A Verifiable Multi-Secret Sharing Scheme for Hierarchical Access Structure

Irfan Alam , Amal S. Alali , Shakir Ali * , Muhammad S. M. ASRI

Posted Date: 30 May 2024

doi: 10.20944/preprints202405.2061.v1

Keywords: access structure; multi-secret; hierarchy; verification; secret sharing; polynomial

Article

A Verifiable Multi-Secret Sharing Scheme for Hierarchical Access Structure

Irfan Alam [1], Amal S. Alali [2], Shakir Ali [3,4,*] and Muhammad S. M. Asri [4]

[1] Department of Computing Science and Engineering, VIT Bhopal University, India; irfanalam@vitbhopal.ac.in
[2] Department of Mathematical Sciences, College of Science, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; asalali@pnu.edu.sa
[3] Department of Mathematics, Faculty of Science, Aligarh Muslim University, Aligarh 202002, India
[4] Institute of Mathematical Sciences, Faculty of Science, University of Malaya, Kuala Lumpur, Malaysia; sufi.maths@gmail.com
* Corresponding author: shakir.ali.mm@amu.ac.in

Abstract: Sharing confidential information is a critical concern in today's world. Secret sharing schemes facilitate the sharing of secrets in a way that ensures only authorized participants (shareholders) can access the secret using their allocated shares. Hierarchical secret sharing schemes (HSSSs) build upon Shamir's scheme by organizing participants into different levels based on priority. Within HSSS, participants at each level can reconstruct the secret if a specified number, denoted as the threshold value (t), or more of them are present. Each level has a predetermined threshold value. If the number of participants falls below the threshold at any level, higher-level participants must be involved in reconstructing the secret at lower levels. Our paper proposes schemes that implement hierarchical access structures and enable the sharing of multiple secrets. Additionally, our proposed scheme includes share verification. We have analyzed potential attacks and demonstrated the scheme's resistance against them. Through security analysis and comparison with existing schemes, we highlight the novelty and superiority of our proposed approach, contributing to advancements in secure information sharing practices.

Keywords: access structure; multi-secret; hierarchy; verification; secret sharing; polynomial

MSC: 94A62; 94A60; 94A17

1. Introduction

Information such as encryption keys, missile launch codes, and numbered bank accounts must be highly confidential. Exposure to such sensitive information could be dangerous. Secret sharing schemes provide an efficient way of storing such sensitive and vital information and prevent unauthorized access. Apart from core cryptography, Researchers have been using secret sharing concepts in various applications such as the cloud and IoT. Recently, Gutte and Paraser [15] have used secret sharing for visual cryptography and suggested a weed optimization algorithm for image sharing. Similarly, Wang et al. [44] , and Ren et al. [35] have worked on low latency cloud-based indoor localization system and secure, anonymous data aggregation schemes, respectively. Considerable work has been done on this topic during the last few years (cf.; [9,12,19,24,26,32,34,36,42] where further references can be found).

Initially, some core concepts of algebra were used by authors to design secret sharing schemes. Shamir [39] used polynomials, Blakley [6] used hyperplane geometry and Simmons [40] as well as Asmuth and Bloom [1] used Chinese remainder theorem. In secret sharing schemes, secret S is distributed among n shareholders $P_1, P_1, \ldots, P_n$ in such a way that t shareholders or more than t shareholders can reconstruct the secret but less than t shareholders know nothing about the secret. Such a scheme is known as the (t, n)-threshold scheme. Schemes given by [1,6,39] have several common drawbacks as follows:

1. These are single secret sharing schemes.
2. For every new secret, a new share has to be generated for every participant after the reconstruction of the previous secret

 doi:10.20944/preprints202405.2061.v1

3. Private channels are essential for the communication between dealers and participants and among the participants.
4. These schemes are not capable of identifying the cheater.

To solve the first and the second problem, "multi secret sharing schemes" have been introduced [20,21,25]. Instead of having a single secret, multiple secrets are shared among the participants in a multi-secret sharing scheme. To include verification and cheater detection, a "Verifiable secret sharing scheme" was proposed in [13,43]. In [17,18], Harn et al. proposed the protected secret sharing scheme to avoid a separate communication channel while exchanging shares among different shareholders. The application of Shamir's scheme is an ideal for the condition where all participants(shareholders) play the same role and there is no distribution of share-based on priority or any unique properties. However, employees are categorized based on their work responsibilities in organizations such as multinational companies and educational institutions. Among several structures, the Hierarchical structure is trendy in which every participant has some weight according to his/her role. Shares are distributed or assigned according to their weight. Hierarchical secret sharing schemes are proposed in the literature, [2,30,40,48,49] .
In hierarchical secret sharing schemes, all the participants are divided into m disjoint sets called levels say $l_1, l_2, ...l_m$. The i^{th} level consists of n_i participants with t_i threshold. In reconstruction of the secret there may be two situations: In the first situation particular level l_i has t_i or more participants on the same level while in the other situation the number of participants in level l_i is less than t_i. In the second situation involvement of the higher level participant is needed.
Let us assume that in a particular level l_i participants are less in number say r_i, than the t_i. So $t_i - r_i$ remaining participants are needed from the upper level to reconstruct the secret. In this paper the level l_i is higher than the level $l_{i+1}, 1 \leq i < m$.

In 2004, Yang et al. [46] proposed a unique multi-secret sharing scheme using a single polynomial, known as the YCH scheme. Low computation and less number public values are required in the YCH scheme. In the YCH scheme, a single polynomial is used for multiple secrets instead of using separate polynomials for individual secrets. We have included a YCH scheme for each level in our work, making the scheme efficient. We have used two variable one-way functions for verifiability, which verify the dealer and other participants. Here we summarize the contribution of this paper:

1. Proposed scheme is efficient due to the use of YCH scheme.
2. The proposed scheme can quickly identify the cheater, whether the dealer or the other participants.
3. Participant's share can be used for both the reconstruction and verification.

The rest of the paper is organized as follows. In Section 2, related literature is explained. In Section 3, we present preliminaries related to our proposed scheme. Section 4 deals with the identification of problems and motivation. Our proposed scheme is discussed in Section 5. In Section 6, the security and performance analysis of the scheme is discussed. In Section 7, a comparison with exiting schemes is explained. Finally, we conclude the paper with future work in Section 8.

2. Related Work

The Shamir [39] and Blakley [6] threshold secret sharing schemes are two particular examples of hierarchical secret sharing (HSS) in which all participants have the same privileges. In order to improve the applicability of hierarchical secret sharing, many researchers have focused on specific families of access structures. Blundo et al. [7] have focused on graph-based access structure, Pardo et al. [33] explained bipartite access structure and Tentu et al. [41] includes multipartite access structure, compartmented access structure, and hierarchical access structure.

In 1979, the weighted thresold secret sharing mechanism was suggested by Shamir [39]. However, this approach is inefficient since it assigns multiple shares to each participant equal to its integral weight. Simmons [40] then proposed a multipartite access structure in 1988, defining the compartmented

 doi:10.20944/preprints202405.2061.v1

access structure and the hierarchical access structure. Following Simmons, Brickell [8] proposed a strategy for constructing an optimal secret sharing scheme that takes into account multilevel and compartmented access arrangements. However, the approach is inefficient since nonsingular matrices require exponential operations. The multipartite access structure is defined as the split of all members of a group into subsets, with members of the same subset having the same rights. The compartmented access structure and the hierarchical access structure are two types of multipartite access structures. The conjunctive hierarchical access structure and the disjunctive hierarchical access structure belong to the hierarchical access structure family. In 2009, Lin et al. [28] had incorporated some modifications to Shamir's scheme [39] and explained hierarchical secret sharing(HTSS) scheme with two types of variations." Multilevel threshold secret sharing (MTSS), and compartmented threshold secret sharing (CTSS)".
Verification of shares is also one of the major concerns in secret sharing schemes. In [13,43] authors have specifically explained the verification of shares in a secret sharing scheme. In 2015, Chanu et al. [10] used Two variable one-way functions to verify the correctness of the received share. Further, in 2017, Basit et al. [4] used Shamir's scheme with the successive application of one-way function and shifted and key technique to propose Multi-stage, Multi-secret sharing for hierarchical Access Structure. Apart from the above papers, the Hierarchical secret sharing (HSSS) scheme are discussed in [3,4,10,17,28,29,47], but his scheme lacks fairness. In 2018, Banerjee et al.[3] proposed Cheating detection and cheater Identification for hierarchical structure but lacks correctness. In 2021 Bisht and Deshmukh [5] proposed work on multi-level secret sharing but lacks fairness and perfectness. Similarly, Yuan et al. [47] used homogenous recurrence relation to propose a new efficient scheme that deals with the multi-secret hierarchical scheme.
This scheme has been proposed to overcome the shortcomings of the above-discussed schemes and incorporate the features in the following ways:

- It supports the hierarchical access structures as discussed in the first paragraph of the current section. It improves and enhances the applicability of the hierarchical access structure.
- It supports weighted threshold secret sharing as discussed in the second paragraph without any exponential operation and extra burden.
- It supports secret sharing with multi-stage, multi-level properties with verification of shares lacking in schemes discussed in the third and fourth paragraphs.
- In the last paragraph of this section, novel schemes is discussed. These schemes do not explain security features such as correctness and forward/backward secrecy.
  Proposed schemes provide essential security features such as fairness and correctness. At the same time, the proposed scheme's computational cost and storage cost is much less.

3. Preliminaries/Foundations

This section describes some of the preliminaries required to design our scheme.

3.1. Shamir's (t, n) Secret Sharing Scheme

In secret sharing principle objective is to partition the secret S into n pieces $s_1, s_2, \ldots, s_n$ such that:

1. Learning of t or more s_i pieces makes S to be uniquely determined.
2. Learning of any $t-1$ or less s_i pieces leaves S totally unpredictable.

This scheme depends on polynomial interpolation.The fundamental idea of Adi Shamir's threshold scheme can be understand by a simple example:

1. At least 2 points are necessary to draw a line. (i.e, one point is not sufficient)
2. At least 3 points are necessary to draw a parabola (i.e, less than 3 points are not sufficient)
3. Similarly, it takes at least 't' points to draw a polynomial of degree '$t-1$' (i.e, less than t points are not sufficient).

 doi:10.20944/preprints202405.2061.v1

Following are the main phases of (t, n) threshold scheme, where n is total number of shareholders and t is minimum number of shareholders necessary to reconstruct the secret S. **Distribution phase**::

1. Select a prime number Q
2. Randomly select a function $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{t-1}x^{t-1}$
3. Compute (i, g(i)) corresponding to the i^{th} shareholder, $i = 1, 2, \ldots, n$.
4. These points (i, g(i)) are distributed securely to n share holder/participants

Reconstruction phase:

1. Compute Lagrange's interpolating polynomial using t shares

$$g(x) = \sum_{i=1}^{t} g(i) \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} mod\ Q$$

2. In this way, we get the polynomial in the form

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{t-1}x^{t-1},$$

where b_0 = S, is the secret.

3.2. Hierarchical Access Structure

Access Structure(Γ) Recovery of secret is authorized for some group of people and it is unauthorized for another group of people. Those sets which are authorized is known as access structure. **Adversary Structure($\overline{\Gamma}$)** The set of all non authorized sets that do not have any information related to the secret, is said to be an adversary structure.
In (t, n) threshold access structure any set of t or more participants out of n is said to be an authorized set and any set less than t in number is said to be non-authorized set. Let λ be the set of n participants. In Set builder form a (t, n) threshold access structure and the corresponding adversary structures are::

$$\Gamma = \{X \in 2^{\lambda} : |X| \geq t\}$$

and

$$\overline{\Gamma} = \{X \in 2^{\lambda} : |X| < t\}$$

respectively.
In 2006, Herranz et al. [22] explained importance of multipartite structure. According to Herranz "In multipartite structure the set of players is divided into K disjoint classes, and all players in each class play exactly the same role within the access structure. These access structures can make a lot of sense in real life applications, where persons or machines are divided into different groups according to their position in a company, their responsibilities, their computational resources or their probability of being corrupted by an attacker ".
A multipartite access structure splits the set of participants in λ into m disjoint sets$l_1, l_2 \cdots, l_m$ called levels and all participants in each level play exactly the same role inside the particular access structure.

3.3. Overview of YCH Scheme

Initialization phase
In this scheme following notations are used :

1. (t, n)- scheme. where t is for threshold and n is for number of participants.
2. $B_1, B_2, \ldots, B_k$, denotes the k secrets to be shared.
3. n secret shadows $s_0, s_1, s_2, \ldots, s_n$ are randomly chosen by the dealer and distributed to the participants through a secure channel.
4. A random value 'r' is chosen.

 doi:10.20944/preprints202405.2061.v1

5. A 2-variable 1-way function h(r,s_i) , $i = 1, 2, \ldots, n$. is chosen.

Construction phase

1. $k \leq t$ (Number of secrets are less than the threshold)
   (a) A prime number 'Q' is chosen by the dealer.
   (b) The dealer choose a polynomial $f(x) \bmod Q$. Degree of polynomial is $(t-1)$ where,
   (c) $B_1, B_2, \ldots, B_k$ are the secrets to be shared and $b_1, b_2, b_3, \ldots b_{t-k}$ are random numbers.
   (d)
   $$f(x) = B_1 + B_2x + , \ldots , + B_kx^{k-1} + b_1x^k + b_2x^{k+1} + \cdots + b_{t-k}x^{t-1} mod\ Q$$
   (e) For every i^{th} participant the dealer computes $g_i = f(h(r, s_i)) \bmod Q$
   (f) Publish $(r, g_1, g_2, \ldots, g_n)$.
2. $k > t$ (Number of secrets is greater than the threshold)
   (a) A prime number Q and a polynomial $f(x) mod\ Q$ is chosen by dealer. Degree of polynomial is $(k-1)$. where $B_1, B_2, \ldots, B_k$ are the secrets.
   $$f(x) = B_1 + B_2x + \cdots + B_kx^{k-1} mod\ Q$$
   (b) For i=1 to n. $g_i = f(h(r, s_i)) mod\ Q$ is computed.
   (c) For $i = 1$ *to* n. $f(i) mod\ Q$ is computed
   (d) calculated values like $r, g_1, g_2, \ldots, g_n$ are publicly published.
   (e) $f(1), f(2), \ldots, f(k-t)$ are also published in public.

Recovery phase

In order to recover the secrets $B_1, B_2, \ldots, B_k$,

1. Each participant uses his/her share to compute $h(r, s_i)$ (for i=1 to t)
2. The polynomial $f(x)$ is determined as follows:
3. $k \leq t$ (Number of secrets are less than the threshold)

$$\begin{aligned} f(x) &= \sum_{i=1}^{t} g_i \prod_{j=1, j\neq i}^{t} \frac{x - h(r, s_j)}{h(r, s_i) - h(r, s_j)} mod\ Q \\ &= B_1 + B_2x + \cdots + B_kx^{k-1} + a_1x^k + a_2x^{k+1} + \cdots + a_{t-k}x^{t-1} mod\ Q. \end{aligned}$$

4. for $k > t$(Number of secrets is greater than the threshold)

$$\begin{aligned} f(x) &= \sum_{i=1}^{k} g_i \prod_{j=1, j\neq i}^{k} \frac{x - h(r, s_j)}{h(r, s_i) - h(r, s_j)} + \sum_{i=1}^{k-t} f(i) \prod_{j=1, j\neq i}^{k-t} \frac{x - j}{i - j} mod\ Q \\ &= B_1 + B_2x + \cdots + B_kx^{k-1} mod\ Q. \end{aligned}$$

5. from the above equations, we get the secrets

$$B_1, B_2, \ldots, B_k$$

3.4. 2- Variable 1- Way Function

Definition A 2-Variable,1-way function $h(r, s)$ is a function that maps a random value r and a share s onto a bit string of fixed length.

Properties: It contains following properties:

1. when r and s, are given $h(r, s)$ is easily computable. But for a given$s$ and $h(r, s)$, it is very difficult to compute r.
2. It is hard to compute $h(r, s)$ when there is no knowledge of s.
3. For the given s, it is hard to find two different values r_1 and r_2 that satisfy the situation $h(r_1, s) = h(r_2, s)$.
4. It is tough to compute s, for the given r and $h(r, s)$.
5. If we have pairs of r and $h(r, s)$, it is difficult to find $h(r^{'}, s) = h(r, s)$ for which $r^{'} \neq r$.

 doi:10.20944/preprints202405.2061.v1

4. Identification of Problem and Motivation

In all the existing scheme, a separate polynomial is taken corresponding to each secret which results in overhead of public values and calculations. Verification in hierarchical system is included in papers like [3] with some limitations. In the present work, we try to reduce the limitations in the verification phase.

4.1. Contribution

In our work, we have proposed "multi-secret sharing scheme for hierarchical access structure "using the YCH scheme. By using YCH scheme we get following advantages:

1. It permits parallel reconstruction of secrets.
2. Number of the secrets to be distributed can be dynamically determined.
3. This scheme is of multi-use. Furthermore, fewer public values, less storage, as well as computing time, are needed in our scheme.

By using 2-variables 1-way function we get the following advantages:

1. Any participant can identify the cheater whether he/she is the dealer or the participant.
2. There is no need of secure channel between the Dealer and the participant.
3. This scheme can also detect the invalid shares.

5. Proposed Scheme

5.1. Overview

All participants are classified into m levels. Each level has fixed (t, n) pair where t is the threshold out of n participants. Dealer chooses pseudo share s_i^l for the i^{th} participant at level l. Pseudo share is distributed through secure channel. $B_1, B_2, \ldots, B_k$ are the secrets. Using YCH scheme dealer computes actual share (d_i^l) for each participant. public share (Z_i^l) is calculated on addition of actual share in the 1-way function.

In the Reconstruction phase, the actual share of the participants is calculated by subtracting 1-way function from the public share. This actual share is used in the Lagrange interpolation polynomial and generates the polynomial having coefficients as secrets. If share's number in a particular level is less than its threshold value then upper-level shareholder provides his share to reconstruct the secret.

5.2. Initialization

1. Number of participants is n.
2. Number of level is m.They are $l_1, l_2, \ldots, l_m$.
3. Each level is associated with a (t_j, n_j), $j \in [1, m]$ access structure.
4. Dealer chooses n shares s_i^j, $i \in [1, n_j]$, $j \in [1, m]$.

5.3. Distribution

At each level l there may be two situations:

- Number of secrets k is less than the threshold
- Number of secrets k is more than the threshold.

1. $k \leq t_j$ (number of secret is less than or equal to t_j)
   (a) A prime number Q is chosen by the dealer.
   (b) The dealer construct polynomial $f(x) \bmod Q$. The degree of polynomial is $(t_j - 1)$. Let ,

$$f(x) = B_1 + \cdots + B_k x^{k-1} + b_1 x^k + \cdots + b_{t-k} x^{t-1} mod\ Q,$$

   where $B_1, B_2, \ldots, B_k$, are the secrets,

 doi:10.20944/preprints202405.2061.v1

(c) $b_1, b_2, b_3, \ldots, b_{t_j-k}$,$j \in [1, m]$ are randomly chosen numbers.
(d) For the i^{th} participant the dealer computes $g_i = f(h(r, s_i))mod\ Q$, $i \in [1, n]$.
(e) Publish $(r, g_1, g_2, \ldots, g_n)$.

2. $k > t_j$(Number of secrets is greater than t_j.)

(a) A prime number Q is chosen.
(b) Dealer construct a polynomial $f(x)mod\ Q$ of degree $(t_j - 1)$. Let

$$f(x) = B_1 + B_2x + \cdots + B_kx^{k-1} mod\ Q,$$

where $B_1, B_2, \ldots, B_k$ are the secrets.
(c) For $i = 1, 2, 3, \ldots, n$. $g_i = f(h(r, s_i))mod\ Q$ is Computed.
(d) For $i = 1$ *to* n. $f(i)mod\ Q$ is Computed
(e) calculated values like $r, g_1, g_2, \ldots, g_n$ are made public
(f) $f(1), f(2), \ldots, f(k - t)$ are published in public.

For both the cases, dealer perform the following calculations:

1. Calculate actual share (d_i^l) and pseudo share(Z_i^l) for the i^{th} participant of level l using following formulas:
$$d_i^l = f(ID_i^l) \ \ and \ \ Z_i^l = d_i^l + g(s_i^l)$$
where g is one-way function in which s_i^l denotes the share of i^{th} participant of level l
2. Calculate actual share ($d_i^{l_u}$) and pseudo share ($Z_i^{l_u}$) of the i^{th} participant of upper level u using formula::
$$d_i^{l_u} = f(ID_i^{l_u}) \ \ and \ \ Z_i^{l_u} = d_i^{l_u} + g(s_i^{l_u})$$
where $ID_i^{l_u}$ is the identifier for i^{th} element of u^{th} level.
3. s_i^l and $s_i^{l_u}$(if needed) is distributed to each participant using a secure channel.
4. All $Z_i^{l_r}$,r values are published.

5.4. Reconstruction

Each participant compute actual share of other participants involved in the reconstruction by using formula

$$d_i^l = Z_i^l - g(s_i^l)$$

and then following two cases are considered

Case 1

Particular level have sufficient number of participant i.e greater or equal to threshold,then participant of same level exchange their pseudo share and use the following formula:

1. for $k \leq t$

$$\begin{aligned} h(x) &= \sum_{i=1}^{n} d_i \prod_{j=1, j\neq i}^{n} \frac{x - ID_j}{ID_i - ID_j} mod\ Q \\ &= B_1 + B_2x + \cdots + B_kx^{k-1} + a_1x^k + a_2x^{k+1} + \cdots + a_{t-k}x^{t-1} mod\ Q. \end{aligned}$$

2. for $k > t$

$$\begin{aligned} h(x) &= \sum_{i=1}^{n} d_i \prod_{j=1, j\neq i}^{n} \frac{x - ID_j}{ID_i - ID_j} + \sum_{i=1}^{k-t} f(i) \prod_{j=1, j\neq i}^{k-t} \frac{x - j}{i - j} mod\ Q \\ &= B_1 + B_2x + ... + B_kx^{k-1} mod\ Z \end{aligned}$$

Case 2

Particular level have insufficient number of threshold, then the share of the upper level participant for this level is used in the above formula. Thus we get the secret $B_1, B_2, B_3, \ldots, B_K$.

 doi:10.20944/preprints202405.2061.v1

5.5. Verification

Following steps are involved in verification phase:

1. Pseudo share s_i^l is distributed to participants securely by dealer.
2. Each i^{th} participant uses his actual share (d_i^l) in two variable one way function with random variable r. Let that two way variable function is $q_i(r, d_i^l)$.
3. Calculated q_i values made public.
4. Public share Z_i^l is also published.
   Now at the time of exchange of shares:
5. Each participant compute actual share of each participants

$$d_i^l = Z_i^l - g(s_i^l).$$

6. Using that actual share , $q_i(r, d_i^l)$ is calculated for i_{th} participant.
7. If $q_i(r, d_i^l)$ is equal to already public value of q_i then participant share is valid otherwise the actual share of participant is not valid.
8. In a similar way, an individual participant will be able to check the legitimacy of his/her share given by the dealer.

5.6. Example

We can understand proposed scheme more clearly by following example with small parameters. Let us consider the hierarchical system with two levels l_1 and l_2. Upper level is l_1 and lower is l_2. Dealer has two secrets, i.e., $B_1 = 2$ and $B_2 = 3$. Identifiers $ID_1^{l_1} = 1$, $ID_2^{l_1} = 2$, $ID_3^{l_1} = 3$ for the level l_1 and $ID_1^{l_2} = 4$, $ID_2^{l_2} = 5$, $ID_3^{l_2} = 6$ for the level l_2.
Dealer chooses shares $s_1^1 = 10$, $s_2^1 = 11$, $s_3^1 = 12$ for the level-1 and $s_1^2 = 13$, $s_2^2 = 14$, $s_3^2 = 15$ for the level-2.

5.6.1. Distribution

For the sake of easiness in calculation, we perform calculations on 2nd level.

$$h(x) = 2 + 3x + 4x^2 mod 23$$

calculate actual share for the i^{th} participants for the level-2 by using formula: $d_i^{l_r} = \mathrm{h}(ID_i^{l_r})$ are

$$d_1^{l_2} = 9,\ d_2^{l_1} = 2,\ d_3^{l_1} = 3$$

Actual share of i^{th} participants of upper level for the level-2

$$d_1^{l_{2,1}} = h(ID_1^{l_1}) = 9.$$

Similarly, we obtain $d_2^{l_{2,1}} = 1$ and $d_3^{l_{2,1}} = 1$
Choose one-way function $g = 2^{s_i^{l_r}} \bmod 23$.
Compute pseudo share of the i^{th} participants of the level R.

$$Z_i^{l_r} = d_i^{l_r} + g(s_i^{l_r}).$$

Therefore, we get $Z_1^{l_2} = 13$, $Z_2^{l_2} = 10$, $Z_3^{l_2} = 19$.
Similarly, pseudo share of the participants of upper level for the level-2 are

$$Z_1^{l_{2,1}} = 21,\ Z_2^{l_{2,1}} = 2,\ Z_3^{l_{2,1}} = 3.$$

Publish all pseudo share and distribute $S_i^{l_r}$ to every participants through secure channel.

 doi:10.20944/preprints202405.2061.v1

Table 1. Comparison in tabular form.

Comparison among the existing scheme.						
Property	Basit et al. [4]	Banerjee et al. [3]	Zhang et al. [48]	Tentu et al. [41]	Chen et al. [11]	proposed scheme
hierarchy	Yes	Yes	No	Yes	Yes	yes
Reusable	Yes	Yes	Yes	No	No	Yes
Multi-secret	Multi	Multi	Multi	Single	Single	Multi
Based on	LPI	LPI	YCH	LPI	Polynomial	YCH
Ideal and Perfect	Yes	Yes	Yes	Yes	Yes	Yes
Cheating detection	partially	Conditional	Complete	Partially	Complete	Compete
Correctness	No	No	No	No	yes	yes
Forward secrecy	No	No	No	No	No	yes
Fairness	No	No	Yes	No	yes	yes

5.6.2. Reconstruction

In reconstruction phase each participant has pseudoshare and the share $s_i^{l_r}$ for the particular level actual share is computed by using

$$d_i^{l_r} = Z_i^{l_r}\text{-}g(s_i^{l_r}).$$

Hence, we have

$$d_1^{l_2} = 9, d_2^{l_2} = 2, d_3^{l_2} = 16.$$

Similarly, actual share of the upper level participants for level-2 is as follows:

$$d_1^{l_1} = 9, d_2^{l_1} = 1, d_3^{l_3} = 1.$$

Now, there is possibility of two case:

- Particular level (here level-2) has sufficient number of participants
- Particular level has less no of participants then upper level participant takes part in reconstruction of secret.

Case-1

$$\begin{aligned} h(x) &= \sum_{i=1}^{t} d_i^l \prod_{j=1, j\neq i}^{t} \frac{x - ID_j}{ID_i - ID_j} mod\ Q \\ &= B_1 + B_2 x + .. + B_k x^{k-1} + a_1^i x^k + a_2^i x^{k+1} + a_{t-k}^i x^{t-1} mod\ Q \\ &= 9 * \frac{(x-5)(x-6)}{(4-5)(4-6)} + 2 * \frac{(x-4)(x-6)}{(5-4)(5-6)} + 3 * \frac{(x-4)(x-5)}{(6-4)(6-5)}. \end{aligned}$$

That is,

$$h(x) = 2 + 3X + 4X^2. \text{ So the secrets are 2, and 3.}$$

Case-2 No. of participants in level-2 is one less than the threshold. Therefore, one of upper level participants takes part in reconstruction. Hence, the pair of (ID,actual share) are::(4,9)(5,2)(1,9) applying same formula as in the Case-1.

$$h(x) = 9 * \frac{(x-5)(x-1)}{(4-5)(4-1)} + 2 * \frac{(x-4)(x-1)}{(5-4)(5-1)} + 3 * \frac{(x-4)(x-5)}{(1-4)(1-5)}$$

$h(x) = 2 + 3x + 4x^2$. Thus, the secrets are 2 and 3.

 doi:10.20944/preprints202405.2061.v1

6. Security and Performance Analysis

While choosing a scheme, we must be clear about the capabilities of adversary along with the explanation of security properties it supports. There must be an strong analysis about computational and communication cost. In this section, we have explained all these concepts in details.

6.1. Adversary Model

There must be an adversary model against which the scheme is safe. The most common adversarial model for analyzing security protocols was presented by Dolev and Yao [14] in 1983. Apart from this, we have considered two types of adversaries:

- **Insider Adversary**, These are legitimate shareholders who acquired shares from the dealer.
- **Outsider Adversary**, The external adversary is an attacker who does not own any of the dealer's shares but may try to gain unauthorized access.
  In general, a dealer is considered as trustworthy as in [3], but here we have considered the worst situation that the dealer is committing fraud by providing fake shares to the participants.

6.2. Security analysis

Any scheme must pass through formal and Informal analysis to verify its applicability in current scenario. In proposed scheme, We have used Random Oracle Modal (RoM) for formal analysis. In informal analysis we have proved our scheme safe from several attacks.

6.2.1. **Formal Security Analysis (Random Oracle Model)**

A cryptographic hash function H is treated as a really random function by the random-oracle model. The random-oracle model more particularly hypothesises the existence of a public, random function H that can only be evaluated by "querying" an oracle, which can be thought of as a "black box," that returns $H(x)$ when given input x. A formal approach that can be used to create and verify cryptographic methods is provided by the random-oracle model. In 2014, Herranz et al. [23] provided the formal definition of security for MSS in the random oracle model. Moreover, they proposed an MSS formally proved its computational security in ROM. As far as we know, that is an MSS's first formal security analysis. Security analysis of multi secret sharing scheme has been performed by [31]. In this section, we prove the computational security of the proposed scheme Ω assuming that the hash function H behaves as a random oracle.
Before we proceed with the proof, the following are the assumptions:

- We assume the proposed scheme as the set of tuples, $\Omega = (Int, dist, Rec)$ where Int stands for Intilization/setup phase, dist stands for distribution and Rec is for recovery phase.
- PP(Public parameters)= $((p, H, \rho, t)$

  1. p : prime number p > n such that p is at least λ bits long
  2. H : a hash function, $H : \mathbb{Z}_p^* \rightarrow \mathbb{Z}$
  3. ρ: Set of participants
  4. t: threshold
- There is an adversary A_1 contains set of participants ρ and threshold value t.

Theorem For an adversary λ, we have

$$\left| pr\left[GMS_{A_1}^{SA}(\lambda) = 1 \right] - \frac{1}{2} \right| \leq \left| \frac{q_H^n}{\lambda^{\lambda+2}} + 0(\frac{q_H^n}{2^{2\lambda+1}}) \right|$$

here adversary makes at most qH queries to the random oracle for H against the GMS and Ω.
Proof For proof we follow the following steps:
Step1 We act as the challenger of the security game $G1$ described in [31].
Step2 We pass public parameters to the initialization algorithm and send the result to the adversary.
Step3 $A1$ broadcast $B \epsilon \rho$, we choose $sh_i \epsilon Z_p$, $\forall p_i \epsilon \rho$

 doi:10.20944/preprints202405.2061.v1

Step4 after masking hash query x to the random oracle H, if $x\epsilon\{sh_i\}p_i\epsilon B$ then abort the game, otherwise proceed for the next step.
Step4 a random value is $k\epsilon Z_p$ is chosen and send to adversary. At the same time, (x,k) is saved in the table.
Step4 Two global secrets

$$S^0 = (s_1^0, s_2^0, \ldots, s_l^0)$$
$$\neq (s_1^1, s_1^2, \ldots, s_l^1) = S^1$$

are broadcasted by adversary A_1.
Step5 We choose a random value $r\epsilon Z_p^*$ such that $r \neq sh_i$ for $P_i\epsilon\rho$ and adversary doesn't query $r, 2r, \ldots, lr$ to the random oracle H.
Step6 a random polynomial $f(x)$ is chosen where, $f(0) = r$ and compute $h_i = H(sh_i)$ and $r_i = f(i) - h_i mod p$ and again store (sh_i, h_i) in the hash table. Similarly choose l no. of random values $(k_1, \ldots, k_l)\epsilon Z_p$ and store $(r, k_1), (2r, k_2), \ldots, (lr, k_l)$ in the hash table.
Step7 Choose a random bit $b\epsilon\{0,1\}$ and compute $y_j = k_j - s_b^j mod p \forall 1 \leq j \leq l$ and give shares of corrupted players $(i, sh_i)_{p_i\epsilon B}$. along with this public output $Out_{pub} = \{r_1, r_2, \ldots, r_n, y_1, \ldots, y_l\}$ are also shared.
Step8 after continuous query to $H(.)$, adversary A_1, outputs a bit $b^{'}$ which is defined in the following equation

$$o/p = \begin{cases} 1, \text{if } b = b^{'} \\ 0, \text{if } b \neq b^{'} \end{cases} \quad (1)$$

from above steps, we conclude that A_1 is not allowed to query sh_i such that $p_i\epsilon B$ and $1 \geq j \leq l$.

6.2.2. Informal Security Analysis

Any proposed protocol must be passed through the following goals:

1. **Correctness** : In verification phase Each participant compute actual share of other participants $d_i^l = Z_i^l - g(s_i^l)$ using that actual share , $q_i(r, d_i^l)$ is calculated for i_{th} participant. If $q_i(r, d_i^l)$ is equal to already public value of q_i then participant share is valid otherwise the actual share of participant is not valid.
2. **Forward secrecy**: keys like $q_i(r, d_i^l)$ can only be computed or stored by members of the closed communication group; if a member leaves the group, the departing member will be unable to access the content of future conversations.
3. **perfectness**: We use Shamir's (t, n) secret sharing scheme for share distribution at each level in the proposed scheme. It is well known that fewer than t participants in Shamir's (t, n) secret sharing scheme cannot reconstruct the secret. Hence, our scheme is also perfect.
4. **Fairness of secret sharing** One desirable quality in secret sharing is Fairness, which indicates that if one member obtains the secret, the other participants are not harmed. Halpern and Teague [16] were the first to offer rational cryptographic protocols in 2004. They pointed out that any method for reassembling secrets with a well-known upper constraint on the running duration is unstable and that parties will not submit anything in the final round since they have no reason to do so because the other participant does. Regrettably, earlier secret-sharing systems necessitated numerous rounds with high overheads. Zhang et al. [48,49] explain the scheme's. Fairness but leave out the access mechanism. To summarise, existing fairness schemes necessitate a trusted third party or many rounds of communication. The proposed scheme provides Fairness without the dependency on a third party and extra overheads in communication.
5. **Freshness of keys**: In the proposed scheme, all the exchangeable values depend upon the random bi-variate polynomial. It makes pseudo share, and shares are always fresh. Hence, it is impossible to impersonate a member by recording a previously used key.
6. **Eavesdropping attack** In proposed scheme, each i^{th} participant uses his actual share (d_i^l) in two variable one way function with random variable r which makes it independent of public

 doi:10.20944/preprints202405.2061.v1

parameters. Therefore, an adversary will not be able to know any secret information from communication parameters. So, the proposed scheme is safe from eavesdropping activities.

7. **Cheating identification** In the proposed scheme, an individual participant can check the legitimacy of his/her share given by the dealer. Thus, the proposed scheme provides cheating identification.
8. **Verifiability** In the reconstruction phase, participants can verify shares received from other participants and dealers. On the other hand, a dealer can also verify the participant's shares. Thus, the proposed scheme provides verifiability.
9. **Unconditional security** While exploring the security analysis, both types of adversaries are considered with their capacity to the full extent. It implies that no assumptions are made about an adversary's computing power and resources.

6.3. Performance analysis

6.3.1. Computational cost

In the proposed scheme, each member must compute pairwise shared keys with others in the verification phase. According to Horner's rule [27], t and h computations are required for each univariate polynomial of $t-1$ and $h-1$ degree. In the proposed protocol, calculation reduces to Shamir's secret sharing scheme. According to [38] computational time for 8 person is 0.0039 second. There is a slight change in computation time as we increase the number of persons, Basit et al. [4] uses extra polynomial, and Tentu et al.[41] uses modular exponentiation, which increases computational cost. The computational cost for the same no. of persons are 0.2439 second and 80.003 second of [4] and [41] respectively. Similarly, computational cost for 8 persons in [49] is 0.23 second. So we conclude that the computation cost is meager compared to the other existing schemes. For more clarity, we have presented a graphical comparison of schemes in terms of computational time and security features it supports in Figure 1.

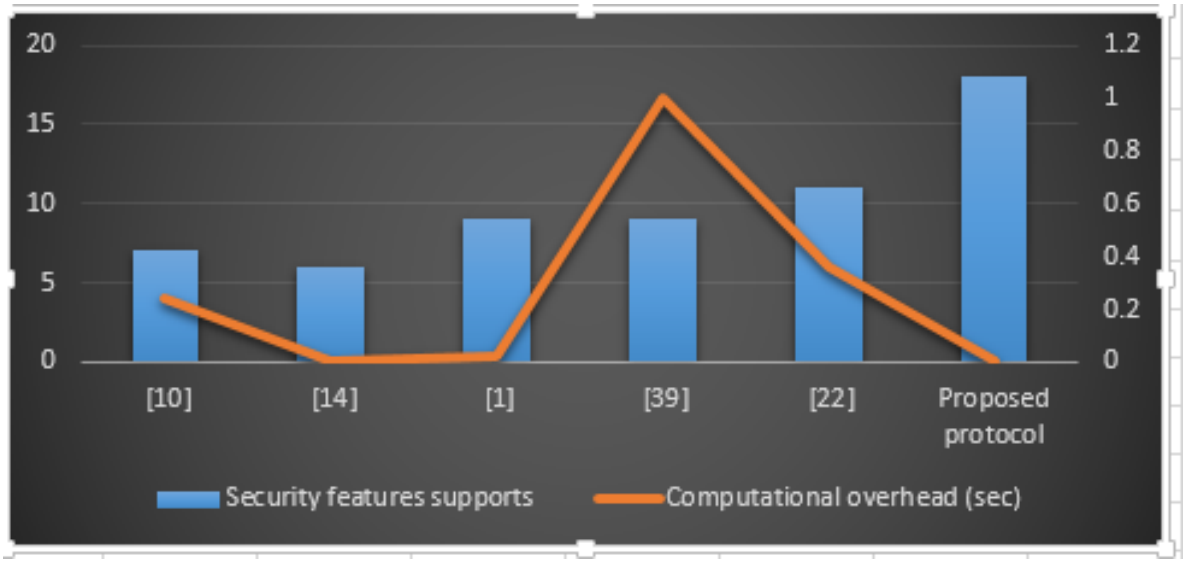

Figure 1. Comparison of computational cost and security features supported

6.3.2. Storage Cost

Each member has to store only uni-variate polynomial of modulus $\mathbb{P}$. So the storage requirement for each member is $t \log \mathbb{P}$ bits. This polynomial-based modulus is far less than the public-key-based modulus [45]. Here threshold is t. To get collusion-free authentication, each member must simultaneously deal with $t+1$ univariate polynomial. So overall storage cost is significantly less compared to symmetric key-based schemes.

 doi:10.20944/preprints202405.2061.v1

7. Comparison with Existing Scheme

The proposed scheme uses the YCH scheme, while all other schemes for hierarchical access structures use simply shamir's scheme. In the proposed scheme "Multiple-secrets "are shared among a group of people for different levels. Our scheme provides a mechanism for verifying the shares, which is also new for hierarchical access structures. This is more efficient than other schemes. Basit et al. [4] used Shamir's scheme with the successive application of one-way function and shift key technique to propose Multi-stage, Multi-secret sharing for hierarchical Access Structure. Apart from the above papers, the Hierarchical secret sharing (HSSS)scheme is discussed in [3,5,28] but his scheme lacks fairness. Banerjee et al. [3] proposed Cheating detection and cheater Identification for hierarchical structure but lacks correctness. Bisht et al. [5] proposed work on multi-level secret sharing but lacks fairness and perfectness. Similarly, Yuan et al. [46] used homogenous recurrence relation to propose a new efficient scheme that deals with a multi-secret hierarchical scheme. It is a novel work but lacks explanation about correctness and forward/backward secrecy Our scheme also avoids the problem of Chen et al. scheme's [11] which requires checking the non-singularity of multiple matrices. Furthermore, during the entire scheme, each participant keeps only one share, which is as long as the secret, indicating that our method is optimum. Furthermore, despite requiring more public values, our scheme can simultaneously disclose many secrets. In Table 1, we can see the importance of the present scheme in comparison with other schemes.
In our proposed scheme, we have used a one-way function, which restricts the outsider Adversary from stealing or breaching information about the secret. To deal with the situation of Case-1 and Case-2,Two variable one-way functions are used. Using a two-variable one-way function, every participant can verify the share received from the dealer and other participants. Our scheme also satisfies the security goals like correctness and secrecy. In Table I, we have compared the recent scheme for multi-secret sharing. From there, we conclude that our scheme can provide many security properties in the case of IoT authentication. Furthermore, in Figure 1, we can see that computational is significantly less than others and security features are more in numbers supported by proposed scheme.

8. Conclusions

In the present work, we categorized participants into different levels with varying thresholds, aligning with a hierarchical structure. Subsequently, we proposed a hierarchical multi-secret sharing scheme based on the YCH scheme. The YCH scheme is highly efficient, and the inclusion of a one-way function enhances its security, making it unconditionally secure. The reusability of shares eliminates the need for frequent refreshment of shares for future communication. In addition to being reusable, multi-secret, and hierarchical, our scheme includes a valuable feature: the verification of shares. Specific participants can verify the shares they receive from other participants or the dealer. This verification feature makes our proposed scheme particularly useful for robust security solutions. Comparisons with existing schemes demonstrate its superiority in preserving security. Our scheme not only improves operational efficiency but also provides a scalable solution adaptable to various access structures. Future work could explore further optimizations and applications in complex, multi-stage security environments.

Author Contributions: All authors made equal contributions.

Funding: Applicable.

Data Availability Statement: Data sharing is not applicable as no datasets were generated or analyzed during the current study.

Acknowledgments: We are very thankful to the "SageMath" open source community. This paper has been executed utilizing free open source arithmetic programming in SageMath [37]. The authors extend their appreciation to Princess Nourah Bint Abdulrahman University (PNU), Riyadh, Saudi Arabia for funding this research under Researchers Supporting Project Number (PNURSP2024R231).

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

 doi:10.20944/preprints202405.2061.v1

References

1. Asmuth C. and Bloom J., "A modular approach to key safeguarding," *IEEE transactions on information theory*, vol. 29, no. 2, pp. 208–210, 1983.
2. Ballico1 E., Boato G., Fontanari C., and Granelli F., "Hierarchical secret sharing in ad hoc networks through birkhoff interpolation," in *Advances in Computer, Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, TeNe 2005, EIAE 2005*, pp. 157–164, Springer, 2006.
3. Banerjee S., Gupta D. S., and Biswas G., "Hierarchy-based cheating detection and cheater identification in secret sharing schemes," in *2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, pp. 1–6, IEEE, 2018.
4. Basit A., Kumar N. C., Venkaiah V. C., Moiz S. A., Tentu A. N., and Naik W., "Multi-stage multi-secret sharing scheme for hierarchical access structure," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 557–563, IEEE, 2017.
5. Bisht K. and Deshmukh M., "A novel approach for multilevel multi-secret image sharing scheme," *The Journal of Supercomputing*, vol. 77, no. 10, pp. 12157–12191, 2021.
6. Blakley G. R., "Safeguarding cryptographic keys," in *Managing requirements knowledge, international workshop on*, pp. 313–313, IEEE Computer Society, 1979.
7. Blundo C., De Santis A., Stinson D. R., and Vaccaro U., "Graph decompositions and secret sharing schemes," *Journal of cryptology*, vol. 8, no. 1, pp. 39–64, 1995.
8. Brickell E. F., "Some ideal secret sharing schemes," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 468–475, Springer, 1989.
9. Bufalo M., Bufalo D., and Orlando G., "Some properties of the computation of the modular inverse with applications in cryptography," *Computation*, vol. 11, no. 4, p. 70, 2023.
10. Chanu O. B., Tentu A. N., and Venkaiah V. C., "Multi-stage multi-secret sharing schemes based on chinese remainder theorem," in *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015)*, pp. 1–6, 2015.
11. Chen Q., Tang C., and Lin Z., "Efficient explicit constructions of multipartite secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 601–631, 2021.
12. Chen H.-Y., Wu Z.-Y., Chen T.-L., Huang Y.-M., and Liu C.-H., "Security privacy and policy for cryptographic based electronic medical information system," *Sensors*, vol. 21, no. 3, p. 713, 2021.
13. Choc B., Goldwasser S., Micali S., and Awerbuch B., "Verifiable secret sharing and achieving simultaneity in the presence of faults.," in *Annual Symposium on Foundations of Computer Science (Proceedings)*, pp. 383–395, 1985.
14. Dolev D. and Yao A., "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.
15. Gutte V. S. and Parasar D., "Sailfish invasive weed optimization algorithm for multiple image sharing in cloud computing," *International Journal of Intelligent Systems*, vol. 37, no. 7, pp. 4190–4213, 2022.
16. Halpern J. and Teague V., "Rational secret sharing and multiparty computation," in *Proceedings of the thirtysixth annual ACM symposium on Theory of computing*, pp. 623–632, 2004.
17. Harn L. and Hsu C.-F., "(t, n) multi-secret sharing scheme based on bivariate polynomial," *Wireless Personal Communications*, vol. 95, pp. 1495–1504, 2017.
18. Harn L., Hsu C.-F., Xia Z., Zhou J., et al., "How to share secret efficiently over networks," *Security and Communication Networks*, vol. 2017, 2017.
19. Hazzazi M. M., Attuluri S., Bassfar Z., and Joshi K., "A novel cipher-based data encryption with galois field theory," *Sensors*, vol. 23, no. 6, p. 3287, 2023.
20. He J. and Dawson E., "Multistage secret sharing based on one-way function," *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1994.
21. He J. and Dawson E., "Multisecret-sharing scheme based on one-way function," *Electronics Letters*, vol. 31, no. 2, pp. 93–95, 1995.
22. Herranz J. and Sáez G., "New results on multipartite access structures," *IEE Proceedings-Information Security*, vol. 153, no. 4, pp. 153–162, 2006.
23. Herranz J., Ruiz A., and Sáez G., "New results and applications for multi-secret sharing schemes," *Designs, codes and cryptography*, vol. 73, pp. 841–864, 2014.
24. Hernández-Álvarez L., Bullón Pérez J. J., Batista F. K., and Queiruga-Dios A., "Security threats and cryptographic protocols for medical wearables," *Mathematics*, vol. 10, no. 6, p. 886, 2022.

 doi:10.20944/preprints202405.2061.v1

25. Hung-Yu C., Jinn-Ke J., and Yuh-Min T., "A practical (t, n) multi-secret sharing scheme," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 83, no. 12, pp. 2762–2765, 2000.
26. Jara-Vera V. and Sánchez-Ávila C., "Some notes on a formal algebraic structure of cryptology," *Mathematics*, vol. 9, no. 18, p. 2183, 2021.
27. Knuth D. E., *The art of computer programming*. Pearson Education, 2005.
28. Lin C., Harn L., and Yea D., "Ideal hierarchical (t, n) secret sharing schemes," in *Proceedings of the Fifth International Conference on Information Assurance and Security (IAS09), Xian, China*, Citeseer, 2009.
29. Liu Y., Zhang F., and Zhang J., "Attacks to some verifiable multi-secret sharing schemes and two improved schemes," *Information Sciences*, vol. 329, pp. 524–539, 2016.
30. Ma C. and Cheng R., "Key management based on hierarchical secret sharing in ad-hoc networks," in *Information Security and Cryptology: Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31-September 5, 2007, Revised Selected Papers 3*, pp. 182–191, Springer, 2008.
31. Mashhadi S., "Toward a formal proof for multi-secret sharing in the random oracle model," *Information Security Journal: A Global Perspective*, vol. 29, no. 5, pp. 244–249, 2020.
32. Masood F., Ahmad J., Shah S. A., Jamal S. S., and Hussain I., "A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.
33. Padró C. and Sáez G., "Secret sharing schemes with bipartite access structure," *IEEE Transactions on Information Theory*, vol. 46, no. 7, pp. 2596–2604, 2000.
34. Rauf A., Wang Z., Sajid H., and Ali Tahir M., "Secure route-obfuscation mechanism with information-theoretic security for internet of things," *Sensors*, vol. 20, no. 15, p. 4221, 2020.
35. Ren P., Li F., Wang, Y., Zhou, H., and Liu P., "Ipsadas: identity-privacy-aware secure and anonymous data aggregation scheme," *International Journal of Intelligent Systems*, vol. 37, no. 8, pp. 5290–5324, 2022.
36. Richter M., Bertram M., Seidensticker J., and Tschache A., "A mathematical perspective on post-quantum cryptography," *Mathematics*, vol. 10, no. 15, p. 2579, 2022.
37. SageMath, "Use SageMath Online — cocalc.com." https://cocalc.com/features/sage. [Accessed 30-04-2024].
38. *Security and So Many Things — asecuritysite.com*. https://asecuritysite.com/. [Accessed 30-04-2024].
39. Shamir A., "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
40. Simmons G. J., "How to (really) share a secret," in *Conference on the Theory and Application of Cryptography*, pp. 390–448, Springer, 1988.
41. Tentu A. N., Bhavani K., Basit A., and Venkaiah V. C., "Sequential (t, n) multi secret sharing scheme for level-ordered access structure," *International Journal of Information Technology*, vol. 13, pp. 2265–2275, 2021.
42. Tito-Corrioso O., Borges-Quintana M., Borges-Trenard M. A., Rojas O., and Sosa-Gómez G., "On the fitness functions involved in genetic algorithms and the cryptanalysis of block ciphers," *Entropy*, vol. 25, no. 2, p. 261, 2023.
43. Tompa M. and Woll H., "How to share a secret with cheaters," *journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.
44. Wang X., Zhang X., Zu C., Yang, Z., Bian G., Zhang, Y., Ruan, W., Wu B., Wu X., Yuan, L., et al., "An accurate cloud-based indoor localization system with low latency," *International Journal of Intelligent Systems*, vol. 37, no. 8, pp. 4794–4809, 2022.
45. Wu S., Hsu C., Xia Z., Zhang J., and Wu D., "Symmetric-bivariate-polynomial-based lightweight authenticated group key agreement for industrial internet of things," *Journal of Internet Technology*, vol. 21, no. 7, pp. 1969–1979, 2020.
46. Yang C.-C., Chang T.-Y., and Hwang M.-S., "A (t, n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.
47. Yuan J., Yang J., Wang C., Jia X., Fu F.-W., and Xu G., "A new efficient hierarchical multi-secret sharing scheme based on linear homogeneous recurrence relations," *Information Sciences*, vol. 592, pp. 36–49, 2022.
48. Zhang E., Li M., Yiu S.-M., Du J., Zhu J.-Z., and Jin G.-G., "Fair hierarchical secret sharing scheme based on smart contract," *Information Sciences*, vol. 546, pp. 166–176, 2021.
49. Zhang Y., Liu Z., and Huang G., "Sure interpolation and its application to hierarchical threshold secret sharing scheme," in *2008 International Symposium on Computer Science and Computational Technology*, vol. 1, pp. 447–450, IEEE, 2008.