Tightly coupled multi-group threshold secret sharing based on Chinese Remainder Theorem

Keju Meng, Fuyou Miao*, Wenchao Huang, Yan Xiong

Abstract

(t, n)-Threshold secret sharing ((t, n)-SS) scheme is a fundamental cryptographic primitive. As a special (t, n)-SS, a Multi-Level threshold Secret Sharing scheme (MLSS) divides shares into different levels. Shares at higher levels can be used at lower ones but shares of lower levels are invalid at higher ones. However, MLSS is limited in applications and vulnerable to Illegal Participant (IP) attack and t-Share Capture (SC) attack. Therefore, the paper first extends the notion of MLSS to multi-group threshold secret sharing (MGSS) to accommodate wider application scenarios. In order to cope with the 2 attacks, the paper then proposes a tightly coupled MGSS scheme based on Chinese Remainder Theorem. In the scheme, a shareholder, with only one private share, is allowed to participate in secret reconstruction of different groups. Moreover, when sufficient shareholders collaborate to recover the secret in a group, they first form a tightly coupled subgroup by constructing a randomized component each so that the secret can be recovered only if each participant has valid share and actually participates in secret reconstruction. Analyses show that the proposed scheme is capable of thwarting IP and SC attacks. Besides, the scheme is more flexible and popular in applications compared with MLSS scheme.

Key words: Chinese Remainder Theorem, Multi-group secret sharing, Tightly coupled, Random component.

1. Introduction

As fundamental cryptographic tools, (t, n)-threshold secret sharing schemes ((t, n)-SS) were proposed by Shamir [1] and Blakley [2] separately in 1979. They divides a secret s into n shares and allocates each share to a shareholder such that t or more that t shareholders can reconstruct s while less than t shareholders cannot. (t, n)-SS scheme guarantees both distributed confidentiality and robustness in keeping the secret. That is, on one hand, even if $t-1$ shareholders collude, they are unable to recover the secret; on the other hand, even if up to $(n-t)$ shareholders lose their shares, the secret can still be recovered.

Since (t, n)-SS was proposed, it has been studied in a lot of literatures [3-8]. And there are many methods to implement secret sharing. Shamir's (t, n)-SS is based on polynomial interpolation while Blakley's (t, n)-SS is based on hyperplane geometry; both Mignotte's (t, n)-SS [9] and Asmuth-Bloom's (t, n)-SS [10] are based on the Chinese Remainder Theorem (CRT). In Asmuth-Bloom (t, n)-SS, the candidates for different secrets may be not equally probable, resulting in an imperfect distribution. Therefore, Kaya and Selçuk [11] proposed a perfect scheme based on CRT which, meanwhile, narrows the secret space.

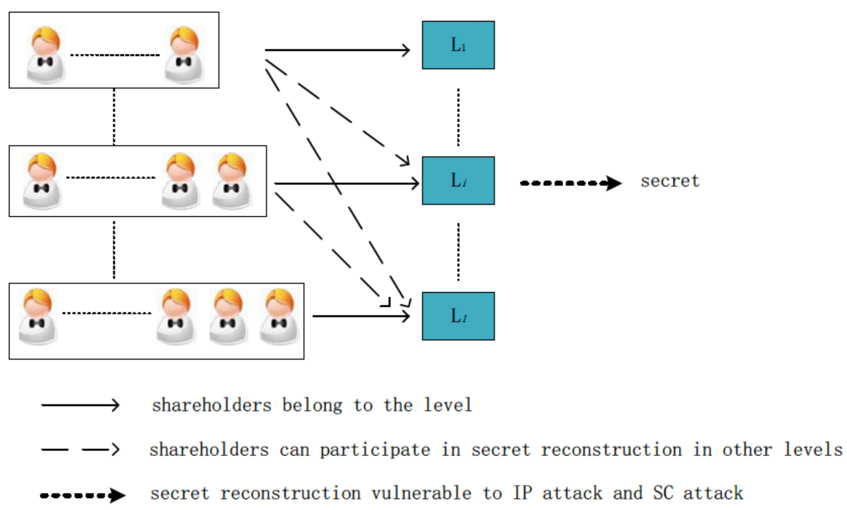

Fig 1. Model of MLSS

As a special threshold secret sharing, Multi-level threshold Secret Sharing scheme (MLSS) has been studied for many years. In MLSS, all shareholders are classified into different levels, each level with a threshold. The secret can be recovered in any level as long as sufficient number of shareholders participate in secret reconstruction in the level. Moreover, a shareholder of higher level is allowed to participate in secret recovering at lower levels. In 1989, Brickell [12] introduced a MLSS but it is

* *Corresponding author. Tel.:+86 138 6616 6896*

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

e-mail: mkj@mail.ustc.edu.cn; mfy@ustc.edu.cn; huangwc@ustc.edu.cn; yxiong@ustc.edu.cn

inefficient because it requires exponential operation to generate nonsingular matrices. Ghodosi et al. [13] proposed a perfect MLSS based on Shamir SS but it is available only when few shareholders participate in the scheme. Siva et al. [14] proposed a MLSS also based on Shamir SS, in which the number of public shares are proportional to the number of participants. Harn and Miao [15] first proposed a MLSS based on Asmuth-Bloom SS in 2014.

The following example can be used to describe an application scenario of MLSS. Suppose there are three presidents and five vice presidents in a bank, any 2 presidents or 3 vice presidents are qualified to transfer accounts. Besides, any president can lower its position as a vice president to participate in transferring accounts with other two vice presidents. But a vice president cannot raise its position as a president to do it. To be suitable for such hierarchical applications, MLSS allows a shareholder of higher level to participate in secret reconstruction at lower levels but prohibits the one in lower level joining the secret reconstruction at higher levels. As a matter of fact, if we remove the hierarchical attribute of levels in MLSS and simply consider different levels as equal groups， each with a threshold, a Multi-Group threshold Secret Sharing (MGSS) scheme can be constructed. A MGSS allows a shareholder in group A to participate in secret reconstruction of group B and may also allow the one in group B to take part in secret recovering in group A. Obviously, MGSS is the generalization of MLSS and finds more applications than the latter. Therefore, the paper will focus on the construction of MGSS scheme.

As an application scenario of MGSS, suppose that there are three business departments in a bank. Three departments have equal status and each department has the right to transfer accounts. A member in a department may be also able to work in other departments. Then, the member can participate in transferring accounts in all the departments which he/she joins in. In our MGSS, shareholders are more flexible to participate in different groups. We show that the MLSS is only a special case of MGSS.

Note that a secret in MGSS (or MLSS) is still recovered in just one group (or level), which is actually the same as (t,n)-SS in nature. So, the security of MGSS depends on (t,n) SS to large extent. In other words, if (t,n)-SS is vulnerable to some attacks, so is MGSS or MLSS. However, there exits the following 2 attacks, Illegal participant (IP) and t-Share Capture (SC) attack in (t,n) SS. To construct a desirable MGSS, both attacks have to be thwarted.

A shareholder is called participant when it participates in secret reconstruction. In IP attack, an adversary pretends a legal shareholder, but without a valid share, and participates in secret reconstruction with other t or more than t legal shareholders. 1) If all the shareholders are supposed to pool shares simultaneously, the adversary can send a wrong share to the others. When the adversary receives any t valid shares, it can compute the original secret. But the other shareholders may not obtain the correct secret because they may use the wrong share to evaluate the secret. In this case, the adversary obtains the right secret while the others may get wrong ones. 2) If a (t,n)-SS does not require all participants to release their shares at the same time, the adversary is also able to reconstruct the secret as long as it waits to receive t valid shares from the others. Having at least t shares, the adversary can forge a valid share and release it to the others. In this way, the adversary can figure out the secret or a valid share without being noticed by others. The attack model is like active attack in cryptography. Figure 2 is an example of IP attack in (t,n)-SS with $t \leq 3$.

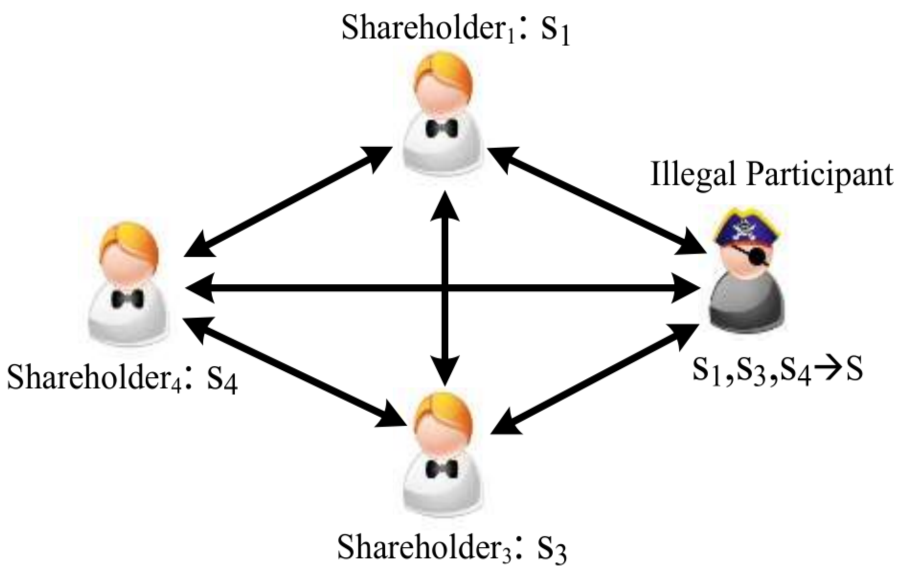

Fig 2. Illegal Participant attack in (t,n)-SS

In SC attack, an adversary cannot participate in recovering secret but aims to obtain the secret by capturing shares from legal participants. The attack model is like passive attack in cryptography. In (t,n)-SS, each pair of participants exchange shares during secret reconstruction. If $m(m \geq t)$ shareholders recover the secret, an adversary merely needs to capture any t messages from different participants, each contains a share, before obtaining the secret. Therefore, if a (t,n)-SS or MGSS scheme ensures that an adversary has to capture all the m messages before figuring out the secret, it is capable of preventing SC attack. Figure 3 shows an example with $m = 4$ participants and $t \leq 3$.

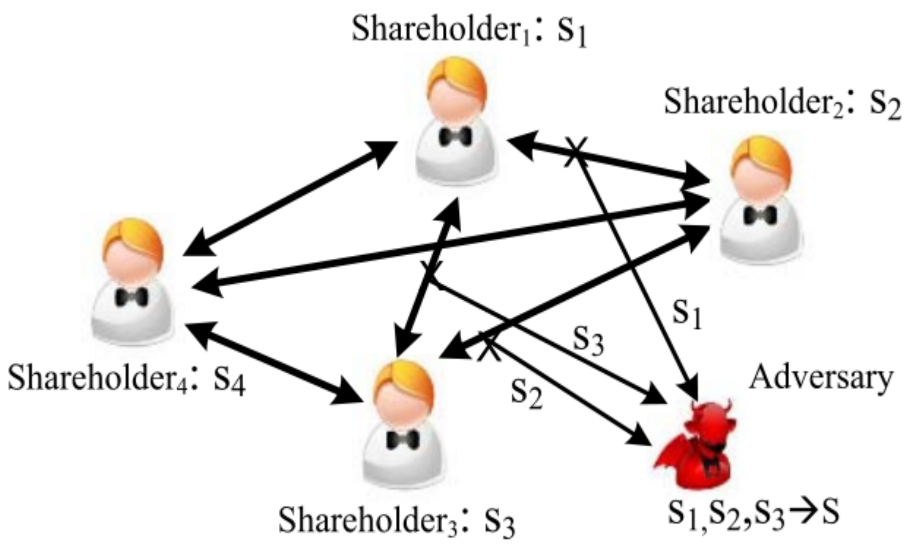

Fig 3. t-Share Capture attack in (t, n)-SS

In order to defeat IP attacks in (t, n)-SS, Chor et al. [16] proposed a notion of verifiable secret sharing (VSS). Up to now, many VSS schemes [17-21] have been proposed in the literature. Habeeb [22] gave a VSS based on non-abelian group. Mashhadi S et al. [23] proposed 2 multi-VSS schemes based on nonhomogeneous linear recursion and linear feedback shift register public-key cryptosystem respectively. Undoubtedly, VSS is able to check the validity of each share, however, they are usually more complicated in computation (e.g. depend on some hard problem in mathematics) and need more information to enable share verification.

In order to prevent SC attack, Harn [24] proposed a security (t, n)-SS using the linear combination of shares based on the property of homomorphism [25] of Lagrange interpolation polynomials. In this scheme, the dealer generates shares using k polynomials so that each shareholder has to keep k shares. During secret reconstruction, each participant releases a linear combination of its k private shares (i.e. Lagrange Component) to recover the secret. In this way, an adversary obtains the secret only when it captures each Lagrange Component from distinct participants.

For supporting the above multi-group application, we need to propose a secure MGSS scheme capable of preventing IP and SC attacks in (t, n)-SS. The proposed scheme has the following contributions.

1) It extends the notion of multilevel to multi-group and presents a more flexible and generic scheme.
2) The proposed scheme can defend IP attack, which means any participant without valid share cannot obtain the secret even if all participants are allowed to pool shares asynchronously.
3) The proposed scheme can defend SC attack, i.e., an adversary cannot obtain the secret if it fails to capture all messages exchanged among different participants during secret reconstruction.
4) Compared with related schemes, each shareholder in MGSS is allowed to keep a single private share no matter how many groups it participates in.

The rest of this paper is organized as follows. In the next section, we give the definition of tightly coupled multi-group threshold secret sharing. In Section 3, we introduce the CRT and Asmuth-Bloom SS, and review Harn-Miao MLSS. In Section 4, we propose our tightly coupled multi-group threshold secret sharing scheme. In Section 5, we prove it is correct. In Section 6, we give security analysis. The conclusion are given in Section 7.

2. Definitions

This section gives the following 2 definitions, Multi-Group threshold Secret Sharing (MGSS) and Tightly Coupled Multi-group threshold secret sharing.

2.1. Multi-group threshold secret sharing scheme

Definition 1: Multi-group threshold secret sharing scheme (MGSS)

A scheme is called multi-group threshold secret sharing scheme if it satisfies the following requirements:

1) There are totally n shareholders U_i, $i = 1,2 \dots n$, and g groups G_j, $j = 1,2 \dots g$, in the scheme. Each group has the

threshold value t_j, where $j = 1,2,\ldots,g$.

2) A shareholder U_i is originally allocated into a group G_j and keeps only one share in this group, where G_j is called the **home group** of U_i and U_i is an **aboriginal shareholder** in G_j accordingly. Futhermore, U_i may be also allowed to participate in secret reconstruction of another group $G_k, k \neq j$. In this case, U_i is called an **immigrant shareholder** of G_k.

3) In each group G_j with totally N_j shareholders (either aboriginal or immigrant), t_j or more than t_j shareholders are able to recover the secret while any less than t_j shareholders cannot obtain the secret for $t_j \leq N_j$.

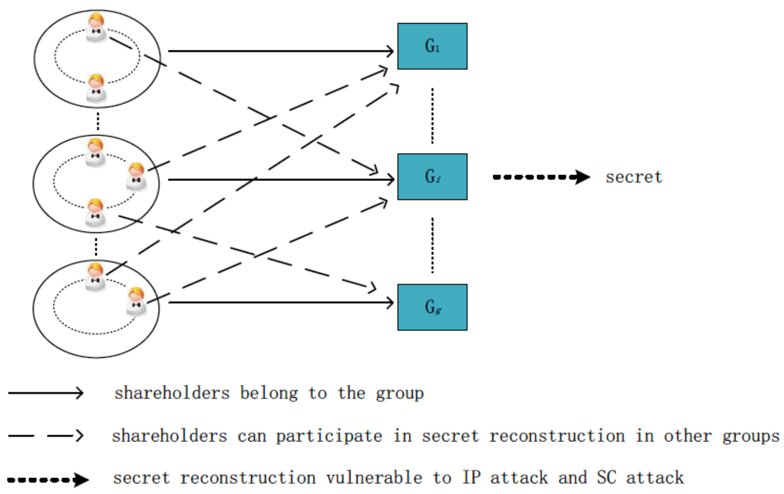

Fig 4. Model of MGSS

Remark 2.1. Fig 4 is a model of MGSS. Compared with multilevel threshold secret share scheme, multi-group scheme is more general and flexible. It breaks shareholders into flat groups instead of hierarchical levels such that groups are not necessarily hierarchical. That is, in multilevel scheme, all shareholders at a higher level are able to participate in secret reconstruction of all lower levels while shareholders at a lower level cannot do it at any higher level. In multi-group scheme, a part of shareholders in group G_i, can participate in secret reconstruction in group G_j. Conversely, some shareholders in group G_j can also do that in group G_i. Of course, there may be some groups in which shareholders from other groups are not allowed to participate in recovering the secret, but some shareholders of these groups can participate in other groups. Therefore, multi-level scheme is only a special case of multi-group scheme.

2.2. Tightly coupled multi-group threshold secret sharing scheme

In order to defeat both IP and SC attack in MGSS, any m shareholders in each group G_j, are supposed to form a tightly coupled subgroup during secret reconstruction with $t_j \leq m \leq N_j$. It means that recovering the secret requires that each of the m participants has a valid share in G_j and actually participates in secret reconstruction. Hence, we first present the notion of tightly coupled multi-group threshold secret sharing scheme.

Definition 2: Tightly Coupled Multi-Group threshold Secret Sharing scheme

A MGSS is called Tightly Coupled MGSS scheme if it satisfies the following requirements:

1) There are totally N_j shareholders (either aboriginal or immigrant) in group G_j and the threshold is t_j.

2) In each group G_j, any t_j or more than t_j shareholders can recover the secret while less than t_j shareholders cannot.

3) In each group G_j, once m, $(t_j \leq m \leq N_j)$ shareholders collaborate to recover the secret, the secret can be reconstructed only if each of them actually participates in secret reconstruction with its valid share.

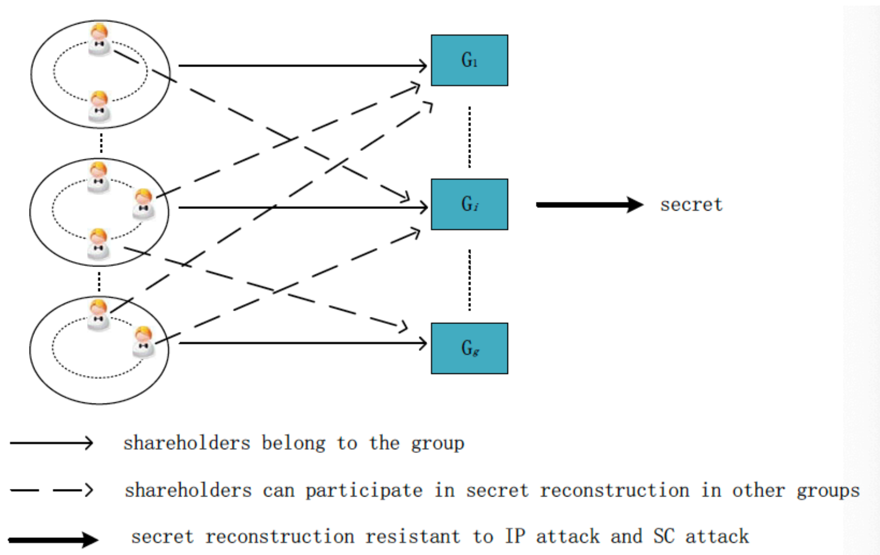

Fig 5. Model of tightly coupled MGSS

Remark 2.2 An ordinary (t,n)-SS scheme does not have the property 3), $m\,(m \geq t)$ shareholders is actually loosely coupled in secret reconstruction. That is, any t of m shareholders, instead of all, may be employed by an adversary to recover the secret. Even if there exist illegal participants without valid shares, the secret may still be recovered as long as the illegal participants do not actually participate in recovering the secret with invalid shares. Therefore, it is vulnerable to IP and SC attack.

To guarantee a MGSS scheme is resistant to the 2 attacks, i.e., possesses the property of 3), all m participants in G_j need to be closely related to each other to prevent an adversary, without a valid share, from obtaining the secret. In other words, all m out of N_j shareholders in G_j need to form a tightly coupled subgroup to force all m participants to actually participate in secret reconstruction and ensure that secret reconstruction fails as long as any participant releases an invalid share. In section 4, we will show how m participants form a tightly coupled subgroup.

3. Preliminaries

3.1. The Chinese Reminder Theorem

The Chinese Reminder Theorem (CRT) is a method of determining a larger integer from given system of congruent equations. That is, given the system of n congruent equations,

$$x = s_1 \, mod \, p_1$$
$$x = s_2 \, mod \, p_2$$
$$\vdots$$
$$\vdots$$
$$x = s_n \, mod \, p_n$$

where $\gcd(p_i, p_j) = 1$ for $i \neq j$. The value of x can be evaluated as $x = \sum_{i=1}^{n} \frac{N}{p_i} y_i s_i \; mod \, N$, where $N = \prod_{i=1}^{n} p_i$ and $\frac{N}{p_i} y_i \; mod \, p_i = 1$.

3.2. Asmuth-Bloom SS [10]

In Asmuth-Bloom (t, n)-SS, the dealer selects a prime integer p_0 and a sequence of pairwise coprime positive integers, $p_1, p_2, \ldots, p_n$ with $p_1 < p_2 < p_n$, $p_0 p_{n-t+2} \ldots p_n < p_1 p_2 \ldots p_t$ and $\gcd(p_i, p_j) = 1$ for $i \neq j$. The modulus p_i is the public information of shareholder U_i, $i = 1,2, \ldots, n$. Then, the dealer picks a secret s and random integer α in Z_{p_0} such that $x = s + \alpha p_0 < p_1 p_2 \ldots p_t$, computes and deliveries $s_i = x \; mod \, p_i$ to U_i as the share securely. If $m, (m \geq t)$ shareholders, e.g., $U_1, U_2, \ldots U_m$ want to recover the secret, each releases its share to the others. After collecting all m shares, the value of x can be evaluated as $x = \sum_{i=1}^{m} \frac{N}{p_i} y_i s_i \; mod \, N$, where $N = \prod_{i=1}^{m} p_i$ and $\frac{N}{p_i} y_i \; mod \, p_i = 1$. Finally, the secret s can be obtained as $s = x \; mod \, p_0$.

Remark 3.1. Asmuth-Bloom's scheme implements the basic function of (t, n)-SS based on CRT, but it is vulnerable to IP and SC attacks. In section 4, the tightly coupled MGSS is proposed based on Asmuth-Bloom (t, n)-SS.

3.3. Harn-Miao MLSS [15]

In Harn-Miao MLSS, all shareholders are classified into l levels L_i, $i = 1,2, \ldots, l$. L_i has the higher level than L_j when i is smaller than j. The shareholder at higher level is allowed to participate in secret reconstruction at lower levels. Each level L_i, has n_i aboriginal shareholder with the threshold, t_i $(t_i \leq \sum_{j=1}^{i} n_j)$. The Harn-Miao MLSS consists of two phases: share generation and secret reconstruction.

Share generation: The dealer selects an integer p_0 and the secret $s \in Z_{p_0}$. For each level, L_i having n_i aboriginal shareholders, the dealer selects a sequence of pairwise coprime positive integers $p_1^i, p_2^i, \ldots p_{n_i}^i$ such that $p_1^i < p_2^i < \ldots < p_{n_i}^i$, $p_0 p_{n_i-t_i+2}^i p_{n_i-t_i+3}^i \ldots p_{n_i}^i < p_1^i p_2^i \ldots p_{t_i}^i$ and $\gcd(p_0, p_k^i) = 1$, $k = 1,2, \ldots, n_i$, where p_k^i is the public modulus associated with shareholder U_k^i. For each level L_i, the dealer selects a random integer α_i such that $p_{n_i-t_i+2}^i p_{n_i-t_i+3}^i \ldots p_{n_i}^i < s + \alpha_i p_0 < p_1^i p_2^i \ldots p_{t_i}^i$ holds, which ensures the value $s + \alpha_i p_0$ falls into the t_i-shreshold range $(p_0 p_{n_i-t_i+2}^i p_{n_i-t_i+3}^i \ldots p_{n_i}^i < p_1^i p_2^i \ldots p_{t_i}^i)$. The dealer computes $s_k^i = s + \alpha_i p_0 \; mod \, p_k^i$ and sends it to shareholder U_k^i as the share secretly. In order to enable U_k^i, with the share s_k^i at L_i to participate in secret reconstruction at L_j $(i < j)$, the dealer selects a new modulus $p_{k,j}^i$ for it with $p_{t_j}^j < p_{k,j}^i < p_{n_j-t_j+2}^j$. Then, the dealer picks α_j with $p_{n_j-t_j+2}^j p_{n_j-t_j+3}^j \ldots p_{n_j}^j < s + \alpha_j p_0 < p_1^j p_2^j \ldots p_{t_j}^j$ and computes $\Delta s_{k,j}^i = (s + \alpha_j p_0 - s_k^i) \; mod \, p_{k,j}^i$. The values $(\Delta s_{k,j}^i, p_{k,j}^i)$ are the public information associated with the shareholder U_k^i at L_j. Consequently, each shareholder U_k^i keeps only one private share s_k^i, which is at the level L_i.

Secret reconstruction: The secret can be recovered if t_j or more than t_j participants, who comes from L_j or higher levels, collaborate to reconstruct the secret in any level L_j. During the secret reconstruction at level L_j, a participant U_k^i, with the original share s_k^i at higher level L_i, uses $(s_k^i + \Delta s_{k,j}^i)$ as the new share and $p_{k,j}^i$ as the new modulus. Then, the unique value $y = s + \alpha_j p_0$ can be computed by using CRT and the secret s is obtained as $s = y \bmod p_0$.

Remark 3.2. Harn-Miao MLSS achieves multilevel threshold secret sharing by a simple way based on CRT. However there are two problems with the scheme.

1) In the scheme, if U_k^i, with the share s_k^i at L_i, needs to participate in recovering the secret at L_j $(i < j)$, the dealer are required to select a modulus $p_{k,j}^i$, such that $p_{t_j}^j < p_{k,j}^i < p_{n_j - t_j + 2}^j$. However, modulus $p_{k,j}^i$ does not exist if t_j is bigger than $n_j - t_j + 2$. Moreover, the value $n_j - t_j + 2$ may be a negative number so that $p_{n_j - t_j + 2}^j$ does not exsit, because t_j is required to be smaller than $\sum_{h=1}^{j} n_h$ rather than n_j. The problem was also mentioned by Ersoy et al. in [26], but they did not give an appropriate countermeasure.
2) Like basic (t, n)-SS, Harn-Miao MLSS cannot defeat IP and SC attacks.

Therefore, the following more general and secure scheme, tightly coupled MGSS, is proposed in the next section.

4. Tightly coupled multi-group threshold secret sharing scheme

4.1. Scheme model and security goals

This section presents a tightly coupled MGSS scheme which is capable of defeating IP and SC attacks. The proposed scheme includes 3 types of entities, the Dealer, shareholders and adversaries.

Dealer: Trusted by all shareholders, the dealer is responsible for the selection of system parameters (e.g. the secret, secret space, moduli and so on) in addition to generation and delivery of shares. Suppose that there is an absolutely secure channel between the dealer and each shareholder and thus the dealer can allocate each shareholder a share securely.

Shareholder: Each shareholder receives a share from the dealer securely. In a group, each pair of shareholders keeps a private channel, through which both shareholders exchange messages (containing shares) privately during secret reconstruction. But a private channel may be cracked and thus messages (or shares) could be captured in some extreme cases. When a shareholder has received all required messages from the other participants, it recovers the secret independently. However, a shareholder may want to know shares of other shareholders. Moreover, less than t of them may try to recover the secret.

Adversary: An adversary has no valid shares but wants to obtain valid shares or the final secret. It is able to capture no more than $(m-1)$ messages in secret reconstruction if there are m shareholders recovering the secret. Moreover, an adversary may use a fake share to pretend a legal shareholder and participate in secret reconstruction with other legal shareholders.

Security goals: The core function of secret sharing is to protect the secret from exposure to adversaries in nature, therefore, our scheme guarantees that an adversary, without any valid share, cannot obtain the secret in any group. In the aforementioned attack model, our scheme aims to achieve the following security goals. It is similar to cheating immune secret sharing described by Martin [27].

(1) In each group G_i, any t_i or more than t_i shareholders can recover the secret if all of them have valid shares while any less than t_i shareholders cannot recover the secret.

(2) Anyone, who does not participate in the secret reconstruction, cannot obtain the secret by capturing no more than $(m-1)$ messages when m $(m \geq t_i)$ shareholders recover the secret in group G_i. In other words, it should be resistant against SC attack.

(3) When m $(m \geq t_i)$ participants collaborate to recover the secret in group G_i, they can obtain the secret only if each of the m participants has a valid share. In other words, anyone cannot obtain the secret if some participant has not a valid share. This is to guarantees the scheme can defeat IP attack.

4.2. Symbol definition

Before describing the scheme, we first define some important notations as listed in Table 1.

4.3. Our scheme

In the proposed scheme, shareholders are divided into g groups G_i, $i = 1,2 \dots g$. Each shareholder keeps only one share in home group. Define n_i and N_i as the numbers of aboriginal shareholders and all shareholders in G_i respectively. Each group G_i has the threshold t_i with $1 \leq n_i \leq N_i$, $1 \leq t_i \leq N_i$. In fact, there is no clear relation between n_i and t_i. An aboriginal shareholder or immigrant shareholder of G_i is uniformly called **participant** if it participates in secret reconstruction in the group. By using the basic (t, n)-SS, the secret can be recovered if there are t_i or more than t_i participants in group G_i.

Table 1: Notations

Symbol	Notion
G_i	the i^{th} group
N_i	the numbers of all shareholders in group G_i
n_i	the numbers of aboriginal shareholders in group G_i
t_i	the threshold in group G_i
U_k^i	the k^{th} aboriginal shareholder in group G_i
s	the original secret
s_k^i	the private share of U_k^i in home group G_i
p_k^i	aboriginal modulus of U_k^i in group G_i
$s_{k,i}^j$	immigrant share of U_k^i used in group G_j
$p_{k,i}^j$	immigrant modulus of U_k^i used in group G_j
$\Delta s_{k,i}^j$	public difference between s_k^i and $s_{k,i}^j$

In the following part, the tightly coupled MGSS scheme is proposed based on Asmuth-Bloom (t, n)-SS, it includes 3 phases: 1) share generation, 2) share protection and 3) secret reconstruction.

1) Share generation: The dealer selects a prime p_0 and define Z_{p_0} as the secret space. For each group G_i, the dealer selects a sequence of pairwise coprime positive integers $p_1^i < p_2^i < \cdots < p_{N_i}^i$, such that $(p_0)^2 p_{N_i-t_i+2}^i p_{N_i-t_i+3}^i \dots p_{N_i}^i < p_1^i p_2^i \dots p_{t_i}^i$, $N_i(p_0)^3 < p_1^i(p_0 - 1)$ and $\gcd(p_0, p_k^i) = 1$, where $k = 1,2 \dots N_i$, $(p_0)^2$ is the square of p_0 and $(p_0)^3$ is the cube of p_0. The dealer first chooses n_i out of the N_i integers and allocates each to an aboriginal shareholder as the aboriginal modulus. Accordingly, the other integers are used as immigrant moduli of immigrant shareholders of the group. In order for not leaking information of the share, an immigrant shareholder of G_i must have a modulus smaller than the one in its home group. Then, the dealer selects the secret $s \in Z_{p_0}$ and a random integer α_i, such that $p_{N_i-t_i+2}^i p_{N_i-t_i+3}^i \dots p_{N_i}^i < y_i = s + \alpha_i p_0 < (p_1^i p_2^i \dots p_{t_i}^i)/p_0$ holds to ensure the value y_i falls into the t_i-threshold range $(p_{N_i-t_i+2}^i p_{N_i-t_i+3}^i \dots p_{N_i}^i, (p_1^i p_2^i \dots p_{t_i}^i)/p_0)$. Finally, the dealer computes $s_k^i = y_i \, mod \, p_k^i$ and sends it to shareholder U_k^i as the share securely, thus U_k^i is the aboriginal shareholder of G_i.

If U_k^i, an aboriginal shareholder of G_i, is allowed to participate in recovering the secret in group G_j, $j \neq i$, the dealer needs to generate extra information related to G_j for the shareholder. Concretely, the dealer selects a random integer α_j such that $p_{N_j-t_j+2}^j p_{N_j-t_j+3}^j \dots p_{N_j}^j < y_j = s + \alpha_j p_0 < (p_1^j p_2^j \dots p_{t_j}^j)/p_0$ and computes the value $\Delta s_{k,i}^j = (s + \alpha_j p_0 - s_k^i) mod \, p_{k,i}^j$, where $p_{k,i}^j$ is picked from the sequence $p_1^j, p_2^j \dots p_{N_j}^j$ with $p_{k,i}^j < p_k^i$. Then, the dealer makes $\Delta s_{k,i}^j$ and $p_{k,i}^j$ publicly known. Obviously, when U_k^i participates in secret reconstruction as the immigrant shareholder in G_j, it uses $p_{k,i}^j$ as the immigrant modulus and $s_{k,i}^j = (s_k^i + \Delta s_{k,i}^j) = (s + \alpha_j p_0) \mathrm{mod} \, p_{k,i}^j$ as the new share in group G_j.

Remark 4.1. Although the dealer publishes some public values $\Delta s_{k,i}^j$, no information about s can be derived from them. The reason is that:

$$
\begin{aligned}
\Delta s_{k,i}^j &= (s + \alpha_j p_0 - s_k^i) mod \, p_{k,i}^j \\
&= (s + \alpha_j p_0 - (s + \alpha_i p_0) mod p_k^i) mod \, p_{k,i}^j \\
&= (s + \alpha_j p_0 - s - \alpha_i p_0 + \beta p_k^i) mod \, p_{k,i}^j \\
&= ((\alpha_j - \alpha_i) p_0 + \beta p_k^i) mod \, p_{k,i}^j \qquad (4-1)
\end{aligned}
$$

where β is a random integer. Obviously, the secret s is not included in equation (4-1), which means that $\Delta s_{k,i}^j$ does not reveal information about s.

Remark 4.2. In our scheme, the dealer selects many moduli in group G_j, uses some of them to compute shares for immigrant shareholders and guarantee there exists $p_{k,j}^i$ available with $p_{k,j}^i > p_k^i$. This ensures that the public information $\Delta s_{k,i}^j$ does not reveal information about $s_{k,i}^j$. Since a shareholder keeps only one private share while both $\Delta s_{k,i}^j$ and $p_{k,i}^j$ are made public, an adversary will obtain an interval $[\Delta s_{k,i}^j, \Delta s_{k,i}^j + p_k^i]\ mod\ p_{k,i}^j$ about the new share $s_{k,i}^j$ in G_j. However, the immigrant share should be over $[0, p_{k,i}^j)$ for the adversary. If $p_{k,j}^i > p_k^i$ holds, $[\Delta s_{k,i}^j, \Delta s_{k,i}^j + p_k^i]\ mod\ p_{k,i}^j$ is a subrange in $[0, p_{k,i}^j)$. In other words, the adversary narrows the range of $s_{k,i}^j$. Therefore, the aboriginal modulus p_k^i should be larger than immigrant modulus $p_{k,j}^i$. In more detail, the only problem is that the value $s_{k,i}^j$ may not be a uniform distribution in the interval $Z_{p_{k,i}^j}$. The probability of values in the interval $[\Delta s_{k,i}^j, \Delta s_{k,i}^j + (p_k^i - 1)\ mod\ p_{k,i}^j]\ mod\ p_{k,i}^j$, is $\lceil p_k^i / p_{k,i}^j \rceil / p_k^i$, and the probability of the other values is $\lfloor p_k^i / p_{k,i}^j \rfloor / p_k^i$. Even so, the adversary cannot narrow the range of $s_{k,i}^j$ by the public information.

2) Share protection: Suppose m $(t_i \le m \le N_i)$ shareholders participate in recovering the secret in group G_i. As an immigrant shareholder among them U_k^j, with the share s_k^j in home group G_j, computes its new share $s_{k,j}^i = s_k^j + \Delta s_{k,j}^i$ in G_i before secret reconstruction. In this case, each participant, either aboriginal or immigrant shareholder, has a share in G_i. For simplicity, we rename each of the m participants as U_{m_k} with the share s_{m_k} and modulus p_{m_k}, $k = 1,2 \ldots m$. Before secret reconstruction, each participant, e.g. U_{m_k} constructs a randomized component $s_{m_k}^* = \left(s_{m_k}\left(\frac{N}{p_{m_k}}\right)a_{m_k} + r_{m_k}\left(\frac{N}{p_{m_k}}\right)p_0\right) mod\ N$, where $N = \prod_{k=1}^m p_{m_k}$, $(\frac{N}{p_{m_k}})a_{m_k}\ mod\ p_{m_k} = 1$ and r_{m_k} is a random integer selected by U_{m_k} in Z_{p_0}.

Remark 4.3. To defeat IP and SC attacks, each shareholder e.g. U_{m_k} constructs a randomized component $s_{m_k}^*$ with its share s_{m_k}, random integer $r_{m_k} \in Z_{p_0}$ and all participants' moduli before secret reconstruction. Obviously, the randomized component $s_{m_k}^*$ servers as 2 functions, one is to protect the share s_{m_k} and the other is to bind all participants together. That is because each participant's randomized component, e.g., $s_{m_k}^*$ contains N, the product of all the moduli and thus the share s_{m_k} cannot be separated from the component $s_{m_k}^*$ without knowing the random number r_{m_k}. In this way, all m participants form a tightly coupled subgroup.

3) **Secret reconstruction:** Each participant e.g., U_{m_k} sends its component $s_{m_k}^*$ to the other $(m-1)$ participants in private channels. On receiving all components, U_{m_k} obtains the secret s by computing $s = \sum_{k=1}^m s_{m_k}^*\ mod\ N\ mod\ p_0$. Once the secret is recovered in a group, the secret is not classified any more because the scheme is a single SS scheme.

5. Correctness analysis

In the proposed scheme, if m $(t_i \le m \le N_i)$ participants are able to recover the secret in group G_i, it means the secret $s = \sum_{k=1}^m s_{m_k}^*\ mod\ N\ mod\ p_0$. Now, let suppose $p_{m_1} < p_{m_2} < \cdots < p_{m_m}$ without losing generality, we prove the equation in 2 steps.

Proof.	**Remark:**
(1) $\boldsymbol{y_i + \sum_{k=1}^m r_{m_k}(N/p_{m_k})\, p_0} < N$	
$y_i + \sum_{k=1}^m r_{m_k}(N/p_{m_k})p_0$	
$< y_i + \sum_{k=1}^m p_0^2 N/p_{m_k}$	$remark 5.1: r_{m_k} \in Z_{p_0}$
$< y_i + m p_0^2 N/p_{m_1}$	$remark 5.2: p_{m_1} \ge\ p_1^i, where\ p_1^i\ is\ the\ smallest\ moudle\ in\ G_i$
$< y_i + N_i p_0^2 N/p_{m_1}$	
$< y_i + (p_0 - 1)N/p_0$	$remark 5.3: N_i p_0^3 < p_1^i(p_0 - 1)$
$< N/p_0 + (p_0 - 1)N/p_0$	$remark 5.4: y_i < (p_1^i p_2^i \ldots p_{t_i}^i)/p_0$
$< N$	

(2) $\boldsymbol{\sum_{k=1}^m s_{m_k}^*\ mod\ N\ mod\ p_0 = s}$

$\sum_{k=1}^m s_{m_k}^*\ mod\ N\ mod\ p_0$

$$= \{\sum_{k=1}^{m}(s_{m_k}(N/p_{m_k})a_{m_k} + r_{m_k}(N/p_{m_k})p_0) \ mod\ N\ \} mod\ p_0$$

$$= \left\{\left(\sum_{k=1}^{m} s_{m_k}\left(\frac{N}{p_{m_k}}\right)a_{m_k}\ mod\ N + \sum_{k=1}^{m} r_{m_k}\left(\frac{N}{p_{m_k}}\right)p_0\right)\ mod\ N\right\} mod\ p_0$$

$$= \{\left(y_i + \sum_{k=1}^{m} r_{m_i}\left(\frac{N}{p_{m_k}}\right)p_0\right)\ mod\ N\ \} mod\ p_0$$

$$= (s + \alpha p_0 + \sum_{k=1}^{m} r_{m_i}(N/p_{m_k})p_0)\ \ mod\ p_0$$

$$= s$$

6. Security analysis

This section aims to prove that our scheme achieve the goals listed in **4.1.** We give the following 3 theorems to prove the security. Not that the secret is selected from Z_{p_0}, thus an event is deemed to be impossible if the probability of its occurrence is equal or less than $1/p_0$.

Theorem 6.1. *In each group G_i, any t_i or more than t_i shareholders can recover the secret if all of them use valid shares, while less than t_i shareholders cannot recover the secret.*

Proof. The proof of the former part has been given in correctness analysis. Thus, we only need to prove the later part, that is, less than t_i shareholders cannot recover the secret in G_i.

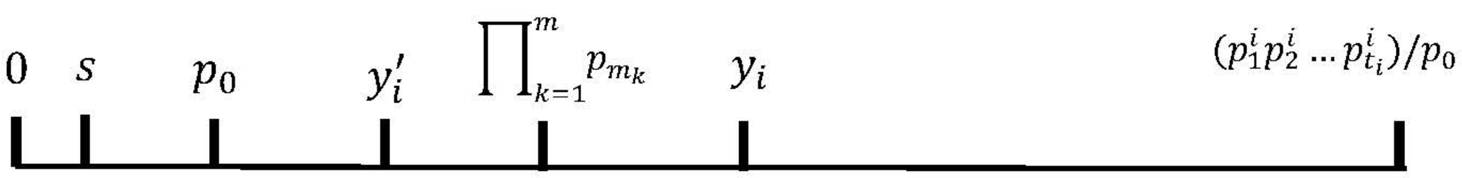

Fig 3. Relationship among parameters in Theorem 6.1

Let us consider the extreme case of $m = (t_i - 1)$ legal shareholders conspiring to recover the secret. Each participant e.g. U_{m_k} sets the random number $r_{m_k} = 0$ in constructing its component. In other words, they pool their shares instead of randomized component together to recover the secret. Then, each shareholder has $m = (t_i - 1)$ shares and thus can compute $y_i' = \sum_{k=1}^{m} s_{m_k}(N/p_{m_k})a_{m_k}\ mod\ N$ by CRT, where $N = \prod_{k=1}^{m} p_{m_k}$ and $(\frac{N}{p_{m_k}})a_{m_k} \mathrm{mod}\ p_{m_k} = 1$. Obviously, we have y_i $=y_i' + lN$ thanks to CRT, where l is an integer. Then l falls in the integer set L, where $L = (0, (p_1^i p_2^i \dots p_{t_i}^i)/Np_0)$. The number of possible candidates for l, denoted by N_l, is bigger than p_0 because of $N\_l = (p_1^i p_2^i \dots p_{t_i}^i)/(Np_0) > (p_1^i p_2^i \dots p_{t_i}^i)/(p_0 p_{N_i - t_i + 2}^i p_{N_i - t_i + 3}^i \dots p_{N_i}^i) > p_0$. So, the probability of less than t_i shareholders recovering the secret is no more than$1/p_0$. It means that the $t_i - 1$ participants cannot obtain more information than they directly guess the secret within the secret space.

Theorem 6.2. *Our scheme can defend SC attack. That is, an adversary cannot obtain the secret even if it captures up to* $m - 1$ *components when m $(m \geq t_i)$ shareholders recover the secret in group G_i.*

Proof. Suppose that an adversary has captured $(m - 1)$ messages sent by different shareholders in secret reconstruction. There are two methods of attempting to recover the secret.

(1) If $m = t_i$, the adversary capture $(t_i - 1)$ components. It cannot obtain the secret obviously. If $m > t_i$, the adversary may attempt to obtain t_i original shares and use CRT to figure out the secret. However, only knowing a component $s_{m_k}^*$, the adversary has the probability $1/p_0$ to derive the original share s_{m_k}. The proof is given as follows.

Due to $s_{m_k}^* = \left(s_{m_k}\left(\frac{N}{p_{m_k}}\right)a_{m_k} + r_{m_k}\left(\frac{N}{p_{m_k}}\right)p_0\right) mod\ N$, the values, N/p_{m_k} and a_{m_k} can be computed by anyone and p_0 and p_{m_k} are public.

$$s_{m_k}^* = (s_{m_k}\left(\frac{N}{p_{m_k}}\right)a_{m_k} + r_{m_k}\left(\frac{N}{p_{m_k}}\right)p_0) mod\ N \quad (6\text{-}1)$$

$$=> \quad \left(\frac{N}{p_{m_k}}\right)a_{m_k}s_{m_k} = \left(s_{m_k}^* - r_{m_k}\left(\frac{N}{p_{m_k}}\right)p_0\right) modN \quad (6\text{-}2)$$

$$=> \quad a_{m_k}s_{m_k} = (s_{m_k}' - r_{m_k}p_0) mod\ p_{m_k} \quad (6\text{-}3)$$

It is followed by $a_{m_k} s_{m_k} = (s'_{m_k} - r_{m_k} p_0) mod\ p_{m_k}$ because of $\left(\frac{N}{p_{m_k}}\right) | s^*_{m_k}$, $\gcd\left(\frac{N}{p_{m_k}}, p_{m_k}\right) = 1$ and $\gcd(a_{m_k}, p_{m_k}) = 1$, where $s'_{m_k} N/p_{m_k} = s^*_{m_k}\ mod\ N$. As the result, each different r_{m_k} produces a unique value of s_{m_k} for given s'_{m_k} in (6-3). Since r_{m_k} is randomly selected in Z_{p_0}, the probability of deriving the original share s_{m_k} is $1/p_0$ with the knowledge $s^*_{m_k}$.

(2) Without losing the generality, suppose the adversary has the $(m-1)$ components $\{s^*_{m_1}, s^*_{m_2}, \dots s^*_{m_{m-1}}\}$ available. Although the adversary cannot derive s_{m_k} from $s^*_{m_k}$, it still can recover the secret if it obtains the following equation from $s^*_{m_k}$

$$c_{m_k} = \frac{s^*_{m_k}}{p_{m_m}} = (s_{m_k}\left(\frac{N'}{p_{m_k}}\right) a'_{m_k} + r'_{m_k}\left(\frac{N'}{p_{m_k}}\right) p_0) mod\ N'$$

where $N' = \frac{N}{p_{m_m}}$, $a'_{m_k}\frac{N'}{p_{m_k}} = 1\ mod\ p_{m_k}$, $r'_{m_k} = r_{m_k}\frac{a'_{m_k}}{a_{m_k}}$. If r'_{m_k} is an integer, $r'_{m_k}\left(\frac{N'}{p_{m_k}}\right) p_0$ is still integral multiple of p_0, which means that the adversary can use the $(m-1)$ new components $c_{m_1}, c_{m_2}, \dots, c_{m_{t-1}}$ to recover the secret. Therefore, we should prove that r'_{m_k} is not an integer. From the definitions of a_{m_k} and a'_{m_k}, we have

$$a_{m_k}\frac{N}{p_{m_k}} = 1\ mod\ p_{m_k} \quad => \ a_{m_k}\frac{N}{p_{m_k}} = 1 + \varsigma_1 p_{m_k} \qquad (6\text{-}4)$$

$$a'_{m_k}\frac{N'}{p_{m_k}} = 1\ mod\ p_{m_k} \quad => \ a'_{m_k}\frac{N'}{p_{m_k}} = 1 + \varsigma_2 p_{m_k} \qquad (6\text{-}5)$$

Let (6-5) divide (6-4), and we get

$$\frac{a'_{m_k} N'}{a_{m_k} N} = \frac{1+\varsigma_2 p_{m_k}}{1+\varsigma_1 p_{m_k}} \quad => \ \frac{a'_{m_k}}{a_{m_k}} = \frac{1+\varsigma_2 p_{m_k}}{1+\varsigma_1 p_{m_k}} p_{m_m} \qquad (6\text{-}6)$$

In (6-6), $\frac{a'_{m_k}}{a_{m_k}}$ is an integer only if $(1+\varsigma_1 p_{m_k}) | (1+\varsigma_2 p_{m_k})$ due to p_{m_m} is a prime number. However, if $(1+\varsigma_1 p_{m_k}) | (1+\varsigma_2 p_{m_k})$ holds, $1+\varsigma_2 p_{m_k}$ must be no less than $1+\varsigma_1 p_{m_k}$. Because ς_1 and ς_2 are random integer in Z_N and $Z_{N'}$, the probability of $1+\varsigma_2 p_{m_k} \geq 1+\varsigma_1 p_{m_k}$ is less than $\frac{2}{N'}$, where $\frac{2}{N'} < \frac{1}{p_0}$. Therefore, the probability of adversary uses the $(m-1)$ new components $c_{m_1}, c_{m_2}, \dots, c_{m_{t-1}}$ to recover the secret is less than $\frac{1}{p_0}$.

Besides, the adversary can directly compute a value $s' = \sum_{k=1}^{m-1} s^*_{m_k}\ mod\ N\ mod\ p_0$, where $N = \prod_{k=1}^{m} p_{m_k}$. If s' happens to be equal to the secret s, the adversary can figure out the secret. Let consider the probability of $s' = s$.

$$s' = s$$

$$<=> \ \sum_{k=1}^{m-1} s^*_{m_k}\ mod\ N\ mod\ p_0 = \sum_{k=1}^{m} s^*_{m_k}\ mod\ N\ mod\ p_0 \qquad (6\text{-}7)$$

$$<=> \ \left(s^*_{m_m} + \sum_{k=1}^{m-1} s^*_{m_k}\ mod\ N\right) mod\ N - \sum_{k=1}^{m-1} s^*_{m_k}\ mod\ N = \gamma' p_0 \quad \gamma' \in \mathrm{Z} \qquad (6\text{-}8)$$

$$<=> \ \frac{N}{p_{m_m}}\left(s_{m_m} a_{m_m} + r_{m_m} p_0\right) mod\ N = \gamma' p_0 \quad \gamma' \in \mathrm{Z} \qquad (6\text{-}9)$$

$$<=> \ \left(s_{m_m} a_{m_m} + r_{m_m} p_0\right) mod\ p_{m_m} = \gamma p_0 \quad \gamma \in \mathrm{Z} \qquad (6\text{-}10)$$

For fixed value of r_{m_m}, the left side of (6-9) varies within the range of N with p_{m_m} discrete values because of $s_{m_m} \in Z_{p_{m_m}}$. Due to $\gcd\left(\frac{N}{p_{m_m}}, p_0\right) = 1$, (6-9) is equivalent to (6-10) with integer $\gamma' = \gamma\frac{N}{p_{m_m}}$. For an adversary, without knowing s_{m_m} and r_{m_m}, the left side of (6-10) is indistinguishable from a random number uniformly distributed in $Z_{p_{m_m}}$. In this case, the number of possible γ is at most $\lfloor p_{m_m}/p_0 \rfloor + 1$. Consequently, the probability of recovering the secret from $(m-1)$ components is $(\left\lfloor\frac{p_{m_m}}{p_0}\right\rfloor + 1)/\ p_{m_m} \approx 1/\ p_0$.

Theorem 6.3. *Our scheme can defeat IP attack. When* m $(m \geq t_i)$ *participants attempt to recover the secret in group* G_i*, they can obtain the secret only if each of the* m *participants has a valid share. In other words, anyone cannot obtain the secret if there is participant without a valid share.*

Proof. Suppose that there are m $(m \geq t_i)$ participants recover the secret in group G_i. However, one of them is an illegal participant, pretending to be a legal shareholder and using a mendacious component $s'_{m_m} = \left(\left(s_{m_m} + \Delta s_{m_m}\right)\left(\frac{N}{p_{m_m}}\right) a_{m_m} + r_{m_m}\left(\frac{N}{p_{m_m}}\right) p_0\right) mod\ N$ to participate in recovering the secret, where $\Delta s_{m_m} \in Z_{p_{m_m}}$ is the difference between the fake share and the correct share s_{m_m}.

(1) A legal shareholder will get $(m-1)$ valid components and a fake component. It computes a value $s' = (s'_{m_m} + \sum_{k}^{m-1} s^*_{m_k})\ mod\ N\ mod\ p_0$. Then, let compute the probability of $s' = s$.

$$s' = s$$

$$<=> \quad (s'_{m_m} + \sum_{k=1}^{m-1} s^*_{m_k})\, mod\ N\ mod\ p_0 = \sum_{k=1}^{m} s^*_{m_k}\ mod\ N\ mod\ p_0 \quad (6\text{-}11)$$

$$<=> \quad (\Delta s_{m_m}\left(\frac{N}{p_{m_m}}\right) a_{m_m}\ mod\ N\ mod\ p_0 + \sum_{k=1}^{m} s^*_{m_k} - \sum_{k=1}^{m} s^*_{m_k})\, mod\ N\ mod\ p_0 = 0 \quad (6\text{-}12)$$

$$<=> \quad \frac{N}{p_{m_m}} \Delta s_{m_m} a_{m_m}\ mod\ N = \mu' p_0 \qquad \mu' \in Z \qquad (6\text{-}13)$$

$$<=> \quad \Delta s_{m_m} a_{m_m}\ mod\ p_{m_m} = \mu p_0 \quad \mu \in Z \quad (6\text{-}14)$$

Similarly, because of $\gcd\left(\frac{N}{p_{m_m}}, p_0\right) = 1$, (6-13) is equivalent to (6-14) with integer $\mu' = \mu \frac{N}{p_{m_m}}$. Note that Δs_{m_m} is actually a random number uniformly distributed in $Z_{p_{m_m}}$ since the illegal participant does not know the true share s_{m_m}. Therefore, the number of possible μ in (6-14) is also no more than $\lfloor p_{m_m}/p_0 \rfloor + 1$. That is, the probability of recovering the secret from $(m-1)$ valid components and a fake component is $(\left\lfloor \frac{p_{m_m}}{p_0} \right\rfloor + 1)/\, p_{m_m} \approx 1/\, p_0$.

(2) For the illegal participant, it can receive $(m-1)$ components from legal participants. It cannot obtain t_i valid original shares, the proof is given in theorem 6.2-(1). If the illegal participant only uses the $(m-1)$ valid components, it cannot obtain the secret. The proof is also given in theorem 6.2-(2). If the illegal participant uses all the $(m-1)$ valid components and its fake component to recover the secret, it computes just like a legal shareholder. The probability also equals about $1/\, p_0$ and it is given in theorem 6.3-(1).

Discussion. For improving the security of our scheme, we introduce the other notion of tightly coupled. As a significant side effect, the secret range has to be narrower. Because in Harn-Miao MLSS scheme, the secret s is in Z_{p_0}, where $p_0 p^i_{n_i-t_i+2} p^i_{n_i-t_i+3} \cdots p^i_{n_i} < p^i_1 p^i_2 \cdots p^i_{t_i}$. But in our scheme, p_0 has to satisfy $p_0^2 p^i_{N_i-t_i+2} p^i_{N_i-t_i+3} \cdots p^i_{N_i} < p^i_1 p^i_2 \cdots p^i_{t_i}$ and $N_i p_0^3 < p^i_1 (p_0 - 1)$. In other words, the information rate of our scheme is much less than it of Harn-Miao MLSS, and thus our scheme is not so efficient as Harn-Miao MLSS.

7. Numerical Example

To make our scheme more understandable, we use the following numerical example to illustrate our proposed scheme.

Suppose that there are 3 groups G_1, G_2 and G_3. U^1_1 and U^1_2 are two aboriginal shareholders in G_1. Then, U^1_2 can participate in secret reconstruction in G_2. Besides, G_2 has two aboriginal shareholders U^2_1 and U^2_2, where U^2_2 is also an immigrant shareholder in G_3. The home group of U^3_2 and U^3_3 is G_3. And U^3_3 is allowed to participate in recovering the secret in group G_1. In this case, each group has totally three shareholders. Let all the three groups are $(2,3)$ threshold. Obviously, the scheme is MGSS instead of MLSS since there is no hierarchical attribute of different groups.

The dealer picks a prime number $p_0 = 7$ and the secret $s = 5$. In group G_1, the dealer selects 3 pairwise coprime integers $p^1_1 = 179$, $p^1_2 = 191$ and $p^1_3 = 193$, where p^1_1 and p^1_2 are associated with U^1_1 and U^1_2, while p^1_3 is a valid modulus of the immigrant shareholder U^3_3, i.e., $p^3_{3,3} = p^1_3$. p_0, p^1_1, p^1_2 and p^1_3 satisfy $p_0^2 p^1_3 < p^1_1 p^1_2$ and $3p_0^3 < p^1_1(p_0 - 1)$, where p_0^2 is the square of p_0 and p_0^3 is the cube of p_0. Then, the dealer selects $\alpha_1 = 512$ such that $p^1_3 < y_1 = s + \alpha_1 p_0 < p^1_1 p^1_2 / p_0$. The private share s^1_1 and s^1_2 of U^1_1 and U^1_2 are computed as $s^1_1 = y_1\ mod\ p^1_1 = 9$ and $s^1_2 = y_1\ mod\ p^1_2 = 151$.

In group G_2, the dealer selects $p^2_1 = 173$, $p^2_2 = 179$ and $p^2_3 = 181$, where p^2_1 and p^2_2 are associated with U^2_1 and U^2_2. Besides, U^1_2 can use p^2_3 participate in secret reconstruction in G_2 due to $p^2_3 < p^1_2$, i.e., $p^2_{2,1} = p^2_3$. Then, the dealer selects $\alpha_2 = 337$ such that $p^2_3 < y_2 = s + \alpha_2 p_0 < p^2_1 p^2_2 / p_0$. The private share s^1_1 and s^1_2 are $s^2_1 = y_2\ mod\ p^2_1 = 115$ and $s^2_2 = y_2\ mod\ p^2_2 = 37$. And the public value of U^1_2 is computed as $\Delta s^2_{2,1} = (s + \alpha_2 p_0 - s^1_2)\, mod\ p^2_{2,1} = 41$.

In group G_3, the dealer selects $p^3_1 = 173$, $p^3_2 = 179$ and $p^3_3 = 197$, where p^3_1 belongs to the immigrant shareholder U^2_2, i.e., $p^3_{2,2} = p^3_1$, and p^3_2 and p^3_3 are associated with aboriginal shareholders U^3_2 and U^3_3. Then, the dealer selects $\alpha_3 = 459$ such that $p^3_3 < y_3 = s + \alpha_3 p_0 < p^3_1 p^3_2 / p_0$. The private share s^3_2 and s^3_3 are $s^3_2 = y_3\ mod\ p^3_2 = 175$ and $s^3_3 = y_3\ mod\ p^3_3 = 66$. Besides, the public value of U^2_2 and U^3_3 are computed as $\Delta s^3_{2,2} = (s + \alpha_3 p_0 - s^2_2)\, mod\ p^3_{2,2} = 67$ and $\Delta s^1_{3,3} = (s + \alpha_1 p_0 - s^3_3)\, mod\ p^1_{3,3} = 122$.

Suppose that U^1_2 and U^2_2 work together to recover the secret in group G_2. U^1_2 is supposed to use its private share s^1_2 and public value $\Delta s_{2,1}^2$ to compute its new share $s_{2,1}^2 = (s_2^1 + \Delta s_{2,1}^2) mod\, p_{2,1}^2 = 11$. Let remark the two shareholders as U_{2_1} and U_{2_2}. And their shares $s_{2,1}^2$, s_2^2, $p_{2,1}^2$ and p_2^2 are remarked as $s_{2_1} = 11$, $s_{2_2} = 37$, $p_{2_1} = 181$ and $p_{2_2} = 179$. Then, U_{2_1} selects a random integer $r_{2_1} = 3$ to constructs a randomized component $s_{2_1}^* = \left(s_{2_1}\left(\frac{N}{p_{2_1}}\right)a_{2_1} + r_{2_1}\left(\frac{N}{p_{2_1}}\right)p_0\right) modN = 18974$, where $N = p_{2_1} * p_{2_2} = 32399$, $a_{2_1} = 90$ such that $(\frac{N}{p_{2_1}})a_{2_1}\, mod\, p_{2_1} = 1$. As the same way, U_{2_1} selects a random integer $r_{2_1} = 6$ to constructs its randomized component $s_{2_1}^* = 27150$. Finally, the secret s can be evaluated as $s = (s_{2_1} + s_{2_2}) modNmodp_0 = 46124mod32399mod7 = 13725mod7 = 5$.

8. Conclusion

To make multilevel threshold secret sharing (MLSS) more flexible and popular in application, the paper presents first the notion of multi-group threshold secret sharing (MGSS), which allows a shareholder of one group to participate in secret reconstruction in another group without hierarchical limitation. However, threshold secret sharing schemes are vulnerable to IP and SC attacks. To construct MGSS scheme resistant to both attacks, the paper further puts forward the notion of tightly coupled MGSS and constructs a CRT-based tightly coupled MGSS scheme accordingly. In the scheme, a shareholder may participate in secret reconstruction in multiple groups while keeps only one private share. Moreover, when sufficient number of shareholders collaborate to recover the secret in a group, they first form a tightly coupled subgroup by producing a randomized component with the share, such that the secret can be recovered only if all shareholders have valid shares in the group and actually participate in secret reconstruction. Therefore, the proposed tightly couple MGSS scheme is not only resistant to IP and SC attacks but also more flexible and popular in applications.

Acknowledgement

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

Reference

[1] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[2] Blakley G R. Safeguarding cryptographic keys[J]. Proc. of the National Computer Conference1979, 1979, 48: 313-317.

[3] Padró C, Vázquez L, Yang A. Finding lower bounds on the complexity of secret sharing schemes by linear programming[J]. Discrete Applied Mathematics, 2013, 161(7-8): 1072-1084.

[4] Halpern J, Teague V. Rational secret sharing and multiparty computation[C]//Proceedings of the thirty-sixth annual ACM symposium on Theory of computing. ACM, 2004: 623-632.

[5] D'Arco P, Kishimoto W, Stinson D R. Properties and constraints of cheating-immune secret sharing schemes[J]. Discrete applied mathematics, 2006, 154(2): 219-233.

[6] Yan X, Liu X, Yang C N. An enhanced threshold visual secret sharing based on random grids[J]. Journal of Real-Time Image Processing, 2018, 14(1): 61-73.

[7] Carlet C, Ding C, Yuan J. Linear codes from perfect nonlinear mappings and their secret sharing schemes[J]. IEEE Transactions on Information Theory, 2005, 51(6): 2089-2102.

[8] Lu H C, Fu H L. The optimal average information ratio of secret-sharing schemes for the access structures based on unicycle graphs and bipartite graphs[J]. Discrete Applied Mathematics, 2017, 233: 131-142.

[9] Mignotte M. How to share a secret[C]//Workshop on Cryptography. Springer Berlin Heidelberg, 1982: 371-375.

[10] Asmuth C, Bloom J. A modular approach to key safeguarding[J]. IEEE Transactions on Information Theory, 1983, 29(2):208-210.

[11] Kaya K, Selçuk A A. Threshold cryptography based on Asmuth–Bloom secret sharing[J]. Information Sciences, 2007, 177(19): 4148-4160.

[12] Brickell E F. Some ideal secret sharing schemes[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Springer Berlin Heidelberg, 1989: 468-475.

[13] Ghodosi H, Pieprzyk J, Safavi-Naini R. Secret sharing in multilevel and compartmented groups[C]//Australasian Conference on Information Security and Privacy. Springer Berlin Heidelberg, 1998: 367-378.

[14] Siva Kumar P V, Kurra R R, Naidu Tentu A, et al. Multi-Level Secret Sharing Scheme for Mobile Ad-Hoc Networks[J].

International Journal of Advanced Networking & Applications, 2014.

[15] Harn L, Miao F. Multilevel threshold secret sharing based on the Chinese Remainder Theorem[J]. Information Processing Letters, 2014, 114(9):504-509.

[16] Chor B, Goldwasser S, Micali S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Foundations of Computer Science, 1985., 26th Annual Symposium on. IEEE, 1985: 383-395.

[17] Feldman P. A practical scheme for non-interactive verifiable secret sharing[C]//Foundations of Computer Science, 1987., 28th Annual Symposium on. IEEE, 1987: 427-438.

[18] Bai G, Damgård I, Orlandi C, et al. Non-Interactive Verifiable Secret Sharing For Monotone Circuits[C]//International Conference on Cryptology in Africa. Springer International Publishing, 2016: 225-244.

[19] Harn L, Lin C. Strong (n, t, n) verifiable secret sharing scheme[J]. Information Sciences, 2010, 180(16): 3059-3064.

[20] Rabin T, Ben-Or M. Verifiable secret sharing and multiparty protocols with honest majority[C]//Proceedings of the twenty-first annual ACM symposium on Theory of computing. ACM, 1989: 73-85.

[21] Fujisaki E, Okamoto T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications[J]. Advances in Cryptology—EUROCRYPT'98, 1998: 32-46.

[22] Habeeb M E. A verifiable secret sharing scheme using non-abelian groups[J]. Algebra and Computer Science, 2016, 677: 79.

[23] Mashhadi S, Dehkordi M H. Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LFSR public-key cryptosystem[J]. Information Sciences, 2015, 294: 31-40.

[24] Harn L. Group authentication[J]. IEEE Transactions on computers, 2013, 62(9): 1893-1898.

[25] Benaloh J C. Secret sharing homomorphisms: Keeping shares of a secret secret[C]//Conference on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1986: 251-260.

[26] Ersoy O, Kaya K, Kaskaloglu K. Multilevel Threshold Secret and Function Sharing based on the Chinese Remainder Theorem[J]. arXiv preprint arXiv:1605.07988, 2016.

[27] Martin K M. Challenging the adversary model in secret sharing schemes[J]. Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts, 2008: 45-63.