A Universal Secret Sharing Scheme with General Access Structure Based on CRT

Keju Meng
University of Science and technology of China
Email: mkj@mail.ustc.edu.cn

Fuyou Miao
University of Science and technology of China
Email: mfy@ustc.edu.cn
Corresponding author

Yue Yu
University of Science and technology of China
Email: yuyue204@mail.ustc.edu.cn

Changbin Lu
University of Science and technology of China
Email: lcb@mail.ustc.edu.cn

***Abstract*—In a (t,n) threshold secret sharing ((t,n)-SS) scheme, any equal to or more than t shareholders are able to reconstruct the secret by pooling shares together. However, (t,n)-SS cannot work when the access structure is not threshold. Later, the notion of secret sharing scheme with general access structure (GAS) was proposed. In a GAS scheme, access structure can be designed for any requirements. If and only if a set of shareholders satisfies required access structure, the secret can be recovered. Because access structures are more complex than simple (t,n) threshold, users need plenty of storage to keep multiple private shares in most GAS schemes. In order to reduce private shares of shareholder, this paper proposes a universal GAS scheme which breaks the hierarchical limitation of levels in a multilevel secret sharing scheme based on Chinese remainder theorem to make the GAS scheme available for any general access structure. More importantly, each shareholder just needs less storage to keep one private share in the proposed scheme.**

***Index Terms*—Secret sharing, Authorized subset, General access structure, Chinese remainder theorem, Private share.**

I. INTRODUCTION

Secret sharing (SS) schemes as fundamental privacy protection tools were first introduced by Shamir [26] and Blakley [3] separately in 1979. The access structure of both the two schemes is (t,n) threshold, i.e., they are (t,n) threshold secret sharing ((t,n)-SS) schemes. In a (t,n)-SS scheme, a dealer divides a secret s into n shares and sends each share to a shareholder. Then, any t or more than t shareholders can reconstruct the secret s by pooling their shares together, while at most $t-1$ shareholders cannot.

Since (t,n)-SS was proposed, it has been studied in a lot of literatures [23], [7], [18], [28], [6]. In order to implement (t,n)-SS, there are many methods. Shamir and Blakley schemes are based on polynomial interpolation and hyperplane geometry separately. McEliece et al. [21] introduced a scheme based on Reed-Solomon codes and Mignotte [22] proposed a ramp (t,n)-SS scheme founded on Chinese remainder theorem (CRT). Later, Asmuth and Bloom [1] implemented a perfect (t,n)-SS scheme also based on CRT. Guisquater et al. [24] showed the security of CRT-based (t,n)-SS schemes. Furthermore, (t,n)-SS has become a fundamental building block in many secure protocols, such as threshold signature schemes [4], threshold encryption schemes [8], [25], image sharing schemes [27], [29], and so on [9], [10], [11].

In a traditional (t,n)-SS scheme, each shareholder is deemed to enjoy the same right in secret reconstruction. Hence, it cannot work when the access structure is not threshold. For example, suppose there are three shareholders A, B, C in a SS scheme. If the dealer just wants that A, B or B, C can recover the secret while A, C cannot, the SS cannot be simple (2,3) threshold. Therefore, more general SS schemes are needed.

In 1987, Ito et al. [16] first introduced the concept of secret sharing scheme with general access structure (GAS). In a GAS scheme, access structure can be designed for any requirements instead of only threshold. Therefore, access structure in GAS is always more complex than it in (t,n)-SS and GAS is more difficult to design and implement. Benaloh et al. [2] proposed that the set of general secret sharing functions are corresponding to the set of monotone functions. In both Ito and Benaloh schemes, each shareholder is required to keep multiple shares. Thus, this type of SS schemes is called multiple assignment schemes. Later, linear SS was proposed to reduce the shares of shareholder in GAS. Iwamoto et al. [17] used integer programming to optimize the size of shares. Li et al. [20] proposed to use linear programming to reduce the shares of each shareholder.

Besides, weighted threshold secret sharing (WTSS) schemes as the foundation are also utilized to design GAS schemes for reducing shares of sharedholer. In a WTSS scheme, each share of a shareholder is allocated a positive weight. If and only if the overall weight of shares is equal to or greater than the threshold, the secret can be recovered. Iftene [15] proposed a GAS scheme based on WTSS. But the scheme just realizes the compartmented access structure. Harn et al. [14] tried to use a CRT-based WTSS scheme to design a GAS scheme. In the scheme, each shareholder can keep only one private share. However, the scheme cannot work for some special access structures. We will give an example to illustrate that in the following. Different from the above GAS schemes, the scheme proposed in this paper is based on a multilevel threshold secret sharing (MTSS) scheme.

As a special threshold secret sharing, MTSS has been studied for many years. In a MTSS scheme, shareholders are divided into different levels, each level with a threshold. Shareholder at higher level is allowed to participate in secret reconstruction at lower levels. If and only if the number of shareholders who come from a level or higher levels is equal to or greater than the threshold at the level, the secret can be recovered. In 1989, Brickell [5] introduced a MTSS scheme which is inefficient, because exponential operations are required to generate nonsingular matrices. Ghodosi et al. [12] proposed a perfect MTSS scheme based on Shamir (t,n)-SS. In the MTSS, the number of shareholders at higher level depends on the threshold at the level. Thus it is available only for few shareholders. Kumar et al. [19] proposed a MTSS scheme also based on Shamir (t,n)-SS, in which the number of public shares are proportional to the number of shareholders. In 2014, Harn and Miao [13] proposed a MTSS scheme based on Asmuth-Bloom SS. In the scheme, each shareholder keeps only one private share and it can use public information to modify its share to participate in secret reconstruction at lower levels. In this paper, we propose a GAS scheme based on Harn-Miao MTSS.

According to the above, we summarize our contributions below.

- We uncover some loopholes in Harn-Miao MTSS and give the corresponding methods to improve it.
- We break the hierarchical limitation of levels in Harn-Miao MTSS scheme to propose a GAS scheme.
- Each shareholder is required to keep only one private share in the GAS scheme.
- The GAS scheme is universal. In other words, it can work for any access structures.

The remainder of the paper is organized as follows. In the next section, we review some preliminary definitions and schemes. Detailed GAS scheme is shown in section III. For a better illustration, we give a numerical example in section IV. Security analysis and properties are given in section V and section VI respectively. We conclude the work in section VII.

II. Preliminaries

In this section, we first introduce some definitions about (t,n) SS, MTSS and GAS. Then, Chinese remainder theorem (CRT), Asmuth-Bloom SS and Harn-Miao MTSS are given as preliminaries.

A. *Definitions*

Definition 2.1. (t,n) secret sharing ((t,n) SS):

For a SS scheme, let $\mathcal{U}$ be a set of n shareholders. If the access structure Γ is

$$\Gamma = \{\mathcal{P} \subset \mathcal{U} : |\mathcal{P}| \geq t\},$$

where $\mathcal{P}$ is a shareholder set, Γ is threshold. In other word, any t or more than t shareholders can recover the secret. Then, the scheme is a (t,n) SS scheme.

Definition 2.2. Multilevel threshold secret sharing (MTSS):

For a SS scheme, let $\mathcal{U}$ be a set of n shareholders and assume that $\mathcal{U}$ is composed of m levels, i.e., $\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$, where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for all $1 \leq i \leq m$, $1 \leq j \leq m$ and $i \neq j$. Each level has a threshold t_i, and $\mathbf{t} = \{t_i\}_{i=1}^{m}$ is a monotonically increasing sequence of integers $0 < t_1 < t_2 < ... < t_m$. If the access structure Γ is

$$\Gamma = \{\mathcal{P} \subset \mathcal{U} : |\mathcal{P} \cap (\bigcup_{j=1}^{i} \mathcal{U}_j)| \geq t_i, \exists i \in \{1, 2, ..., m\}\},$$

where $\mathcal{P}$ is a shareholder set, Γ is multilevel threshold. Then, the scheme is a MTSS scheme.

Remark 2.1. Obviously, MTSS is a generalization of classical threshold SS. According to the definition of Γ in MTSS, shareholders at higher levels are allowed to participate in secret reconstruction at lower levels. Moreover, the secret can be recovered at any level L_i as long as equal to or more than t_i shareholders at L_i or higher levels pool their shares together.

Definition 2.3. Secret sharing scheme with general access structure (GAS):

For a SS scheme, let $\mathcal{U}$ be a set of n shareholders. For a shareholder set $\mathcal{A}$ ($\mathcal{A} \subseteq \mathcal{U}$), it is called a minimal authorized subset if it satisfies the two conditions:

1. It can recover the secret easily.

2. It will not recover the secret if any one shareholder is removed from it.

The family of all minimal authorized subsets is called the access structure Γ, where $\Gamma \subseteq 2^{\mathcal{U}}$ and $2^{\mathcal{U}}$ is the power set including all the subsets of $\mathcal{U}$. Then, if Γ can be designed as any structure, the scheme is a GAS scheme. In other words, the access structure Γ of a GAS scheme does not need to meet any restrictions such as threshold, multilevel, weighted and so on.

Remark 2.2. GAS has the monotone property. In other words, not only minimal authorized sets but also any supersets of a minimal authorized set can realize secret reconstruction, and they are collectively called authorized sets.

B. *Chinese remainder theorem*

Given the following system of equations,

$$\begin{aligned} x &= x_1 \bmod p_1 \\ x &= x_2 \bmod p_2 \\ &...... \\ x &= x_t \bmod p_t \end{aligned}$$

where all moduli are pairwise co-prime, i.e. $\gcd(p_i, p_j) = 1$ for $i \neq j$. The unique solution of x can be computed as $x = \sum_{i=1}^{t} \frac{P}{p_i} \cdot y_i \cdot x_i \bmod P$, where $P = p_1 \cdot p_2 \cdot ... \cdot p_t$ and $y_i \cdot \frac{P}{p_i} \bmod p_i = 1$.

C. *Asmuth-Bloom SS [1]*

In Asmuth-Bloom SS which is based on CRT, there are n shareholders $U_1, U_2, ..., U_n$, and a mutually trusted dealer $\mathcal{D}$. The scheme consists of two process:

Shares generation: At first, $\mathcal{D}$ selects a prime p_0 and a sequence of pairwise co-prime positive integers, $p_1, p_2, ..., p_n$

with $p_1 < p_2 < ... < p_n$, $p_0 \cdot p_{n-t+2} \cdot p_{n-t+1} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$ and $\gcd(p_0, p_i) = 1$ for $i = 1, 2, ..., n$. Then, $\mathcal{D}$ picks a secret s and random integer α in $\mathbb{Z}_{p_0}$, such that $x = s + \alpha p_0 < p_1 \cdot p_2 \cdot ... \cdot p_t$. Finally, $\mathcal{D}$ computes and sends $s_i = x \bmod p_i$ to shareholder U_i as the share securely.

Secret reconstruction: If m $(m \geq t)$ shareholders, e.g. $U_1, U_2, ..., U_m$, collaborate to recover the secret, each of them releases its private share to the others. After receiving the other $m-1$ shares, each shareholder U_i has a system of equations:

$$\begin{aligned} x &= s_1 \bmod p_1 \\ x &= s_2 \bmod p_2 \\ &\cdots\cdots \\ x &= s_m \bmod p_m \end{aligned}$$

Using standard CRT, the value of x is determined as $x = \sum_{i=1}^{m} \frac{P}{p_i} \cdot y_i \cdot s_i \bmod P$, where $P = p_1 \cdot p_2 \cdot ... \cdot p_m$ and $y_i \cdot \frac{P}{p_i} \bmod p_i = 1$. Then, the secret s can be obtained as $s = x \bmod p_0$.

D. Harn-Miao MTSS [13]

In the scheme, shareholders are partitioned into m levels $L_1, L_2, ..., L_m$, where L_i is higher level than L_j if i is less than j. Harn-Miao MTSS scheme consists of two phases:

Shares generation: The dealer $\mathcal{D}$ picks a prime p_0 and secret $s \in \mathbb{Z}_{p_0}$. For each level L_i having n_i shareholders, $\mathcal{D}$ selects a sequence of pairwise co-prime positive integers $p_1^i < p_2^i < ... < p_{n_i}^i$, such that $p_0 \cdot p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+1}^i \cdot ... \cdot p_{n_i}^i < p_1^i \cdot p_2^i \cdot ... \cdot p_{t_i}^i$ and $\gcd(p_0, p_k^i) = 1$ for $k = 1, 2, ..., n_i$, where p_k^i is public modulus associated with U_i in level L_i. For each such sequence, $\mathcal{D}$ picks a random integer α_i such that $p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+1}^i \cdot ... \cdot p_{n_i}^i < x_i = s + \alpha_i \cdot p_0 < p_1^i \cdot p_2^i \cdot ... \cdot p_{t_i}^i$. In this way, the value of $s + \alpha_i \cdot p_0$ is in the t_i-threshold range, $\mathbb{Z}_{p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+1}^i \cdot ... \cdot p_{n_i}^i, p_1^i \cdot p_2^i \cdot ... \cdot p_{t_i}^i}$. The private share for shareholder U_k^i is computed as $s_k^i = s + \alpha_i \cdot p_0 \bmod p_k^i$. The dealer $\mathcal{D}$ sends s_k^i to U_k^i in private. According to the definition of MTSS, shareholders at higher levels can participate in secret reconstruction at lower levels. In this scheme, to enable s_k^i of U_k^i to be used as a share at L_j, where $j > i$, the dealer $\mathcal{D}$ selects a new modulus $p_{k,i}^j$ such that $p_{t_j}^j < p_{k,i}^j < p_{n_j-t_j+2}^j$. Then, it computes a difference $\Delta s_{k,i}^j = (s + \alpha_j p_0 - s_k^i) \bmod p_{k,i}^j$. The pair $(\Delta s_{k,i}^j, p_{k,i}^j)$ is public information associated with U_k^i for $j = i+1, i+2, ..., m$, so that U_k^i keeps only one private share s_k^i.

Secret reconstruction: When equal to or more than t_j shareholders who come from L_j or higher levels collaborate to recover the secret at L_j, shareholder U_k^j uses its modulus p_k^j and private share s_k^j directly while shareholder U_k^i at higher level needs to use a new modulus $p_{k,i}^j$ and modified share $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j)$. After pooling shares together, the value of x_i can be evaluated by using standard CRT. And the secret s is computed as $s = x_i \bmod p_0$.

Remark 2.3. Different from Asmuth-Bloom SS, the value of $s + \alpha_i \cdot p_0$ falls into the range $(p_0 \cdot p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+1}^i \cdot ... \cdot p_{n_i}^i, p_1^i \cdot p_2^i \cdot ... \cdot p_{t_i}^i)$ in Harn-Miao MTSS. In this way, the secret cannot be recovered at level L_i by less than t_i shareholders who come from L_i or higher levels. Hence, $s + \alpha_i \cdot p_0$ is in the t_i-threshold range.

Remark 2.4. In Harn-Miao MTSS, there still exist two loopholes.

1) When shareholder U_k^i participates in secret reconstruction at lower level L_j $(i < j)$, it needs a new modulus $p_{k,i}^j$, such that $p_{t_j}^j < p_{k,i}^j < p_{n_j-t_j+2}^j$. Nevertheless, the modulus $p_{k,i}^j$ is non-existent if the number of shareholders n_j and threshold t_j at L_j satisfy $n_j - t_j + 2 < t_j$.

2) The new share $s_{k,i}^j$ of U_k^i used at L_j should be computed as $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j) \bmod p_{k,i}^j$ instead of $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j)$, because the value of $s_k^i + \Delta s_{k,i}^j$ may be greater than $p_{k,i}^j$.

We give the corresponding measures to solve the loopholes in our GAS scheme. Moreover, Harn's paper [13] does not explain why the public numbers $\Delta s_{k,i}^j$ do not reveal information about the secret s. Likewise, the proof is given after our proposed scheme.

III. Our scheme

In this section, we propose our GAS scheme based on CRT in detail. In Harn-Miao MTSS, levels are strictly hierarchical. A shareholder at higher level is allowed to use public information and private share to compute new shares to participate in recovering the secret at lower levels. However, shares at lower levels cannot be modified as valid shares at higher levels. In this paper, we break the hierarchical restriction in Harn-Miao MTSS to propose a universal GAS scheme.

Our scheme consists of three algorithms: 1) Pretreatments, 2) Shares generation, 3) Secret reconstruction.

A. Algorithms

1) Pretreatments: Let n be the total number of all the shareholders and each shareholder is marked as U_i for $i = 1, 2, ..., n$. Define $\mathcal{U} = \{U_1, U_2, ..., U_n\}$ as the shareholder set. Furthermore, let m be the total number of all minimal authorized subsets and each minimal authorized subset is $\mathcal{A}_j$ $(\mathcal{A}_j \subseteq \mathcal{U})$ for $j = 1, 2, ..., m$. The family of all minimal authorized subsets is the access structure Γ, i.e., $\Gamma = \{\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_m\}$. Parts of minimal authorized subsets can constitute a part access structure γ, where $\gamma \subseteq \Gamma$.

For the given access structure Γ, it can be divided into two parts Γ_t and Γ_o. If a part access structure γ is threshold, it belongs to Γ_t, i.e., minimal authorized subsets in γ are added into Γ_t. For the minimal authorized subsets which cannot constitute a part access structure satisfying threshold structure, they pertain to Γ_o.

For a part access structure in Γ_t or a minimal authorized subset in Γ_o, it is a (t,n) threshold structure. Furthermore, it can be regarded as a level in our GAS scheme. In more detail, if a level is a part access structure in Γ_t, the threshold t is less than n. If a level is a minimal authorized subset in Γ_o, the threshold t is equal to n. But unlike hierarchical levels in MTSS, the levels in our scheme have equal status. For simplicity, suppose there are total h levels in both Γ_t and Γ_o, and we rename each level as L_i for $i = 1, 2, ..., h$. Moreover, each level L_i has n_i shareholders and the threshold is t_i.

Each shareholder at L_i is marked as U_k^i for $k = 1, 2, ..., n_i$.

Remark 3.1. In order to make pretreatments easily understandable, we give an example to explain them. Suppose there are 5 shareholders U_1, U_2, U_3, U_4, U_5 and all the minimal authorized subsets are $\mathcal{A}_1 = \{U_1, U_2\}$, $\mathcal{A}_2 = \{U_1, U_3\}$, $\mathcal{A}_3 = \{U_2, U_3\}$, $\mathcal{A}_4 = \{U_3, U_4, U_5\}$, $\mathcal{A}_5 = \{U_2, U_4\}$, $\mathcal{A}_6 = \{U_1, U_5\}$. Obviously, the access structure is

$$\begin{aligned}\Gamma &= \{\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_5, \mathcal{A}_6\} \\ &= \{\{U_1, U_2\}, \{U_1, U_3\}, \{U_2, U_3\}, \\ &\qquad \{U_3, U_4, U_5\}, \{U_2, U_4\}, \{U_1, U_5\}\}\end{aligned}$$

For the part access structure $\gamma = \{\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3\} = \{\{U_1, U_2\}, \{U_1, U_3\}, \{U_2, U_3\}\}$, it is a (2,3) threshold structure. Therefore, $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}_3$ belong to Γ_t. Because $\mathcal{A}_4$, $\mathcal{A}_5$ and $\mathcal{A}_6$ cannot form a part access structure which is threshold, they are part of Γ_o. After division, there are 4 levels. L_1 has $n_1 = 3$ shareholders $\{U_1, U_2, U_3\}$ and the threshold t_1 equals 2. L_2 is a (3,3) SS with $\{U_3, U_4, U_5\}$. L_3 and L_4 are both (2,2) SSs with $\{U_2, U_4\}$ and $\{U_1, U_5\}$ respectively.

2) Shares generation: The dealer $\mathcal{D}$ selects a prime p_0 and the secret s, defining the secret space as $\mathbb{Z}_{p_0}$. For each level L_i, $\mathcal{D}$ picks a sequence of pairwise co-prime positive integers $p_1^i < p_2^i < ... < p_{n_i}^i$, such that $p_0 \cdot p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+1}^i \cdot ... \cdot p_{n_i}^i < p_1^i \cdot p_2^i \cdot ... \cdot p_{t_i}^i$ and $\gcd(p_0, p_k^i) = 1$ for $k = 1, 2, ..., n_i$, where p_k^i is public modulus associated with U_k^i in L_i. For each such sequence, $\mathcal{D}$ picks a random integer α_i such that $p_{n_i-t_i+2}^i \cdot p_{n_i-t_i+1}^i \cdot ... \cdot p_{n_i}^i < x_i = s + \alpha_i \cdot p_0 < p_1^i \cdot p_2^i \cdot ... \cdot p_{t_i}^i$. On this point, we follow Harn-Miao MTSS rather than Asmuth-Bloom SS to ensure x_i in the t_i-threshold range. The dealer $\mathcal{D}$ generates a value of s_k^i as $s_k^i = s + \alpha_i \cdot p_0 \bmod p_k^i$. s_k^i as the private share is sent to U_k^i in secret.

In fact, a shareholder is usually included in many minimal authorized subsets. Therefore, it may be able to participate in secret reconstruction at multiple levels. In order to ensure that a shareholder uses its private share to participate in secret reconstruction at more than one levels, extra information is needed. Concretely, if a shareholder U_k^i at L_i is allowed to recover the secret at another level L_j, the dealer $\mathcal{D}$ is required to provide a new modulus $p_{k,i}^j$ and difference $\Delta s_{k,i}^j$ between s_k^i and $s_{k,i}^j$, where $p_{k,i}^j$ and $s_{k,i}^j$ are the modulus and share of U_k^i used at L_j. For the level L_j, $\mathcal{D}$ also selects a sequence of pairwise co-prime positive integers $p_1^j < p_2^j < ... < p_{n_j}^j$, such that $p_0 \cdot p_{n_j-t_j+2}^j \cdot p_{n_j-t_j+1}^j \cdot ... \cdot p_{n_j}^j < p_1^j \cdot p_2^j \cdot ... \cdot p_{t_j}^j$ and $\gcd(p_0, p_k^j) = 1$ for $k = 1, 2, ..., n_j$. The new modulus $p_{k,i}^j$ of U_k^i is picked from the sequence $p_1^j, p_2^j, ..., p_{n_j}^j$, such that $p_{k,i}^j \leq p_k^i$. Moreover, $\mathcal{D}$ selects a random integer α_j such that $p_{n_j-t_j+2}^j \cdot p_{n_j-t_j+1}^j \cdot ... \cdot p_{n_j}^j < x_j = s + \alpha_j \cdot p_0 < p_1^j \cdot p_2^j \cdot ... \cdot p_{t_j}^j$. The difference $\Delta s_{k,i}^j$ can be computed as $\Delta s_{k,i}^j = (s + \alpha_j \cdot p_0 - s_k^i) \bmod p_{k,i}^j$. Then, the pair $(p_{k,i}^j, \Delta s_{k,i}^j)$ as public information is sent to shareholder U_k^i.

3) Secret reconstruction: If a shareholder set $\mathcal{H}$ is a superset of a minimal authorized subset, i.e.,

$$\mathcal{H} = \{\exists \mathcal{A} \subseteq \mathcal{H} | \mathcal{A} \subseteq \Gamma, \Gamma = \{\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_m\}\},$$

$\mathcal{H}$ can recover the secret s according to the definition of GAS and Remark 2.2. Suppose that $\mathcal{H}$ is a superset of $\mathcal{A}_i$ which is divided into the level L_j in the process of pretreatments. Then, m ($m \geq t_j$) shareholders who are able to participate in secret reconstruction at L_j are included in $\mathcal{H}$ and they can form a subset $\mathcal{H}_m$, such that $\mathcal{H}_m \subseteq \mathcal{H}$. If U_k^j in $\mathcal{H}_m$ receives its private share s_k^j at L_j, it uses s_k^j and p_k^j to participate in secret reconstruction directly. If U_k^i in $\mathcal{H}_m$ receives its private share s_k^i at another level L_i, it should first use the pair $(\Delta s_{k,i}^j, p_{k,i}^j)$ to compute a new share as $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j) \bmod p_{k,i}^j$. And then U_k^i uses $s_{k,i}^j$ and $p_{k,i}^j$ to participate in secret reconstruction. After each shareholder in $\mathcal{H}_m$ releases its share to the others in $\mathcal{H}$, the value of x_j can be evaluated by using the standard CRT, and the secret s is computed as $s = x_j \bmod p_0 = (s + \alpha_j \cdot p_0) \bmod p_0$.

B. Discussion

As mentioned above about the loopholes in Harn-Miao scheme, the new module $p_{k,i}^j$ of U_k^i may be non-existent since the dealer selects $p_{k,i}^j$ after the sequence $p_1^j, p_2^j, ..., p_{n_j}^j$ is fixed. Therefore, in our GAS scheme, the dealer D is supposed to add $p_{k,i}^j$ to $p_1^j, p_2^j, ..., p_{n_j}^j$ when D picks the sequence. Besides, the new share $s_{k,i}^j$ of U_k^i used at L_j is computed as $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j) \bmod p_{k,i}^j$ instead of $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j)$ so that $s_{k,i}^j$ is limited in $\mathbb{Z}_{p_{k,i}^j}$.

In this scheme, if a shareholder U_k^i receives private share from level L_i and it is allowed to participate in secret reconstruction at L_j, its the new modulus $p_{k,i}^j$ used at L_j is picked from the sequence of pairwise co-prime positive integers $p_1^j, p_2^j, ..., p_{n_j}^j$ at L_j. In this way, $p_{k,i}^j$ is always existent no matter what relationship between n_j and t_j. Moreover, the new modulus $p_{k,i}^j$ of U_k^i should be not greater than the original modulus p_k^i used at L_i. This condition can secure our scheme. Since U_k^i only keeps one private share s_k^i while p_k^i, $p_{k,i}^j$ and $\Delta s_{k,i}^j$ are public, an adversary can derive a range $[\Delta s_{k,i}^j, \Delta s_{k,i}^j + p_k^i) \bmod p_{k,i}^j$ about the new share $s_{k,i}^j$. However, for the adversary, $s_{k,i}^j$ is supposed to be over the range $[0, p_{k,i}^j)$ because the new modulus is $p_{k,i}^j$. If $p_{k,i}^j$ is greater than p_k^i, $[\Delta s_{k,i}^j, \Delta s_{k,i}^j + p_k^i) \bmod p_{k,i}^j$ is just a sub-range in $[0, p_{k,i}^j)$. It means that the adversary narrows the range of $s_{k,i}^j$. Thus, $p_{k,i}^j$ should be not greater than p_k^i. In more detail, there still is a minor problem that $s_{k,i}^j$ may be not a uniform distribution in $[0, p_{k,i}^j)$. The probability of $s_{k,i}^j$ in $[\Delta s_{k,i}^j, \Delta s_{k,i}^j + p_k^i \bmod p_{k,i}^j) \bmod p_{k,i}^j$ is $\left\lceil p_k^i / p_{k,i}^j \right\rceil / p_k^i$. The probability of $s_{k,i}^j$ in the other sub-range is $\left\lfloor p_k^i / p_{k,i}^j \right\rfloor / p_k^i$. Even so, the adversary cannot narrow the range of $s_{k,i}^j$ as long as the condition $p_{k,i}^j \leq p_k^i$ holds.

IV. Numerical Example

In this section, we give a numerical example about our proposed GAS scheme for a better illustration.

Suppose that there are $n = 6$ shareholders $U_1, U_2, U_3, U_4, U_5, U_6$ and $m = 6$ minimal authorized subsets $\mathcal{A}_1 = \{U_1, U_2\}$, $\mathcal{A}_2 = \{U_1, U_3\}$, $\mathcal{A}_3 = \{U_2, U_3\}$, $\mathcal{A}_4 = \{U_1, U_4\}$, $\mathcal{A}_5 = \{U_2, U_5\}$, $\mathcal{A}_6 = \{U_4, U_5, U_6\}$. Therefore, the access structure is

$$\begin{aligned}\Gamma &= \{\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_5, \mathcal{A}_6\}\\ &= \{\{U_1, U_2\}, \{U_1, U_3\}, \{U_2, U_3\},\\ &\qquad \{U_1, U_4\}, \{U_2, U_5\}, \{U_4, U_5, U_6\}\}\end{aligned}$$

In the given access structure, $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$ form a part access structure γ which is a (2,3) threshold structure. Thus, γ belongs to Γ_t. The other minimal authorized subsets $\mathcal{A}_4$, $\mathcal{A}_5$, and $\mathcal{A}_6$ cannot form a threshold part access structure, so they are included in Γ_o. Then, we get 4 levels. L_1 is a (2,3) SS with $\{U_1, U_2, U_3\}$. L_2 is a (2,2) SS with $\{U_1, U_4\}$. L_3 is also a (2,2) SS with $\{U_2, U_5\}$. L_4 is a (3,3) SS with $\{U_4, U_5, U_6\}$.

The dealer $\mathcal{D}$ selects a prime $p_0 = 139$ and the secret $s = 101$ initially. In the level L_1 ((2,3) threshold), remark U_1 as U_1^1, U_2 as U_2^1 and U_3 as U_3^1. $\mathcal{D}$ picks 3 pairwise co-prime moduli $p_1^1 = 239$, $p_2^1 = 257$ and $p_3^1 = 277$, such that $p_0 \cdot p_3^1 < p_1^1 \cdot p_2^1$. Thus, the t_1-threshold range is $(277, 61423)$. $\mathcal{D}$ selects an integer $\alpha_1 = 346$ and $x_1 = s + \alpha_1 \cdot p_0 = 48195$, such that $277 < x_1 < 61423$. The private share s_1^1 of U_1^1 is computed as $s_1^1 = x_1 \bmod p_1^1 = 156$. The other two shares are $s_2^1 = x_1 \bmod p_2^1 = 136$ and $s_3^1 = x_1 \bmod p_3^1 = 274$. s_k^1 as private share is sent to the corresponding shareholder U_k^1 secretly for $k = 1, 2, 3$.

In the level L_2 ((2,2) threshold), remark U_1 as U_1^2 and U_4 as U_2^2. The dealer $\mathcal{D}$ picks 2 co-prime moduli $p_1^2 = p_{1,1}^2 = 179$ and $p_2^2 = 197$, such that $p_{1,1}^2 < p_1^1$ and $p_0 \cdot p_2^2 < p_1^2 \cdot p_2^2$. So the t_2-threshold range is $(197, 35263)$. $\mathcal{D}$ selects an integer $\alpha_2 = 195$ and $x_2 = s + \alpha_2 \cdot p_0 = 27206$, such that $197 < x_2 < 35263$. $\mathcal{D}$ computes $\Delta s_{1,1}^2 = (x_2 - s_1^1) \bmod p_{1,1}^2 = 21$ because $\mathcal{D}$ sends private share to U_1 at L_1. $\Delta s_{1,1}^2$ as public information is associated with U_1. The private share $s_2^2 = x_2 \bmod p_2^2 = 20$ is sent to U_2^2 in secure.

In the level L_3 ((2,2) threshold), remark U_2 as U_1^3 and U_5 as U_2^3. The dealer $\mathcal{D}$ picks 2 co-prime moduli $p_1^3 = p_{2,1}^3 = 151$ and $p_2^3 = 191$, such that $p_{2,1}^3 < p_2^1$ and $p_0 \cdot p_2^3 < p_1^3 \cdot p_2^3$. Hence, the t_3-threshold is $(191, 28841)$. $\mathcal{D}$ selects an integer $\alpha_3 = 106$ and $x_3 = s + \alpha_3 \cdot p_0 = 14835$, such that $191 < x_3 < 28841$. Because U_2 receives its private share at L_1, $\mathcal{D}$ computes $\Delta s_{2,1}^3 = (x_3 - s_2^1) \bmod p_{2,1}^3 = 148$ which is public information associated with U_2. The private share $s_2^3 = x_3 \bmod p_2^3 = 128$ is sent to U_2^3 secretly.

In the level L_4 ((3,3) threshold), remark U_4 as U_1^4, U_5 as U_2^4 and U_6 as U_3^4. The dealer $\mathcal{D}$ picks 3 pairwise co-prime moduli $p_1^4 = p_{2,2}^4 = 149$, $p_2^4 = p_{2,3}^4 = 173$ and $p_3^4 = 199$, such that $p_{2,2}^4 < p_2^2$, $p_{2,3}^4 < p_2^3$ and $p_0 \cdot p_2^4 \cdot p_3^4 < p_1^4 \cdot p_2^4 \cdot p_3^4$. Therefore, the t_4-threshold range is $(34427, 5129623)$. $\mathcal{D}$ selects an integer $\alpha_4 = 25976$ and $x_4 = s + \alpha_4 \cdot p_0 = 3610765$, such that $34427 < x_4 < 5129623$. Because U_4 and U_5 receive private shares at other levels, $\mathcal{D}$ computes $\Delta s_{2,2}^4 = (x_4 - s_2^2) \bmod p_{2,2}^4 = 28$ which is public information associated with U_4 and $\Delta s_{2,3}^4 = (x_4 - s_2^3) \bmod p_{2,3}^4 = 127$ which is public information associated with U_5. The private share $s_3^4 = x_4 \bmod p_3^4 = 109$ is sent to U_3^4 in secret.

(Case 1) Suppose that U_1, U_3 and U_5 collaborate to recover the secret s. They form a shareholder set $\mathcal{H} = \{U_1, U_3, U_5\}$. Because there exists a subset $\mathcal{H}_2 = \{U_1, U_3\}$ such that $\mathcal{H}_2 \subseteq \mathcal{H}$ and $\mathcal{H}_2 = \mathcal{A}_2$, $\mathcal{H}$ can recover the secret at L_1. Since both U_1 and U_3 receive private shares at L_1, they can use their shares directly without modification. After U_1 and U_3 send shares to the others in $\mathcal{H}$, each shareholder in $\mathcal{H}$ gets has a system of equations:

$$\begin{aligned}x_1 &= s_1^1 \bmod p_1^1\\ x_1 &= s_3^1 \bmod p_3^1\end{aligned}$$

Using standard CRT, the value of x_1 can be evaluated as

$$\begin{aligned}x_1 &= (\frac{239*277}{239}*195*156+\frac{239*277}{277}*51*274) \bmod (239*277)\\ &= (8426340+3339786) \bmod 66203\\ &= 11766126 \bmod 66203\\ &= 48195\end{aligned}$$

So, the secret s is computed as

$$\begin{aligned}s &= x_1 \bmod p_0\\ &= 48195 \bmod 139\\ &= 101\end{aligned}$$

(Case 2) Suppose that U_3, U_4, U_5 and U_6 collaborate to recover the secret s. They form a shareholder set $\mathcal{H} = \{U_3, U_4, U_5, U_6\}$. Because there exists a subset $\mathcal{H}_3 = \{U_4, U_5, U_6\}$ such that $\mathcal{H}_3 \subseteq \mathcal{H}$ and $\mathcal{H}_3 = \mathcal{A}_6$, $\mathcal{H}$ can recover the secret at L_4. U_4 receives its private share s_2^2 at other level, hence it should compute a new share $s_{2,2}^4 = (s_2^2 + \Delta s_{2,2}^4) \bmod p_{2,2}^4 = 48$. Likewise, U_5 is required to compute its new share $s_{2,3}^4 = (s_2^3 + \Delta s_{2,3}^4) \bmod p_{2,3}^4 = 82$. U_6 can use its share directly without modification since the dealer $\mathcal{D}$ sends s_3^4 to it at level L_4. After U_4, U_5 and U_6 send shares to the others in $\mathcal{H}$, each shareholder in $\mathcal{H}$ gets has a system of equations:

$$\begin{aligned}x_4 &= s_{2,2}^4 \bmod p_{2,2}^4\\ x_4 &= s_{2,3}^4 \bmod p_{2,3}^4\\ x_4 &= s_3^4 \bmod p_3^4\end{aligned}$$

Using standard CRT, the value of x_1 can be evaluated as

$$\begin{aligned}x_4 &= (\frac{149*173*199}{149}*56*48+\frac{149*173*199}{173}*28*82\\ &\quad +\frac{149*173*199}{199}*92*109) \bmod (149*173*199)\\ &= (92539776+68078696+258491756) \bmod 5129623\\ &= 419110228 \bmod 5129623\\ &= 3610765\end{aligned}$$

So, the secret s is computed as

$$\begin{aligned} s &= x_4 \bmod p_0 \\ &= 3610765 \bmod 139 \\ &= 101 \end{aligned}$$

V. Security analysis

In this section, we give two theorems to analyse the security of our scheme.

Theorem 1. No information about the secret s can be derived from public number $\Delta s^j_{k,i}$.

Proof: From the equation $\Delta s^j_{k,i} = (s+\alpha_j \cdot p_0 - s^i_k) \bmod p^j_{k,i}$, we can get

$$\begin{aligned} \Delta s^j_{k,i} &= (s + \alpha_j p_0 - s^i_k) \bmod p^j_{k,i} \\ &= (s + \alpha_j p_0 - (s + \alpha_i p_0) \bmod p^i_k) \bmod p^j_{k,i} \\ &= (s + \alpha_j p_0 - s - \alpha_i p_0 + \beta p^i_k) \bmod p^j_{k,i} \\ &= ((\alpha_j - \alpha_i)p_0 + \beta p^i_k) \bmod p^j_{k,i} \quad (5-1) \end{aligned}$$

where β is a random integer. Obviously the secret s is not included in the equation (5-1). That means $\Delta s^j_{k,i}$ does not reveal any information about s.

Theorem 2. The value of x_i is required to fall into the range $(p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+1} \cdot ... \cdot p^i_{n_i}, p^i_1 \cdot p^i_2 \cdot ... \cdot p^i_{t_i})$ in our scheme. This condition ensures our scheme secure. In other words, for a shareholder set $\mathcal{H}$,

(1) it can recover the secret, if there is a minimal authorized subset $\mathcal{A}_i$ such that $\mathcal{A}_i \subseteq \mathcal{H}$.

(2) it cannot recover the secret, if the intersection of $2^{\mathcal{H}}$ (the power set including all the subsets of $\mathcal{H}$) and access structure Γ is empty set, i.e., $2^{\mathcal{H}} \cap \Gamma = \varnothing$.

Proof: For shareholders in a minimal authorized subset $\mathcal{A}_i$ which is divided into L_k, each of them keeps or is able to compute a valid share used at the common level L_k. According to the rules of shares generation, the number of shareholders in $\mathcal{A}_i$ is just equal to the threshold t_k at L_k. Thus a minimal authorized subset $\mathcal{A}_i$ can recover the secret at L_k. Furthermore, because GAS has the monotone property, a superset of $\mathcal{A}_i$ can also recover the secret.

For an unauthorized shareholder set $\mathcal{N}$, because of $2^{\mathcal{N}} \cap \Gamma = \varnothing$, all the minimal authorized subsets are not subsets of $\mathcal{N}$, i.e., $\mathcal{A}_i \subsetneq \mathcal{N}$ for $i = 1, 2, ..., m$. In other word, the number of shareholders who come from $\mathcal{N}$ and are able to recover the secret at L_i is less than the threshold t_i at L_i, for $i = 1, 2, ..., h$. Each value x_i is in the t_i-threshold range $\mathbb{Z}_{p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+1} \cdot ... \cdot p^i_{n_i}, p^i_1 \cdot p^i_2 \cdot ... \cdot p^i_{t_i}}$, hence the unauthorized shareholder set $\mathcal{N}$ cannot recover the secret.

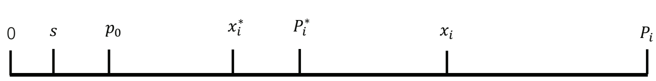

Fig. 1: Relationship among parameters

In more detail, suppose that $\mathcal{N}$ tries to recover the secret at L_i. Without losing the generality, assume that $t_i - 1$ shareholders from $\mathcal{N}$ have valid shares at L_i and their moduli are $p^i_{n_i-t_i+2}, p^i_{n_i-t_i+1}, ..., p^i_{n_i}$. They can use the standard CRT to compute a false value x^*_i, where $x^*_i < p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+1} \cdot ... \cdot p^i_{n_i}$. But x^*_i satisfies the equation $x^*_i = x_i + l \cdot P^*$, where $P^*_i = p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+1} \cdot ... \cdot p^i_{n_i}$. Then, the integer l falls into the range $\mathcal{L} = (0, P/P^*)$, where $P_i = p^i_1 \cdot p^i_2 \cdot ... \cdot p^i_{t_i}$. Because the sequence of pairwise co-prime positive integers satisfies $p_0 \cdot p^i_{n_i-t_i+2} \cdot p^i_{n_i-t_i+1} \cdot ... \cdot p^i_{n_i} < p^i_1 \cdot p^i_2 \cdot ... \cdot p^i_{t_i}$, $|\mathcal{L}|$ is greater than p_0. This means $\mathcal{N}$ cannot narrow the secret range $\mathbb{Z}_{p_0}$ to a smaller interval. Relationship among the above parameters is shown in figure 1.

VI. Properties

We compare our scheme (based on MTSS) with Ito et al. scheme [16] (original GAS scheme), Li et al. scheme [20] (based on linear SS) and Harn et al. scheme [14] (based on WTSS) in this section.

For the number of shares of a shareholder, in both Ito et al. and Li et al. schemes, each shareholder should keep multiple private shares to realize general access structure. In Ito scheme, the number of shares which a shareholder keeps is equal to the number of minimal authorized sets which the shareholder belongs to. Li et al. utilized linear programming to reduce the shares of each shareholder relative to Ito scheme. But in Harn et al. and our scheme, only one private share is sent to a shareholder.

Schemes in [16], [20] and this paper, they are all universal. In other words, they can realize any access structure. But in Harn et al. scheme, some special access structure cannot be realized. For example, Harn et al. GAS scheme cannot work for the numerical example in section 5. According to the rules in [14], the weight of any maximal unauthorized subset is less than it of any minimal authorized subset. Therefore, we can get the two inequalities, where w_{U_i} is the weight of U_i.

$$w_{U_1} + w_{U_5} + w_{U_6} < w_{U_4} + w_{U_5} + w_{U_6} => w_{U_1} < w_{U_4}$$

$$w_{U_2}+w_{U_4}+w_{U_6} < w_{U_1}+w_{U_2} => w_{U_4}+w_{U_6} < w_{U_1} => w_{U_4} < w_{U_1}$$

Obviously, the two inequalities are incompatible. Thus, Harn et al. GAS scheme is not available for the given access structure.

We give a table 1 to show the comparisons.

TABLE I: Comparisons table

scheme	the number of shares	universality
Ito et al. scheme [16]	multiple	yes
Li et al. scheme [20]	multiple (fewer than Ito scheme)	yes
Harn et al. scheme [14]	one	no
Our scheme	one	yes

VII. Conclusion

Traditional (t,n)-SS schemes are effective only when access structures are threshold. In this paper, we propose a universal secret sharing with general access structure (GAS) based on Chinese remainder theorem. The scheme brakes the hierarchical limitation of levels in Harn-Miao multilevel secret sharing

(MTSS) scheme so that it can realize general access structure. Furthermore, just like the Harn-Miao MTSS, each shareholder is required to keep only one private share in our GAS scheme.

ACKNOWLEDGEMENT

This work is supported by National Natural Science Foundation of China under 61572454, 61572453, 61472382, 61520106007.

REFERENCES

[1] Charles Asmuth and John Bloom. A modular approach to key safeguarding. *IEEE transactions on information theory*, 29(2):208–210, 1983.

[2] Josh Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *Proceedings on Advances in cryptology*, pages 27–35. Springer-Verlag New York, Inc., 1990.

[3] George Robert Blakley et al. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, pages 313–317, 1979.

[4] Alexandra Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *International Workshop on Public Key Cryptography*, pages 31–46. Springer, 2003.

[5] Ernest F Brickell. Some ideal secret sharing schemes. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 468–475. Springer, 1989.

[6] Christian Cachin, Klaus Kursawe, Anna Lysyanskaya, and Reto Strobl. Asynchronous verifiable secret sharing and proactive cryptosystems. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 88–97. ACM, 2002.

[7] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pages 383–395. IEEE, 1985.

[8] Yvo G Desmedt. Threshold cryptography. *Transactions on Emerging Telecommunications Technologies*, 5(4):449–458, 1994.

[9] Keke Gai and Meikang Qiu. Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. *IEEE Transactions on Industrial Informatics*, 2017.

[10] Keke Gai, Meikang Qiu, Zhong Ming, Hui Zhao, and Longfei Qiu. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Transactions on Smart Grid*, 8(5):2431–2439, 2017.

[11] Keke Gai, Meikang Qiu, Zenggang Xiong, and Meiqin Liu. Privacy-preserving multi-channel communication in edge-of-things. *Future Generation Computer Systems*, 2018.

[12] Hossein Ghodosi, Josef Pieprzyk, and Rei Safavi-Naini. Secret sharing in multilevel and compartmented groups. In *Information Security and Privacy*, pages 367–378. Springer, 1998.

[13] Lein Harn and Miao Fuyou. Multilevel threshold secret sharing based on the chinese remainder theorem. *Information processing letters*, 114(9):504–509, 2014.

[14] Lein Harn, Chingfang Hsu, Mingwu Zhang, Tingting He, and Maoyuan Zhang. Realizing secret sharing with general access structure. *Information Sciences*, 367:209–220, 2016.

[15] Sorin Iftene. General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science*, 186:67–84, 2007.

[16] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.

[17] Mitsugu Iwamoto, Hirosuke Yamamoto, and Hirohisa Ogawa. Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 90(1):101–112, 2007.

[18] Kamer Kaya and Ali Aydın Selçuk. Threshold cryptography based on asmuth–bloom secret sharing. *Information Sciences*, 177(19):4148–4160, 2007.

[19] PV Siva Kumar, Rajasekhara Rao Kurra, Appala Naidu Tentu, and G Padmavathi. Multi-level secret sharing scheme for mobile ad-hoc networks. *International Journal of Advanced Networking and Applications*, 6(2):2253, 2014.

[20] Qiang Li, Xiang Xue Li, Xue Jia Lai, and Ke Fei Chen. Optimal assignment schemes for general access structures based on linear programming. *Designs, Codes and Cryptography*, 74(3):623–644, 2015.

[21] Robert J. McEliece and Dilip V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[22] Maurice Mignotte. How to share a secret. In *Workshop on Cryptography*, pages 371–375. Springer, 1982.

[23] Abhishek Parakh and Subhash Kak. Space efficient secret sharing for implicit data security. *Information Sciences*, 181(2):335–341, 2011.

[24] Michaël Quisquater, Bart Preneel, and Joos Vandewalle. On the security of the threshold scheme based on the chinese remainder theorem. In *Public Key Cryptography*, volume 2274, pages 199–210. Springer, 2002.

[25] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, and Sundaram Vats. Threshold cryptography based data security in cloud computing. In *Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on*, pages 202–207. IEEE, 2015.

[26] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[27] Shyong Jian Shyu. Efficient visual secret sharing scheme for color images. *Pattern Recognition*, 39(5):866–880, 2006.

[28] Markus Stadler. Publicly verifiable secret sharing. In *Eurocrypt*, volume 96, pages 190–199. Springer, 1996.

[29] Ching-Nung Yang and Chi-Sung Laih. New colored visual secret sharing schemes. *Designs, Codes and cryptography*, 20(3):325–336, 2000.