}$ converges to infinity. Thus, the asymptotically perfect security is proved. □

Table 1. The performance comparison with other CSS schemes.

Scheme	Share size	Security	Computation complexity	Recovery quality
CSS([16])	$H(S)$	perfect	$O(k\log^2 k)$	exact
CVS([11])	$mH(S)$	perfect	0(visual)	lower
ours	$H(S)$	perfect	$O(k)$	exact

Remark. $m(>1)$ is the pixel expansion which is determined by the detailed scheme.

4.2. Comparison with related schemes

The efficiency of the proposed scheme is compared with that of the previous CSS scheme in terms of share size, broadcast message size, security, recovery complexity and recovery quality in Table 1. From Table 1, we can see that scheme [16] requires high recovery complexity with the exact reconstructed secret. The scheme in [11] has zero computational complexity in the recovery phase, but it decreases the visual effect of the secret and expands the share size. The proposed CSS scheme can reconstruct the secret exactly with lower recovery complexity. Furthermore, it can process complex participant intersections. It provides broad applications for group collaborations.

The proposed CSS scheme is different from the multi-secret sharing scheme [33, 34]. But it can be used to construct such schemes when $u = 0$ or $u_{i,j} = 0$. Under such application, it has the same structure with the multi-secret sharing scheme which allows a single secret to be shared per threshold value [33, 34]. But such multi-secret sharing schemes cannot be used to construct the proposed CSS scheme. The CSS scheme has special collaborative properties that general multi-secret sharing schemes don't have.

4.3. Experimental results

To demonstrate the construction strategy of the collaborative schemes, two numerical examples are used to illustrate our proposed scheme. A $((3,5);(4,6))$-CSS with its U is shown in Example 2 by combining step 1 and step 2. A $((3,5);(4,6);(5,7))$-CSS with its U is obtained by combining step 1, step 2 and step 3. The experimental results also demonstrate the correctness and security of the proposed CSS scheme.

Example 2. *Suppose there are three secrets (s_1, s_2 and s_3) that can be protected by three dealers with three traditional threshold schemes as a $(3,5)$ scheme, a $(4,6)$ scheme and a $(5,7)$ scheme, respectively. The participant intersections are shown in Figure 3. Five participants with the first secret form the group $\mathbb{P}_1 = \{A_1, A_2, A_3, A_4, A_5\}$, and six participants with the second secret form the group $\mathbb{P}_2 = \{B_1(A_1), B_2(A_2), B_3, B_4, B_5, B_6\}$, and seven participants with the third secret form the group $\mathbb{P}_3 = \{C_1(A_2), C_2(B_3), C_3, C_4, C_5, C_6, C_7\}$. The share generation process is conducted in three steps as follows. The main parameters are shown in Table 2. The multi-privilege shares are labelled with the asterisks.*

Step 1: Share construction for a $(3,5)$ scheme.

The secret $s_1 = 112$ and $p_{0,1} = 113$, and the pairwise coprime numbers and shares are shown in Table 2. Because $\mathbb{Z}(\Phi^1_{k_1-1}, \Phi^1_{k_1}] = \mathbb{Z}(51983, 9363547]$, we have $\alpha_1 \in [461, 82863]$ such that $S_1 = s_1 + \alpha_1 p_{0,1} \in \mathbb{Z}(\Phi^1_{k_1-1}, \Phi^1_{k_1}]$. We take $\alpha_1 = 1000$, $S_1 = 113112$. Shares for the participants

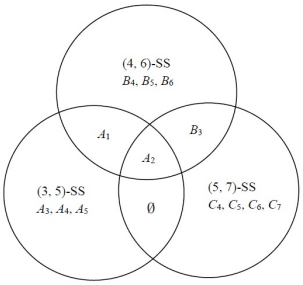

Figure 3. The participant intersections occur in a $((3,5);(4,6);(5,7))$-CSS scheme.

Table 2. The moduli and shares for a $((3,5);(4,6);(5,7))$-CSS scheme with U.

Scheme	i	$p_{0,i}$	s_i	$(p_{i,1}, S_{i,1})$	$(p_{i,2}, S_{i,2})$	$(p_{i,3}, S_{i,2})$	$(p_{i,4}, S_{i,4})$	$(p_{i,5}, S_{i,5})$	$(p_{i,6}, S_{i,6})$	$(p_{i,7}, S_{i,7})$
(3,5)	1	113	112	(119,80*)	(211,16**)	(223,51)	(227, 66)	(229,115)	−−	−−
(4,6)	2	151	150	(263,80*)	(269,16**)	(271,260***)	(277,249)	(281,46)	(283,72)	−−
(5,7)	3	191	178	(397,16**)	(401,260***)	(409,155)	(419,215)	(421,120)	(431,363)	(433,313)

Remark. 80^* denotes the multi-privilege share for for $A_1(B_1)$; 16^{**} denotes the multi-privilege for $A_2(B_2,\ C_1)$; 260^{***} denotes the multi-privilege for $B_3(C_2)$.

in $\mathbb{P}_1$ can be computed by $S_{j,1} \equiv 113112 \bmod p_{j,1}$. The multi-privilege participant sets are $\mathrm{U}_{2,1} = \{p_{1,1}, p_{2,1}\}$, $\mathrm{U}_{3,1} = \{p_{2,1}\}$. Share 80 for participant $A_1(B_1)$ and share 16 for participant $A_2(B_2, C_1)$ are picked and handed over to Dealer 2. Share 16 for participant $A_2(C_1)$ is handed over to Dealer 3.

Step 2: Share construction for the $(4,6)$ scheme.

Dealer 2 chooses a secret $s_2 = 150$, $p_{0,2} = 151$, and a sequences of pairwise coprime positive integers shown in Table 2. Dealer 2 already has two shares: 80 and 16 and the secret 150. By using (3.1) and Remark 2, the unique solution $w_2 = 9317907 \in (39713, 10682797]$ is obtained. We can take a random variable x_2 such that $S_2 = w + x_2 p_{0,2} p_{1,2} p_{2,2} \in \mathbb{Z}(\Phi^2_{k_2-1}, \Phi^2_{k_2}] = \mathbb{Z}(22027871, 5310765049]$. Assuming $x_2 = 300$, then $S_2 = 9317907 + 300 \cdot 10682797 = 3214157007 \in \mathbb{Z}(\Phi^2_{k_2-1}, \Phi^2_{k_2}]$. Thus, $\alpha_2 = 21285807$. The remaining shares can be generated as $s_{j,2} = S_2 \bmod p_{j,2}$ for $3 \le j \le 6$. The generated shares are shown in Table 2.

Step 3: Share construction for the $(5,7)$ scheme.

Dealer 3 already receives shares $S_1^{3,1} = 16$ for C_1 and $S_1^{3,2} = 260$ for C_2. He or she chooses randomly $s_3 = 178$, $p_{0,3} = 191$ and the sequences of pairwise coprime positive integers to constructs a (5, 7) threshold scheme shown in Table 2. The shares (191, 178), (397, 16), and (401, 260) are used to generate the secret related value S_3. By using formula (3.7) and Remark 2, the unique solution $w_3 = 7298861 \in (75827, 30406627]$ is obtained. Since $S_3 = w_3 + x_3 \prod_{j=0}^{2} p_{j,3} \in \mathbb{Z}(\Phi^3_{k_3-1}, \Phi^3_{k_3}] = \mathbb{Z}(32920110577, 11485616365627]$, it is derived that $x_3 \in \mathbb{Z}(1082, 377733]$. We choose $x_3 = 99999$ and obtain $S_3 = 7298861 + 99999 \cdot 30406627 = 3040639592234 \in \mathbb{Z}(\Phi^3_{k_3-1}, \Phi^3_{k_3}]$. The remaining shares can be generated using $S_{j,3} = S_3 \bmod p_{j,3}$ for $3 \le j \le 7$.

The ((3,5); (4,6))-CSS scheme with its U can be verified correct. When any three participants of the first (3,5) scheme present their shares, for example, (211,16), (223,51), and (227,66), then the first secret is obtained as

$$\begin{aligned} S_1 &\equiv 16 \times 50621 \times 111 + 51 \times 47897 \times 144 + 66 \times 47053 \times 188 \bmod 211223227 = 113112, \\ s_1 &\equiv 113112 \bmod 113 = 112. \end{aligned}$$

The correctness and security for the ((3,5);(4,6);(5,7))-CSS with its U can be verified in the same manner. It is clear that the collaborative scheme can reveal each secret correctly when the participant sets are in the corresponding qualified subsets family. The participant set which includes all multi-privilege participants belongs to the unqualified subsets family of any secret and cannot obtain any information about that secret. The multi-privilege shares uniting the participants in $\mathbb{P}_i$ cannot obtain any secret information about s_j when $i \neq j$. The conclusions can be verified by using the data in Example 2. The CSS scheme has the same asymptotically perfect security as that of the Asmuth-Bloom scheme.

5. Conclusion

In this paper, we proposed a collaborative SS scheme which provides a secure and efficient strategy to ease the share management in group collaborative environment. Each participant just needs to keep only one share to participate in multiple key management systems. It can solve the contradiction between privacy protection and collaborative sharing of confidential data. It can be used for secure data management across systems or joint computing platforms. Its efficiency and convenience in operation are attractive in distributed networks. The comparative study of the proposed scheme with the state of the art approaches validates its efficiency.

The collaborative scheme raises a number of related open problems, such as security concerns involving dishonest multi-privilege participants, dishonest dealers in different schemes, and the situation where other dealers become participants of a scheme. Various combinations of risks exist in this "open" environment. For example, some dishonest multi-privilege participants could work with other illegal participants or dealers to steal secrets. Tracing traitors could become more difficult than in the traditional single scheme situation.

Acknowledgement

This work was supported the National Natural Science Foundation Nos. U1636219, 61872289, and 41807150, in part by Plan for Scientific Innovation Talent of Henan Province No. 2018JR0018 and the Science Foundation of Guangxi Nos. AA17204096 and AD16380076, in part by China Mobile Research Fund Project No. MCM20170407, and Key Laboratory of Digital Content Anti-Counterfeiting and Security Forensics of the state Administration of Press, Publication, Radio, Film and Television of the People's Republic of China.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. Y. Liu, Y. Wang, X. Wang, Z. Xia and J. Xu, Privacy-preserving raw data collection without a trusted authority for IoT, *Comput. Netw.*, **1** (2018), 1–1.
2. Y. Liu, W. Guo, C. Fan, L. Chang and C. Cheng, A practical privacy-preserving data aggregation (3PDA) Scheme for Smart Grid, *IEEE T. Ind. Inform.*, **1** (2018), 1–1.
3. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613.
4. G. R. Blakley, Safeguarding cryptographic keys, in *Proceedings of the 1979 AFIPS National Computer Conference*, AFIPS Press, (1979), 313–317.
5. C. N. Yang, L. Z. Sun, X. Yan, and C. Kim, Design a new visual cryptography for human-verifiable authentication in accessing a database, *J. Real-Time Image Process.*, **12** (2016), 483–494.
6. L. Harn, Group authentication, *IEEE Trans. Comput.*, **62** (2013), 1893–1898.
7. L. Harn and C. Lin, Authenticated group key transfer protocol based on secret sharing, *IEEE Trans. Comput.*, **59** (2010), 842–846.
8. S. Wüller, D. Mayer, F. Förg, S. Schüppen, B. Assadsolimani, U. Meyer and S. Wetzel, Designing privacy-preserving interval operations based on homomorphic encryption and secret sharing techniques, *J. Comput. Secur.*, **25** (2017), 1–23.
9. D. Agrawal, A. E. Abbadi, F. Emekci, A. Metwally and S. Wang, Secure data management service on cloud computing infrastructures, *Springer Berlin Heidelberg*, (2011), 57–80.
10. Y. Wang, Privacy-preserving data storage in cloud using array BP-XOR codes, *IEEE T. Cloud Comput.* , **3** (2015), 425–435.
11. X. Jia, D. Wang, D. Nie and C. Zhang, Collaborative visual cryptographic schemes, *IEEE Trans. Circuits Syst. Video Technol.*, **28** (2018), 1056–1070.
12. M. Nojoumian, D. R. Stinson and M. Grainger, Unconditionally secure social secret sharing scheme, *IET Inf. Secur.*, **4** (2010), 202–211.
13. S. Song and K. Hwang and R. Zhou and Y. K. Kwok, Trusted P2P transactions with fuzzy reputation aggregation, *IEEE Internet Comput.*, **9** (2005), 24–34.
14. J. S. Lin, Cloud data storage with group collaboration supports, in *International Conference on Networked Digital Technologies*, Springer Berlin Heidelberg, (2011), 423–431.
15. F. Mármol and G. M. Pérez, TRIP, A trust and reputation infrastructure-based proposal for vehicular ad hoc networks, *J. Netw. Comput. Appl.*, **35** (2012), 934–941.
16. D. Wang, Z. Ye and X. Li, How to collaborate between threshold schemes, preprint, (2013), `arXiv:1305.1146`.
17. M. Mignotte, How to share a secret, in *Proceedings of the Workshop on Cryptography Burg Feuerstein*, Springer Berlin Heidelberg, (1983), 371–375.
18. C. Asmuth and J. Bloom, A modular approach to key safeguarding, *IEEE Trans. Inf. Theory*, **29** (1983), 208–210.
19. C. C. Drăgan and F. L. Tiplea, On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme, *Inf. Sci.*, **463-464** (2018), 75–85.

20. B. Preneel and J. Vandewalle, On the security of the threshold scheme based on the Chinese Remainder Theorem, in *International Workshop on Public Key Cryptography 2002*, Springer-Verlag, (2002), 199–210.
21. O. Goldreich, D. Ron and M. Sudan, Chinese remaindering with errors, *IEEE Trans. Inf. Theory*, **46** (2000), 1330–1338.
22. R. Steinfeld, J. Pieprzyk and H. Wang, Lattice-based threshold-changeability for standard CRT secret-sharing schemes, *Finite Fields their Appl.*, **12** (2006), 653–680.
23. I. E. Shparlinski and R. Steinfeld, Noisy Chinese Remaindering in the Lee norm, *J. Complex.*, **20** (2004), 423–437.
24. Y. H. Liu and R. J. Chen, An asymptotically perfect secret sharing scheme based on the Chinese Remainder Theorem, *Int. J. Comput. Math.*, **94** (2017), 1890–1915.
25. L. Harn and F. Miao, Multilevel threshold secret sharing based on the Chinese Remainder Theorem, *Inf. Process Lett.*, **114** (2014), 504–509.
26. L. Harn, C. Hsu, M. Zhang, T. He and M. Zhang, Realizing secret sharing with general access structure, *Inf. Sci.*, **367** (2016), 209–220.
27. C. C. Drăgan and L. F. Ţiplea, Distributive weighted threshold secret sharing schemes, *Inf. Sci.*, **339** (2016), 85–97.
28. K. M. Martin, J. Pieprzyk, S. N. Rei and H. Wang, Changing thresholds in the absence of secure channels, in *Proceedings of the 4th Australasian Conference on Information Security and Privacy*, Springer Berlin Heidelberg, (1999), 177–191.
29. X. Jia, D. Wang, D. Nie, X. Luo and J. Z. Sun, A new threshold changeable secret sharing scheme based on the Chinese Remainder Theorem, *Inf. Sci.*, **473** (2019), 13–30.
30. C. Ding, D. Pei and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific Press, 1996.
31. C. Li, Y. Liu, L. Y. Zhang and K.-W. Wong, On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme, *Signal Process Image*, **29** (2014), 914–920.
32. P. Ribenboim, *The Book of Prime Number Records*, 2^{nd} edition, Springer-Verlag, New York, 1994.
33. J. Shao and Z. Cao, A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme, *Appl. Math. Comput.*, **168** (2005), 135–140.
34. C. W. Chan and C. C. Chang, A scheme for threshold multi-secret sharing, *Appl. Math. Comput.*, **166** (2009), 1–14.

AIMS Press