Scientific Research Publishing

Journal of Information Security, 2026, 17(3), 189-208
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Weighted Threshold Changeable Multi-Secret Sharing Scheme

Lingyi Chen

School of Mathematics and Statistics, Guilin University of Technology, Guilin, China
Email: 373486066@qq.com

How to cite this paper: Chen, L.Y. (2026) A Weighted Threshold Changeable Multi-Secret Sharing Scheme. *Journal of Information Security*, **17**, 189-208.
https://doi.org/10.4236/jis.2026.173010

Received: April 13, 2026
Accepted: May 25, 2026
Published: May 28, 2026

Copyright © 2026 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Secret sharing, an essential cryptographic technique for protecting sensitive data, faces the challenge of simultaneously addressing hierarchical access control, dynamic adjustments to access policies, and the parallel safeguarding of multiple secrets in complex practical scenarios. To address this challenge, this paper presents a novel weighted threshold changeable multi-secret sharing scheme that incorporates the Chinese Remainder Theorem (CRT) and polynomial theory. This scheme introduces a weighting mechanism that associates participants with secrets, allowing distinct participants to possess independent access permission thresholds for specific secrets, thereby facilitating hierarchical access control for multiple secrets. Additionally, to enhance system flexibility and scalability, the proposed solution implements a dynamic adjustment strategy for access permissions, which involves updating the polynomial order and modulus set without reconstructing the original secret. Furthermore, by establishing a system of congruent equations with coprime moduli using CRT, the scheme enables the simultaneous distribution of multiple secrets among participants within the same group. Each secret is assigned an independently adjustable threshold value, thus achieving parallel protection of multiple secrets. Security analysis indicates that the proposed scheme meets information-theoretic security under weight constraints and threshold conditions, and effectively mitigates internal collusion attacks and external eavesdropping attacks. Performance analysis demonstrates that the scheme achieves non-interactive computation during the reconstruction phase, optimizes communication rounds to approach the theoretical lower limit, and the information rate reaches the ideal value of 1.

Keywords

Threshold Changeable Secret Sharing, Multi-Secret Sharing, Chinese Remainder Theorem (CRT), Non-Interactive Reconstruction

1. Introduction

Secret sharing [1] [2] serves as a foundational protocol in modern cryptography, with applications spanning secure multi-party computation [3], cloud storage security [4], and blockchain [5]. As the Internet of Things and cloud computing continue to advance, the scenarios in which secret sharing is utilized are becoming increasingly complex and diverse, leading to heightened demands for data privacy protection [6] [7]. In practical scenarios, users typically have varying levels of permissions [8]-[10]. For example, in the key management systems of multinational enterprises, regional directors should possess greater decision-making authority than ordinary staff members [8]. Similarly, in the context of smart healthcare data sharing, attending physicians ought to have more extensive data access authority than interns [10]. However, the conventional (t,n) threshold secret sharing method fails to accommodate varying trust levels, duty permissions, or resource contributions among participants [11]. Consequently, the integration of a weighting mechanism to facilitate hierarchical access control has emerged as a significant focus in secret sharing research.

In complex security-level application scenarios, systems often require the simultaneous protection of multiple secrets, each with distinct security levels. The access policies governing these secrets may need to be dynamically adjusted in response to changing requirements [12]-[15]. For example, during an emergency, it may be necessary to temporarily lower the access threshold for specific types of medical data to expedite response efforts, or to raise the access threshold for financial transaction keys prior to sensitive operations to bolster security. The frequent reconstruction of secrets and redistribution of shares is not only inefficient but also heightens the risk of secret exposure during transmission. Consequently, achieving parallel sharing of multiple secrets alongside dynamic variable thresholds represents a critical challenge for enhancing the practicality of secret sharing schemes.

In recent years, the research on secret sharing technology has been carried out in three directions. The first is the study of weighted secret sharing. In practical applications, participants often exhibit varying levels of trust, responsibilities, and permissions. Traditional secret sharing schemes that utilize equal shares struggle to accommodate the requirements of multi-level management. By assigning differentiated weights to participants, weighted secret sharing enhances the flexibility of the participant combinations necessary for secret reconstruction, thereby facilitating hierarchical access control. Zhang *et al.* proposed an identity-based weighted dynamic secret sharing scheme [16]. However, this scheme does not effectively prevent attackers from acquiring secret information through illicit means. Harn *et al.* introduced a CRT-based weighted multi-secret sharing scheme [17], which achieved differential weight distribution among participants and enabled the parallel sharing of multiple secrets. Nevertheless, this scheme lacks verifiability and remains susceptible to malicious attacks. To mitigate computational overhead, Hsu *et al.* developed a (t,n) multi-secret sharing scheme based on bivariate pol-

ynomials [18]. However, due to its equal weight design and fixed threshold, this scheme cannot accommodate dynamic threshold adjustments or flexible weight allocation. In the context of single secret sharing, Garg *et al.* introduced a comprehensive framework of weighted cryptography [19], wherein the share size possessed by each participant is proportional to their assigned weight. However, the weights in this scheme remain fixed post-distribution, and the construction is notably intricate. Tan *et al.* developed a weighted secret image sharing scheme [20] that facilitates hierarchical image protection through the integration of visual cryptography. Nevertheless, it does not offer the capability for dynamic threshold adjustment. Consequently, the aforementioned schemes struggle to simultaneously satisfy the practical requirements of weight differentiation, multi-secret support, and dynamic adjustment.

The second area of focus is multi-secret sharing. As an extension of traditional secret sharing schemes, multi-secret sharing enables the distribution of multiple secrets [21]. This approach not only addresses the inefficiencies associated with protecting multiple secrets in single-secret schemes but also minimizes the communication overhead resulting from multiple rounds of repeated exchanges. Harn *et al.* [22] introduced an efficient multi-secret sharing scheme; however, it lacks support for differentiated weights. In another contribution, Harn *et al.* [23] developed a verifiable multi-secret sharing scheme aimed at enhancing overall security and detecting cheating, yet this scheme operates under equal weights, with each secret sharing the same threshold. Alam *et al.* [9] presented a hierarchical verifiable multi-secret sharing scheme that accommodates complex access structures. Nonetheless, the scheme's capacity for threshold adjustment is limited, making it challenging to support differentiated dynamic multi-secret access. Consequently, the implementation of weight allocation and dynamic threshold adjustment in multi-secret scenarios remains a critical issue to be addressed.

The final section addresses dynamic secret sharing, which is primarily applicable in situations where the number of participants and security levels may fluctuate. Miao *et al.* [24] introduced a (t, m, n) group-oriented secret sharing scheme that facilitates group-level privilege management; however, it maintains fixed group divisions based on equal weight, and the threshold remains static. To achieve flexible threshold adjustment, Wu *et al.* [25] developed a secret image sharing scheme with a variable threshold, yet it lacks support for weight differentiation. Xu *et al.* [26] proposed another group-oriented scheme that enhances security and addresses vulnerabilities, but it remains constrained to the group level, necessitating secret reconstruction for threshold adjustments, which poses a risk of leakage. While these schemes have advanced the variability of thresholds, improvements are still needed in supporting weight differentiation and ensuring the security of the threshold adjustment process.

In summary, in complex application scenarios, the above-mentioned schemes usually cannot support weight differentiation, multi-secret sharing, independently adjustable threshold and maintain non-interactive reconstruction at the same

time. Hence, it is difficult to meet the comprehensive requirements of flexibility, security and efficiency of multi-secret sharing. Addressing the limitations of existing research, this paper introduces a novel multi-secret sharing scheme that integrates a weighting mechanism with a dynamic threshold. The primary contributions of this study are as follows:

- First, we propose a hierarchical protection mechanism that employs weighted multi-secret fusion. Each participant is assigned an independent weight value corresponding to different secrets, thereby regulating their access to specific secrets based on these weights. Successful reconstruction of a secret occurs only when the sum of the weights of the parameters and the participants involved meets or exceeds the predetermined threshold for that secret. This design enhances the overall flexibility of the scheme and accommodates the requirements of differentiated rights management in complex scenarios.
- Second, we develop a multi-secret sharing mechanism that combines CRT with polynomial techniques. By leveraging the mathematical properties of CRT, each secret is assigned a unique set of coprime moduli, ensuring that different secrets maintain independence within their mathematical structure. This approach allows for the parallel sharing of multiple secrets among the same group of participants, with each secret's access policies remaining distinct. Consequently, the disclosure of one secret does not compromise the security of the others.
- Third, a threshold dynamic adjustment mechanism is realized without exposing the original secret. The thresholds of each secret can be adjusted independently. During the adjustment process, the existing shares are required to be collected by the dealer, and new shares are generated and distributed to the participants, while the original secret is never disclosed to any participant. By this mechanism, transmission of secret values over public channels is avoided, and the exposure risk caused by frequent reconstruction is effectively reduced.
- Fourth, a non-interactive secret reconstruction protocol is established. During the secret reconstruction phase, participants do not need to engage in multiple rounds of information exchange; instead, they utilize their own shares and public parameters to complete the reconstruction through Lagrange interpolation and the Chinese remainder theorem. This design optimizes the number of communication rounds to approach the theoretical lower limit, significantly decreasing communication overhead.

The rest of the paper is organized as follows: Section 2 introduces the preparatory knowledge related to the proposed scheme, including the Chinese Remainder theorem, the Lagrange interpolation theorem, the Shamir secret sharing scheme, and the basic definition of the access structure. Section 3 illustrates the system model, security model, and design goals. Section 4 describes the concrete construction of the proposed scheme in detail, including three stages of system initialization, secret distribution and secret reconstruction, and carries out security and performance analysis. Section 5 is the conclusion of this paper.

2. Preliminaries

2.1. Shamir's Secret Sharing Scheme

Based on Lagrange interpolation, Shamir proposed the classical (t,n) threshold secret sharing scheme [1]. In this scheme, the secret dealer D divides the secret s into n shares s_i and distributes them to n participants $P_1, P_2, \cdots, P_n$ respectively. Only more than or equal to t participants can cooperate to recover s in the secret reconstruction phase, while any fewer than t participants cannot obtain any information about s. The specific construction is as follows.

The distributor D selects a large prime number p over the finite field $GF(p)$ and constructs a $t-1$-degree random polynomial:

$$f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p}, \tag{1}$$

where the coefficients $a_1, a_2, \cdots, a_{t-1}$ are randomly selected from $GF(p)$ and the secret s is embedded as a constant term. The distributor assigns a unique nonzero identity $ID_i \in GF(p)$ to each participant P_i and computes shares $s_i = f(ID_i)$ to send to P_i over a secure channel. In the reconstruction phase, any t participants can jointly use Lagrange interpolation to recover $f(x)$ and calculate $f(0) = s$. The scheme is information theoretic secure because for any $t-1$ players, the constant terms of the polynomial are uniformly distributed over a finite field and they cannot obtain any information about s.

2.2. The Chinese Remainder Theorem (CRT)

CRT is a fundamental theorem in number theory and the core mathematical tool for multi-secret sharing in our scheme. Let $M_1, M_2, \cdots, M_k$ be pairwise coprime positive integers, that is, for any $i \neq j$ we have $\gcd(M_i, M_j) = 1$. Let $M = \prod_{r=1}^{k} M_r$ denote the product of these moduli. For any given sequence of integers $a_1, a_2, \cdots, a_k$, consider the following congruence equation system:

$$\begin{cases} x \equiv a_1 \pmod{M_1}, \\ x \equiv a_2 \pmod{M_2}, \\ \quad \vdots \\ x \equiv a_k \pmod{M_k}. \end{cases} \tag{2}$$

A unique solution exists for the above system of equations under modulus M. This solution can be obtained by using the following equation:

$$x \equiv \sum_{r=1}^{k} a_r \cdot N_r \cdot N_r^{-1} \pmod{M}, \tag{3}$$

where $N_r = M/M_r$, N_r^{-1} denotes the multiplicative inverse of N_r modulo M_r, *i.e.*, the unique integer satisfying $N_r \cdot N_r^{-1} \equiv 1 \pmod{M_r}$.

In this scheme, CRT is used to embed the secret S_j into multiple polynomial constant terms with different moduli, enabling parallel protection and independent recovery of multiple secrets.

2.3. Lagrange Interpolation Theorem

Lagrange interpolation theorem is the mathematical basis for Shamir's secret sharing scheme and the scheme in this paper to realize secret reconstruction. It is described as follows: Let $f(x)$ be a d-th degree polynomial defined over a finite field $GF(p)$, where p is a large prime number. Given $d+1$ distinct points (x_i, y_i) where $y_i = f(x_i)$ and $i = 1, 2, \cdots, d+1$, there exists a unique polynomial with degree no greater than d that passes through these points. This polynomial can be expressed explicitly as:

$$f(x) = \sum_{i=1}^{d+1} y_i \cdot \ell_i(x) \pmod{p}, \tag{4}$$

where $\ell_i(x)$ denotes Lagrange polynomials and is defined as:

$$\ell_i(x) = \prod_{j=1, j\neq i}^{d+1} \frac{x - x_j}{x_i - x_j} \pmod{p}. \tag{5}$$

Specially, when the constant term of the polynomial $f(0)$ needs to be recovered,

$$f(0) = \sum_{i=1}^{d+1} y_i \cdot \prod_{j=1, j\neq i}^{d+1} \frac{-x_j}{x_i - x_j} \pmod{p} = \sum_{i=1}^{d+1} y_i \cdot \lambda_i \pmod{p}, \tag{6}$$

where λ_i is the Lagrange interpolation coefficient.

This theorem guarantees that the polynomial can be uniquely determined and the secret embedded in it can be extracted in the secret reconstruction phase, provided that a sufficient number of valid share points are obtained.

2.4. Access Structure and Weight Function

In the secret sharing scheme, access structures are used to describe which subsets of participants are authorized to recover secrets. Let there be n participants in the system, and denote the set of participants as $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$. A subset of participants is called an authorized subset if it is allowed to recover the secret, otherwise it is an unauthorized subset. The access structure is the set consisting of all authorized subsets.

The traditional (t, n) threshold scheme corresponds to an access structure of:

$$\Gamma = \{A \subseteq \mathcal{P} \mid |A| \geq t\}. \tag{7}$$

This implies that once the number of participants meets the threshold t, the subset is permitted to recover the secret, with all participants holding equal status. To accommodate practical scenarios where participants possess varying levels of authorization, weighted secret sharing incorporates a weight function. The weight mapping is defined as:

$$w: \mathcal{P} \times \mathcal{S} \to \mathbb{Z}^+, \tag{8}$$

where $\mathcal{S} = \{S_1, S_2, \cdots, S_m\}$ represents the set of secrets. Let $w(P_i, S_j) = w_{i,j}$ denote the contribution of participant P_i to secret S_j. For a given secret S_j, each participant possesses an independent weight, with the weight assignment po-

tentially varying across different secrets. The access structure for secret S_j is defined by both the weights and the associated thresholds:

$$\Gamma_j = \left\{ A \subseteq \mathcal{P} \mid \sum_{P_i \in A} w_{i,j} \geq t_j \right\}, \tag{9}$$

where t_j is a predetermined threshold for the secret S_j. This weight-sum-based access structure serves as a direct generalization of the conventional threshold structure, offering enhanced flexibility in privilege management.

3. Scheme Model

3.1. System Model

This scheme comprises three primary entities: the secret distributor, the participants, and the secrets.

1) The secret distributor, denoted as D, functions as a trusted central entity responsible for setting up the system, distributing secrets, assigning weights, and adjusting thresholds dynamically. Following the initialization phase, D can disconnect and intervene again solely for threshold adjustments or new secret additions.

2) The participants, represented as $\mathcal{U} = \{U_1, U_2, \cdots, U_n\}$, consist of n unique individuals. Each participant U_i possesses a distinct identity ID_i selected from the finite field $GF(p)$. Additionally, each participant holds a secret share vector $s_i = (s_{i,1}, s_{i,2}, \cdots, s_{i,m})$, where m denotes the number of secrets. The vector enables participants to reconstruct any one or more secrets.

3) The set of secrets, denoted as $\mathcal{S} = \{S_1, S_2, \cdots, S_m\}$, comprises m secrets requiring protection. Each secret S_j is linked to an individual access threshold t_j and a specific array of moduli $\{M_{j,1}, M_{j,2}, \cdots, M_{j,k}\}$, where k represents the quantity of moduli.

A secret sharing scheme typically comprises three phases. The first phase is system initialization, during which D generates the public parameters and various constants necessary for selecting the mathematical structure. The second phase, known as secret distribution, involves D calculating the share vector for each participant based on the weight allocation strategy and distributing it via a secure channel. Finally, in the secret reconstruction phase, a subset of authorized participants, who meet the specified weights and conditions, collaboratively reconstructs the secret.

When the threshold of a secret S_j needs to be changed, the threshold update protocol is executed by the dealer D: at least t_j existing shares are collected by D over a secure channel, the original polynomial is reconstructed without revealing the secret value, and then a new polynomial of degree $t_j' - 1$ with the same constant term is constructed. New shares are computed and distributed to the participants. During this process, the shares are required to be redistributed, but the original secret is not exposed to any participant, and the secret itself is not transmitted over any public channel.

3.2. Security Model

This scheme addresses two primary attacker models: internal attackers and external attackers.

1) Internal attackers are malicious participants within the system. They may attempt a collusive attack, wherein multiple participants jointly seek to recover a secret despite an insufficient total weight, or a single participant may endeavor to recover a secret to which they lack access. Furthermore, an internal attacker might provide false share information during the secret reconstruction phase, aiming to compromise the reconstruction process or to facilitate the recovery of an incorrect secret.

2) External attackers are third parties without any legal shares who attempt to obtain secret information by eavesdropping on the public channel, intercepting communication data, or analyzing public parameters. An external attacker may seek to infer the secret value or share information by leveraging the public identity, modulus set, and historical reconstruction records.

The proposed scheme is predicated on the following security assumption: the dealer D is honest and trustworthy during the initialization phase, capable of correctly executing the initialization algorithm and securely distributing shares. The communication channel among participants is public yet authenticated, meaning that while the attacker can eavesdrop on the communication content, they cannot forge messages. The selection of the finite field $GF(p)$ and the modulus M_r adheres to the safety parameter requirements, rendering exhaustive search computationally infeasible.

3.3. Security Goals

Based on the above model and assumptions, our scheme aims to achieve the following security and functional goals:

1) Correctness: Any subset of authorized participants that meets the specified weights and conditions must be capable of accurately reconstructing the target secret. Conversely, any unauthorized subset with a weight sum below the threshold cannot acquire any information regarding the secret, thereby satisfying information-theoretic security.

2) Weighted access control: The scheme facilitates the assignment of varying weights to different participants, enabling flexible hierarchical permission management. Participants assigned higher weights should contribute more significantly to the reconstruction of the secret, and the allocation of weights should be independently adjustable for different secrets.

3) Threshold changeability: The scheme must allow for the dynamic adjustment of the access threshold for each secret, accommodating both increases and decreases in the threshold. This adjustment process should not necessitate the reconstruction of the original secret or the recomputation and redistribution of shares among all participants; rather, it should involve only the update of public parameters.

4) Multi-secret independence: The protective mechanisms for different secrets should be mathematically independent of one another. The disclosure, reconstruction, or threshold adjustment of one secret should not impact the security of any other secrets.

5) Security: The scheme must be resilient against both internal and external attacks. In instances where unauthorized participants are present during the secret reconstruction phase, the scheme should safeguard the secret information from theft by the attacker, thereby ensuring the integrity of secret sharing.

6) Non-interaction: The reconstruction process must minimize communication interactions among participants. Ideally, participants should only submit their shares or complete the secret recovery through local calculations, eliminating the need for multiple rounds of information exchange. This approach effectively reduces both communication overhead and computational complexity.

4. The Weighted Threshold Changeable Multi-Secret Sharing Scheme

Addressing the limitations of secret sharing schemes, a novel weighted threshold changeable multi-secret sharing scheme is designed, which combines CRT and polynomial theory. In the scheme, individual weights are assigned to participants for different secrets, enabling the reconstruction of secrets only when the total weight of participants meets the threshold requirement. This approach allows for adaptable hierarchical access control. Additionally, the adoption of coprime moduli through the Chinese remainder theorem ensures mathematical independence among multiple secrets, facilitating simultaneous sharing without interference. By linking the threshold to the polynomial degree, adjustments to the threshold for each secret can be made independently without the need to reconstruct the original secret. The reconstruction process is streamlined, requiring participants only to provide their shares, thereby eliminating the necessity for multiple rounds of interaction and reducing computational and communication overheads. This scheme encompasses four key elements: weighting, multi-secrecy, variable threshold, and non-interactive reconstruction, surpassing existing methods in functionality, security, and efficiency. The solution comprises three fundamental stages: system initialization, secret distribution, and secret reconstruction. The subsequent section provides a detailed account of these stages.

4.1. Initialization Phase

This subsection describes the initialization process of the proposed scheme, which mainly consists of the initialization of the system parameters' and participants' identity information, as well as the weight values. The notation about the proposed scheme and its description are shown in Table 1. The specific process of the initialization phase is as follows.

Step 1: Let the secret distributor be D, which is responsible for selecting the base parameters of the scheme. Choose a sufficiently large security prime p and

define the finite field $GF(p)$. The secret distributor D holds m secret data to be shared $S_1, S_2, \cdots, S_m$, all belonging to the finite domain $GF(p)$.

Step 2: A total of n participants are involved in the secret sharing process together, and the secret distributor D randomly selects n positive integers ID_i from the finite domain $GF(p)$ as the unique identifiers of the participants U_i, $i = 1, 2, \cdots, n$. At the same time, assign each participant a weight $w_{i,j}$ for secret S_j, $j = 1, 2, \cdots, m$.

Step 3: For each secret S_j, D sets a corresponding threshold t_j. That is, secret S_j can be reconstructed only if the weight sum of the participants involved in the reconstruction phase is greater than or equal to t_j. These thresholds t_i are variable and $t \le n$.

Step 4: For each secret S_j ($j = 1, \cdots, m$), the secret distributor D independently chooses k_j pairwise coprime positive integers as the modulus set dedicated to that secret, denoted as $\{M_{j,1}, M_{j,2}, \cdots, M_{j,k_j}\}$. Compute $M_j = \prod_{r=1}^{k_j} M_{j,r}$. To ensure the CRT-based secret embedding, each M_j must satisfy $S_j < M_j$. The modulus sets for different secrets are independent of each other, guaranteeing that the recovery of one secret does not leak information about another.

Step 5: Disclose the finite domain $GF(p)$, the identifiers of all participants ID_i, the set of all moduli M_r, and the weight values.

Table 1. Notations.

Symbol	Description
D	Secret distributor
n	Total number of participants
U_i	The i-th participant, $1 \le i \le n$
ID_i	Identity of U_i
m	Total number of secrets
S_j	The j-th secret, $1 \le j \le m$
t_j	Threshold of secret S_j
$w_{i,j}$	Weight of participant U_i for secret S_j
p	Large secure prime, $p > n$
k	Number of moduli
$M_{j,r}$	The r-th modulus of the j-th secret S_j, $1 \le r \le k_j$
M_j	Product of moduli $M_j = \prod_{r=1}^{k_j} M_{j,r}$
$f_{j,r}(x)$	Polynomial of secret S_j under modulus $M_{j,r}$
$a_{j,r,0}$	Constant term of polynomial $f_{j,r}(x)$
$s_{i,j,r}$	Share of participant U_i under modulus M_r
$s_{i,j}$	Share vector of participant U_i for secret S_j
$\mathcal{A}$	Subset of participants involved in reconstruction

4.2. Sharing Phase

In this phase, the secret distributor D employs CRT in conjunction with a polynomial to create a distinct share of the secret for each participant, which is then securely distributed to them.

Step 1: For each secret S_j, the secret distributor D constructs a random polynomial of degree $t_j - 1$ over the modulus $M_{j,r}$:

$$f_{j,r}(x) = a_{j,r,0} + a_{j,r,1}x + \cdots + a_{j,r,d_j}x^{d_j} \left(\mathrm{mod}\, M_{j,r}\right),\ r = 1, \cdots, k_j, \tag{10}$$

where $a_{j,r,d_j} \neq 0$, and the constant term $a_{j,r,0}$ satisfies:

$$a_{j,r,0} \equiv S_j \left(\mathrm{mod}\, M_{j,r}\right). \tag{11}$$

The polynomial for each secret is generated independently and randomly within the modulus component to ensure that the security of the secrets remains unaffected by one another.

Step 2: Based on the generated polynomial $f_{j,r}(x)$, the secret dealer D computes the share for each participant regarding each secret. For the secret S_j and participant U_i, the polynomial values are evaluated at their identity information ID_i:

$$s_{i,j,r} = f_{j,r}(ID_i)\left(\mathrm{mod}\, M_{j,r}\right),\ r = 1, \cdots, k_j. \tag{12}$$

Step 3: The secret dealer D combines all module components $\left\{s_{i,j,1}, \cdots, s_{i,j,k_j}\right\}$ to form the participants' share vector for the secret S_j, denoted as $s_{i,j}$. Each participant U_i receives their final secret share $s_{i,j}$ through a secure channel.

In the distribution process, a weight constraint must be adhered to: the share $s_{i,j}$ is sent only if the weight $w_{i,j} > 0$ for participant U_i concerning secret S_j. This design ensures that the polynomial degree d_j and modulus $M_{j,r}$ corresponding to high-weight secrets are larger, thereby necessitating more effective shares for recovery and achieving hierarchical protection.

4.3. Reconstruction Phase

In this phase, the secret S_j is independently reconstructed by the authorized participants through one round of broadcast communication, using their own secret shares and the properties of the CRT, without the participation of the dealer D. Let the set of members engaged in the reconstruction be denoted as $\mathcal{A}$, which comprises l participants U_i. Prior to the reconstruction phase, it is essential to ascertain the weights of the set and to verify whether they satisfy the threshold conditions. If

$$\sum_{U_i \in \mathcal{A}} w_{i,j} \geq t_j, \tag{13}$$

then the preset safety requirements are met, and secret recovery is possible. Otherwise, the reconstruction process will be halted and any secret cannot be restored. The specific process is as follows:

Step 1: Under each module $M_{j,r}\left(r = 1, 2, \cdots, k_j\right)$, participant $U_i \in \mathcal{A}$ utilizes

their share $s_{i,j,r}$ associated with the publicly available identity ID_i. The polynomial $f_{j,r}(x)$ is reconstructed using the Lagrange interpolation method.

Step 2: For each modulus $M_{j,r}$, the constant term $a_{j,r,0}$ is derived from the reconstructed polynomial $f_{j,r}(x)$. This constant term represents the residue of the secret S_j modulo $M_{j,r}$. These residues collectively establish a system of congruence equations:

$$\begin{cases} S_j \equiv a_{j,1,0} \left(\mathrm{mod}\, M_{j,1}\right), \\ S_j \equiv a_{j,2,0} \left(\mathrm{mod}\, M_{j,2}\right), \\ \quad \vdots \\ S_j \equiv a_{j,k_j,0} \left(\mathrm{mod}\, M_{j,k_j}\right). \end{cases} \tag{14}$$

Step 3: Apply CRT to solve the above system of congruent equations and obtain a unique solution, which is the secret S_j.

4.4. Correctness Analysis

Theorem 1: The weighted multi-secret sharing scheme, formulated utilizing CRT and polynomials, ensures correctness. Specifically, any subset of participants with a combined weight exceeding t_j can collectively reconstruct the secret S_j. Conversely, if the total weight falls below t_j, the retrieval of secret S_j becomes infeasible.

Proof: In the initialization phase, the secret distributor D generates random polynomials for each secret S_j across various mutually prime moduli, integrating the secret into the constant coefficients of these polynomials. Each participant U_i acquires a share equivalent to the polynomial value at their unique identifier, with only participants possessing a weight $w_{i,j} > 0$ being eligible to receive the corresponding secret share.

In the reconstruction phase, if the sum of the weights of the participant set $\mathcal{A}$ satisfies:

$$\sum_{U_i \in \mathcal{A}} w_{i,j} \geq t_j, \tag{15}$$

then the number of effective shares uniquely determines the corresponding polynomial at each modulus. Sufficient valid points ensure the uniqueness of Lagrange interpolation, allowing the extraction of the constant term determined by t_j. The constant terms under each modulus represent the remainders of the secret S_j under that modulus. According to the Chinese remainder theorem, these remainders constitute a system of congruent equations regarding the secret S_j. By solving this system of equations, a unique solution can be found, enabling the successful reconstruction of S_j. Conversely, if the sum of weights is less than t_j, the number of effective shares is insufficient to uniquely determine the polynomial. In this case, the constant term is evenly distributed among all possible polynomials, preventing the attacker from narrowing down the possibilities. Consequently, no effective information about S_j can be obtained, and the secret remains un-

recoverable.

In conclusion, this scheme accurately reconstructs the secret if any participant set meets a weight sum equal to or greater than the threshold. Otherwise, recovery is impossible, ensuring compliance with correctness requirements.

4.5. Security Analysis

The security analysis of the proposed scheme is conducted from four perspectives: internal attack, external attack, changeable threshold security, and non-interactive security. The comprehensive evaluation of the scheme's security performance is performed under various threat models.

4.5.1. Internal Attack

Theorem 2: Let $\mathcal{C}$ be the set of internal colluding participants, and let $\sum_{U_i \in \mathcal{C}} w_{i,j} < t_j$. Then:

$$I\left(S_j; \{s_{i,j}\}_{U_i \in \mathcal{C}}\right) = 0.$$

That is, no information about S_j is obtained by the colluders. Moreover, for active forgery attacks, the submission of fake shares by malicious participants can only cause reconstruction failure or the output of an incorrect secret, but the real secret cannot be obtained. Therefore, the proposed weighted multi-secret sharing scheme is able to resist internal attacks.

Proof: For each modulus $M_{j,r}$, the coefficients of the polynomial $f_{j,r}(x)$ are chosen uniformly and independently from $GF(p)$, with only the constant term fixed to a value satisfying $a_{j,r,0} \equiv S_j \left(\mathrm{mod}\, M_{j,r}\right)$ (this value is determined by the secret). The colluders collectively hold $W_{\mathcal{C}} < t_j$ distinct evaluation points. For a polynomial of degree $t_j - 1$, given $t_j - 1$ points, the remaining point can take any value in $GF(p)$, so p different polynomials can be generated, and the constant terms of these polynomials are uniformly distributed over $GF(p)$. Since S_j is in one-to-one correspondence with these constant terms (under the fixed modulus), it follows that $H\left(S_j \mid \mathrm{shares}_{\mathcal{C}}\right) = \log p = H\left(S_j\right)$, and thus the mutual information is zero. As this argument holds for all moduli and each modulus is independent, the overall mutual information is also zero.

If a malicious participant submits $s'_{i,j,r} \neq s_{i,j,r}$, then the combiner performs Lagrange interpolation using the set that includes this fake point. The resulting polynomial $f'_{j,r}(x)$ will differ from the real polynomial with high probability (at least $1 - 1/p$). Its constant term $a'_{j,r,0}$ is uniformly random, so the secret S'_j recovered via CRT is independent of the real secret S_j. The attacker cannot infer the real secret from such disruptive behavior, though the scheme cannot identify the forger. Hence, the proposed scheme effectively resists deceptive actions from internal attackers.

4.5.2. External Attack

Theorem 3: Let

$$\text{Pub} = \left\{ GF(p), \{ID_i\}_{i=1}^{n}, \{M_{j,r}\}_{j=1,r=1}^{m,k_j}, t_j, w_{i,j} \right\}$$

be all the public parameters. For any external attacker E who holds no shares, it holds that

$$I(S_j; \text{Pub}) = 0.$$

That is, no information about S_j is leaked by the public parameters. Therefore, the proposed weighted multi-secret sharing scheme is able to resist external attacks.

Proof: The secret S_j appears only in the condition on the constant term of the polynomial, *i.e.*, $a_{j,r,0} \equiv S_j \left(\text{mod } M_{j,r}\right)$. Among the public parameters: $GF(p)$ and ID_i are independent of the secret; the moduli $M_{j,r}$ only require that $S_j < M_j$, and M_j is typically chosen to be much larger than any possible upper bound of the secret, so M_j carries no specific information about S_j; the threshold t_j and the weights $w_{i,j}$ belong to policy configuration and are statistically independent of the secret value. Since E has no polynomial evaluation points, no constraints are imposed on the distribution of the polynomial coefficients $a_{j,r,1}, \cdots, a_{j,r,t_j-1}$. For any two candidate secrets S_j^0, S_j^1, when the dealer generates the polynomials, the constant term is fixed to the corresponding remainder value, but the remaining coefficients are chosen uniformly at random. Therefore, the probability distributions of the public parameters under the two hypotheses are exactly identical (the statistical distance is zero). Hence $I(S_j; \text{Pub}) = 0$.

In the proposed scheme, the Chinese Remainder Theorem is only used to encode the secret into multiple congruences, and it does not provide any distinguishable statistical pattern to an external adversary. Without any shares, the adversary cannot obtain any remainder, and thus the possible range of the secret cannot be narrowed down. Therefore, the proposed scheme effectively resists deceptive actions from external attackers.

4.5.3. Threshold Changeability

Theorem 4: The proposed weighted multi-secret sharing scheme has threshold changeability.

Proof: In the proposed scheme, the secret distributor D independently generates a $t_j - 1$-degree polynomial $f_{j,r}(x)$ for each secret S_j, where the threshold t_j is directly linked to the polynomial's degree. Adjusting the threshold t_j of a specific secret S_j, whether increasing or decreasing, only necessitates modifying the polynomial's degree $f_{j,r}(x)$ and regenerating the corresponding shares, leaving the polynomials of other secrets unaffected. This design allows for individual and flexible adjustment of each secret's threshold without disrupting the sharing mechanism of other secrets, thereby fulfilling the requirement for threshold changeability.

4.5.4. Non-Interactive Reconstruction

Theorem 5: The proposed weighted multi-secret sharing scheme is non-interactive in the secret reconstruction stage.

Proof: At the secret reconstruction stage, participant U_i simply conducts Lagrange interpolation using the shares $s_{i,j,r}$ it possesses and the public parameters $\left\{M_{j,1},\cdots,M_{j,k_j},ID_1,\cdots,ID_n\right\}$. Consequently, $f_{j,r}(x)$ is reconstructed, and the constant term $a_{j,r,0}$ is derived. Subsequently, the constant terms within each module are amalgamated via CRT to yield a unique solution, specifically the secret S_j. This entire process eliminates the need for multiple rounds of information exchange among participants or real-time involvement of D. All essential information is encompassed in the initial share and public parameters, thereby achieving non-interactivity in secret reconstruction.

4.6. Performance Analysis

In the subsection, a detailed analysis of the weighted multi-secret sharing scheme is conducted from computational overhead and communication overhead.

4.6.1. The Analysis of Computation Cost

The computational burden of the proposed scheme primarily lies in three phases: the initialization phase, the secret distribution phase, and the secret reconstruction phase. In the initialization phase, the secret distributor must choose a secure prime number p, create n identity identifiers, establish m thresholds for the secret, and determine k pairwise coprime moduli. The computational complexity of this phase amounts to $O(mk)$ modulo operations.

At the secret distribution phase, for each secret S_j and each modulus $M_{j,r}$, where $r=1,\cdots,k_j$, the distributor must generate a polynomial of degree t_j-1 and compute n share values. To create the polynomial, t_j coefficients are randomly selected, resulting in a computational complexity of $O(t_j)$. The calculation of each share necessitates $O(t_j)$ modulo multiplications. Consequently, the overall computational complexity of the distribution stage is $O(m\cdot k\cdot n\cdot \bar{t})$, where $\bar{t}=\max_j t_j$. Given that k is typically a constant, this level of complexity is deemed acceptable.

At the reconstruction phase, the authorized subset $\mathcal{A}$ of size l is essential for secret restoration, where $\mathcal{A}$ must meet the condition $\sum w_{i,j}\geq t_j$. The computational complexity of Lagrange interpolation in each module amounts to $O(l\cdot t_j)$ since t_j basis polynomials must be computed. Subsequently, the complexity of merging k congruences via CRT is $O(k^2)$. Given that $l\approx t_j$, the reconstruction complexity becomes $O(t_j^2+k^2)$. In contrast to methods necessitating multiple rounds of interaction, the non-interactive nature of this approach circumvents computational delays stemming from communication.

4.6.2. The Analysis of Communication Cost

Communication overhead encompasses the volume of communication during both the share distribution stage and the secret reconstruction stage. In the share distribution stage, the secret distributor transmits the share vector for each participant via a secure channel. Each share vector consists of $m\cdot k_j$ modular components, with each component approximately $|M_{j,r}|$ bits in size. Consequently, the total commu-

nication volume is $O\left(n \cdot m \cdot \bar{k} \cdot \log M_{\max}\right)$, where $M_{\max} = \max_{j,r} M_{j,r}$. Given that the distribution stage is performed only once, this overhead remains within an acceptable range.

At the secret reconstruction stage, this scheme ensures non-interactivity, as participants are not required to exchange messages. Each participant simply provides their share, resulting in a single communication round. In contrast, traditional interactive solutions necessitate multiple rounds of broadcasting or point-to-point communication, involving at least $O\left(t_j\right)$ communication rounds. Consequently, the communication overhead associated with this scheme during the reconfiguration stage is significantly lower than that of existing solutions.

Furthermore, during the threshold adjustment phase, the existing shares are required to be collected by the dealer and new shares are distributed, resulting in a communication overhead of $O\left(n \cdot m \cdot k \cdot \log M_{\max}\right)$, which is of the same order as that of the initial distribution phase. Since threshold adjustments are usually infrequent, this overhead remains acceptable. Compared with a full reinitialization scheme, the proposed protocol avoids the cost of reselecting moduli and resetting all system parameters, and the original secret is never exposed over any public channel.

4.7. Information Rate

The information rate is defined as the ratio of the total size of the secrets to the total size of the shares held by each participant. Let the length of the secret S_j be denoted as $\left|S_j\right|$ bits, and let the length of each modulus $M_{j,r}$ be $\left|M_{j,r}\right|$ bits. According to CRT,

$$\left|S_j\right| \approx \sum_{r=1}^{k_j} \left|M_{j,r}\right|. \tag{16}$$

The total size of the shares stored in each participant's share vector $\boldsymbol{s}_{i,j}$ (for all secrets) is

$$\sum_{j=1}^{m} \sum_{r=1}^{k_j} \left|M_{j,r}\right| = \sum_{j=1}^{m} \left|S_j\right|. \tag{17}$$

Therefore, the information rate of a single participant is

$$\rho_{\text{single}} = \frac{\sum_{j=1}^{m} \left|S_j\right|}{\sum_{j=1}^{m} \left|S_j\right|} = 1. \tag{18}$$

The total storage capacity for all participants in the system is $n \cdot \sum_{j=1}^{m} \left|S_j\right|$, while the total amount of secrets is $\sum_{j=1}^{m} \left|S_j\right|$. Consequently, the system information rate is

$$\rho_{\text{system}} = \frac{\sum_{j=1}^{m} \left|S_j\right|}{n \cdot \sum_{j=1}^{m} \left|S_j\right|} = \frac{1}{n}. \tag{19}$$

Since each participant's share can be utilized concurrently to reconstruct all se-

crets, the proposed scheme attains an optimal information rate of 1. Specifically, because each participant solely retains one secret share vector $s_{i,j}$, multiple secrets can be reconstructed, ensuring information-theoretic security.

Comparison

To fully evaluate the performance advantages, the proposed schemes are compared with several representative secret sharing schemes, where the compared schemes include Shamir's scheme [1], Harn's scheme [17], Hsu's scheme [18] and Wu's scheme [25]. The results are shown in **Table 2**.

It can be seen from the table that Shamir's scheme has the highest information rate and operates non-interactively, but it lacks both weighting and multi-secret capabilities. Conversely, the other compared schemes support for weighting and multi-secrecy. However, they feature an immutable threshold and necessitate interactive reconstruction. Hsu's scheme allows for multi-secrecy and non-interaction but does not accommodate weighting or variable thresholds. Wu *et al.*'s scheme enables variable thresholds and non-interaction yet fails to support weighting and multi-secrecy. In contrast, the proposed scheme integrates all desired features, including weighted support, multi-secret parallelism, independently adjustable thresholds, and non-interactive reconstruction. Furthermore, it achieves the theoretical maximum information rate of 1, effectively countering collusion attacks. Its overall performance markedly surpasses that of existing comparative schemes.

Table 2. Performance comparison of different schemes.

Schemes	Shamir [1]	Harn [17]	Hsu [18]	Wu [25]	Our Scheme
Weighted	No	Yes	No	No	Yes
Multi-secret	No	Yes	Yes	No	Yes
Threshold changeable	No	No	No	Yes	Yes
Non-interactive	Yes	No	Yes	Yes	Yes
Information rate	1	0.5	0.8	0.9	1
Resist attacks	No	Partial	Yes	Yes	Yes

5. Conclusion

This paper introduces a weighted multi-secret sharing scheme that utilizes polynomials and CRT to address the demands of multi-secret sharing schemes in intricate application scenarios involving graded protection and dynamic scalability. The key innovation of this approach is the assignment of weight values to participants and the use of CRT to allocate a distinct set of mutually prime moduli for each secret, thereby providing hierarchical protection of secrets. Additionally, when incorporating new secret values, it is only necessary to select modulus sets meeting the relevant criteria and create a new polynomial, and there is no need to recalibrate or redistribute shares among existing participants, significantly improving the scheme's dynamic scalability. Concerning security, by maintaining

the confidentiality of the relationship between secrets and moduli and combining the confidentiality of polynomial interpolation with the dependability of the CRT, the approach effectively withstands both internal and external attacks, ensuring information-theoretic security. In terms of efficiency, the approach achieves non-interactivity during the secret reconstruction phase. Participants simply need to reconstruct the polynomials under each modulus using their secret shares and public data, extract the constant terms, and independently solve the CRT system of equations. This significantly diminishes communication overhead and computational complexity, thereby attaining optimal performance in both communication and computation. As the inaugural threshold-changeable multi-secret sharing scheme to thoroughly incorporate weighting mechanisms, polynomial theory, and CRT, the scheme introduced in this paper theoretically broadens the access control model of multi-secret sharing. In practical terms, it offers new theoretical foundations and technical support for application scenarios, such as smart environments, which impose stringent requirements for the secure, efficient, and flexible sharing of private data.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. https://doi.org/10.1145/359168.359176

[2] Blakley, G.R. (1979) Safeguarding Cryptographic Keys. 1979 *International Workshop on Managing Requirements Knowledge* (*MARK*), New York, 4-7 June 1979, 313-318. https://doi.org/10.1109/mark.1979.8817296

[3] Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C., Li, H., *et al*. (2019) Secure Multi-Party Computation: Theory, Practice and Applications. *Information Sciences*, **476**, 357-372. https://doi.org/10.1016/j.ins.2018.10.024

[4] Wang, B.Y., Li, B.C. and Li, H. (2014) Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud. *IEEE Transactions on Cloud Computing*, **2**, 43-56. https://doi.org/10.1109/tcc.2014.2299807

[5] Sharma, P., Namasudra, S., Gonzalez Crespo, R., Parra-Fuente, J. and Chandra Trivedi, M. (2023) EHDHE: Enhancing Security of Healthcare Documents in IoT-Enabled Digital Healthcare Ecosystems Using Blockchain. *Information Sciences*, **629**, 703-718. https://doi.org/10.1016/j.ins.2023.01.148

[6] Xie, B., Zhou, Y., Yi, X. and Wang, C. (2023) An Improved Multi-Authority Attribute Access Control Scheme Base on Blockchain and Elliptic Curve for Efficient and Secure Data Sharing. *Electronics*, **12**, Article 1691. https://doi.org/10.3390/electronics12071691

[7] Shree, S., Zhou, C. and Barati, M. (2023) Data Protection in Internet of Medical Things Using Blockchain and Secret Sharing Method. *The Journal of Supercomputing*, **80**, 5108-5135. https://doi.org/10.1007/s11227-023-05657-7

[8] Liu, G.L., Li, L.Y., Zheng, J. and Li, Z.G. (2010) A Hierarchical Key Management Scheme in Role-Based Access Control. 2010 *International Conference on Computer Design and Applications*, Qinhuangdao, 25-27 June 2010, V5-581-V5-584.

https://doi.org/10.1109/iccda.2010.5541164

[9] Alam, I., Alali, A.S., Ali, S. and Asri, M.S.M. (2024) A Verifiable Multi-Secret Sharing Scheme for Hierarchical Access Structure. *Axioms*, **13**, Article 515. https://doi.org/10.3390/axioms13080515

[10] Motta, G.H.M.B. and Furuie, S.S. (2003) A Contextual Role-Based Access Control Authorization Model for Electronic Patient Record. *IEEE Transactions on Information Technology in Biomedicine*, **7**, 202-207. https://doi.org/10.1109/titb.2003.816562

[11] Beimel, A. (2011) Secret-Sharing Schemes: A Survey. In: Chee, Y.M., *et al.*, Eds., *Coding and Cryptology*, Springer, 11-46. https://doi.org/10.1007/978-3-642-20901-7_2

[12] Dehkordi, M.H. and Mashhadi, S. (2008) An Efficient Threshold Verifiable Multi-Secret Sharing. *Computer Standards & Interfaces*, **30**, 187-190. https://doi.org/10.1016/j.csi.2007.08.004

[13] Chen, D., Lu, W., Xing, W. and Wang, N. (2019) An Efficient Verifiable Threshold Multi-Secret Sharing Scheme with Different Stages. *IEEE Access*, **7**, 107104-107110. https://doi.org/10.1109/access.2019.2929090

[14] Wang, F., Zhou, Y. and Li, D. (2015) Dynamic Threshold Changeable Multi-Policy Secret Sharing Scheme. *Security and Communication Networks*, **8**, 3653-3658. https://doi.org/10.1002/sec.1288

[15] Zhang, Z., Chee, Y.M., Ling, S., Liu, M. and Wang, H. (2012) Threshold Changeable Secret Sharing Schemes Revisited. *Theoretical Computer Science*, **418**, 106-115. https://doi.org/10.1016/j.tcs.2011.09.027

[16] Zhang, Y. and Liu, Z. (2007) Dynamic and Verifiable Secret Sharing among Weighted Participants. *Journal of Systems Science and Complexity*, **20**, 481-485. https://doi.org/10.1007/s11424-007-9044-z

[17] Harn, L. and Miao, F.Y. (2014) Weighted Secret Sharing Based on the Chinese Remainder Theorem. *International Journal of Network Security*, **16**, 420-425.

[18] Harn, L. and Hsu, C. (2016) (T, N) Multi-Secret Sharing Scheme Based on Bivariate Polynomial. *Wireless Personal Communications*, **95**, 1495-1504. https://doi.org/10.1007/s11277-016-3862-z

[19] Garg, S., Jain, A., Mukherjee, P., Sinha, R., Wang, M. and Zhang, Y. (2023) Cryptography with Weights: MPC, Encryption and Signatures. In: Handschuh, H. AND Lysyanskaya, A., Eds., *Advances in Cryptology—CRYPTO* 2023, Springer, 295-327. https://doi.org/10.1007/978-3-031-38557-5_10

[20] Tan, L., Lu, Y., Yan, X., Liu, L. and Li, L. (2019) Weighted Secret Image Sharing for a (k, n) Threshold Based on the Chinese Remainder Theorem. *IEEE Access*, **7**, 59278-59286. https://doi.org/10.1109/access.2019.2914515

[21] Hsu, C., Cheng, Q., Tang, X. and Zeng, B. (2011) An Ideal Multi-Secret Sharing Scheme Based on MSP. *Information Sciences*, **181**, 1403-1409. https://doi.org/10.1016/j.ins.2010.11.032

[22] Harn, L., Hsu, C., Xia, Z. and Zhou, J. (2017) How to Share Secret Efficiently over Networks. *Security and Communication Networks*, **2017**, Article ID: 5437403. https://doi.org/10.1155/2017/5437403

[23] Harn, L., Xia, Z., Hsu, C. and Liu, Y. (2020) Secret Sharing with Secure Secret Reconstruction. *Information Sciences*, **519**, 1-8. https://doi.org/10.1016/j.ins.2020.01.038

[24] Miao, F., Fan, Y., Wang, X., Xiong, Y. and Badawy, M. (2016) A (t, M, N)-Group Oriented Secret Sharing Scheme. *Chinese Journal of Electronics*, **25**, 174-178. https://doi.org/10.1049/cje.2016.01.026

[25] Wu, G., Wang, M., Wang, Q., Yao, Y., Yuan, L. and Miao, G. (2021) A Novel Threshold Changeable Secret Image Sharing Scheme. *Symmetry*, **13**, Article 286. https://doi.org/10.3390/sym13020286

[26] Xu, R., Wang, X., Morozov, K., Cheng, C. and Ding, J. (2022) Revisiting Group Oriented Secret Sharing Schemes. *Information Sciences*, **589**, 751-769. https://doi.org/10.1016/j.ins.2021.12.053