

Extendable Weighted Evolving Threshold Secret Sharing Schemes over Polynomial Quotient Rings

Qi Cheng¹, Guang Hu^{2,3}, Hongru Cao⁴, Sian-Jheng Lin⁴(✉),
and Yunghsiung S. Han⁵(✉)

¹ School of Artificial Intelligence, Anhui Agricultural University, Hefei 230036, China, chengqi@ahau.edu.cn

² Mathematics School, Shandong University, Jinan 250100, China, 202490000031@sdu.edu.cn

³ Faculty of Mathematics, Dresden University of Technology, 01069 Dresden, Germany,

⁴ School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230027, China, chrkeith@mail.ustc.edu.cn, sjlin@ustc.edu.cn

⁵ School of Computing and Information Technology, Great Bay University, Dongguan 523000, China, yunghsiung@gmail.com

Abstract. In conventional (k, n) secret sharing schemes, a dealer distributes shares of a secret among n participants such that any subset of at least k participants can reconstruct the secret. While such schemes often fail to accommodate practical scenarios in which participants have different management permissions over the secret. To address this problem, weighted (t, n) secret sharing was introduced. In this case, each participant is assigned a specific weight, and the dealer distributes a share to each participant according to their weight, so that any subset of participants whose sum of weights is at least t can recover the secret. However, in weighted (t, n) secret sharing schemes, the number of participants n is known in advance. When n is uncertain and even grows over time, traditional weighted (t, n) secret sharing schemes remain inadequate in such dynamic environments. To solve the problem, we propose the concept of a weighted evolving t -threshold secret sharing. Based on the prefix codes, we first propose a construction of a weighted evolving 3-threshold scheme over the polynomial quotient ring for an ℓ -bit secret. And then we extend the framework to a general weighted evolving t -threshold scheme for any $t \geq 3$. Moreover, we prove the correctness and security of the proposed scheme by leveraging the properties of the polynomial quotient ring and prefix codes. Finally, we analyze the corresponding share size. The result shows that for the m -th participant with the weight w_m satisfying $1 \leq w_m \leq t - 1$, the size of the corresponding share is $w_m(t - 1 - \frac{w_m - 1}{2})(\ell_m - 1) + w_m \ell$ bits, where ℓ_m denotes the length of a binary prefix code of encoding integer m . In contrast, a baseline scheme that allocates w_m independent full evolving shares to this participant would require $w_m(t - 1)(\ell_m - 1) + w_m \ell$ bits. Our proposed scheme saves $\frac{(w_m - 1)w_m}{2}(\ell_m - 1)$ bits, thereby achieving a smaller share size.

Keywords: Weighted · Evolving secret sharing · Prefix codes · Hasse derivative · Polynomial quotient rings · Correctness · Security · Share size.

1 Introduction

A secret sharing scheme is a protocol that divides a secret into many shares, which are distributed to corresponding participants so that only a certain number of shares can recover the secret. Therefore, when using secret sharing schemes to transmit secret information, the security of the information can be ensured by resisting multi-party intrusions. The conventional (k, n) -threshold secret sharing scheme divides the secret to n participants such that any k out of n participants can reconstruct the secret, and any $k - 1$ participants cannot obtain any information about the secret. In 1979, Shamir [1] and Blakley [2] independently proposed the (k, n) secret sharing scheme.

Conventional secret sharing schemes require the dealer to know the maximum number of participants n , in advance. When allowing a new participant to join, the maximum number of n cannot be determined. Hence, most conventional schemes do not apply to this scenario. To solve this problem, Komargodski et al. [3] first proposed the evolving k -threshold secret sharing scheme, which allows the number of participants to be uncertain and even to grow over time, making it suitable for dynamic systems. In an evolving k -threshold scheme, the secret can be reconstructed by any k participants out of infinitely many participants, while any $k - 1$ or fewer participants cannot obtain any information about the secret. Although the work of Komargodski et al. opened up a new direction, their construction is not easy to implement. To achieve a simpler design, Cheng et al. [4] proposed a brand new construction of evolving k -threshold scheme over the polynomial ring. The scheme is more direct and concise, and is also the first evolving scheme that generalizes Shamir’s scheme to a polynomial ring. Given that Shamir’s scheme is the standard in conventional secret sharing, Cheng’s scheme has become the benchmark for evolving schemes. Moreover, many works [5–9] related to evolving secret sharing schemes were also proposed.

In practical applications, participants often possess different levels of access to sensitive data. A canonical example is banking systems, where senior managers may require higher access privileges to customer information compared to junior employees. Conventional secret sharing schemes, which assign uniform weights to all participants, often fail to meet practical requirements. To address this limitation, Shamir [1] first proposed a weighted (t, n) secret sharing scheme, which allows the dealer to distribute appropriate shares to each participant according to its weight value, so that a group of participants can recover the secret only if their weights sum up to at least t . This weighted secret sharing model more matches real-world security requirements. For instance, Zhang et al. [10] constructed a weighted threshold Pointcheval–Sanders signature scheme using CRT-based weighted ramp secret sharing, demonstrating a practical application of weighted secret sharing in threshold signatures.

However, existing research on weighted secret sharing schemes mainly focuses on static, conventional scenarios and does not support the dynamic joining of participants. In practical applications, systems must allow different weights to be assigned to participants and also allow participants to join dynamically. To solve the problem, Francati et al. [11] recently formalized weighted evolving threshold access structures and provided two constructions for weighted evolving threshold secret sharing under different assumptions. Their fixed-weight scheme achieves adaptive security in the plain model assuming OWFs and iO, while the dynamic-weight scheme achieves static security under OWFs, iO, and SSB hash functions. In this paper, we revisit weighted evolving threshold secret sharing and propose a different construction achieving perfect security in the information-theoretic sense, without relying on any cryptographic assumptions. Specifically, for weighted evolving threshold schemes, when assigning weights to participants, the weight values must be positive integers and must be less than the threshold. Consequently, when considering the minimal threshold value 2, we observe that a weighted evolving 2-threshold scheme is equivalent to a conventional evolving 2-threshold scheme. Therefore, our construction begins with the case where the threshold is set to 3. Based on this, we propose a construction of the weighted evolving 3-threshold secret sharing scheme, and then extend it to the general weighted evolving t -threshold secret sharing scheme, where $t > 3$.

1.1 Our Contributions

The main contributions are summarized as follows.

- We introduce the novel concept of weighted evolving secret sharing, linking the concepts of “evolving” and “weight” in secret sharing. This scheme is designed for dynamic environments in which participants can continuously join the system and are assigned different management privileges for the shared data.
- Based on integer prefix codes, we propose a general construction for the weighted t -threshold evolving secret sharing scheme over polynomial quotient rings for any t . Our approach offers an intuitive and concise design. Moreover, the scheme proposed by Cheng et al. [4] at ASIACRYPT 2025 can be regarded as a special case of our scheme when all participants have equal weights of 1. Thus, our scheme can serve as a natural extension of Cheng et al.’s work. Given that Cheng et al.’s scheme is the standard in evolving secret sharing, we believe that our proposed scheme has the potential to become the benchmark for weighted evolving schemes.
- The proposed weighted evolving t -threshold scheme is proved to have correctness and perfect security. In fact, providing the correctness and security proofs for our scheme is a difficult challenge. We give an ingenious and rigorous mathematical proof that leverages the properties of Hasse derivative, polynomial quotient rings and prefix codes. This innovative approach greatly improves the clarity and understandability of the proof process.

- We analyze the share size of our scheme in detail. Given an ℓ -bit secret, for the m -th participant with the weight w_m satisfying $1 \leq w_m \leq t-1$, the size of the corresponding share is $w_m(t-1-\frac{w_m-1}{2})(\ell_m-1) + w_m\ell$ bits, where ℓ_m denotes the length of a binary prefix code of encoding integer m . For comparison, a baseline scheme that allocates w_m independent full evolving shares to this participant would require $w_m(t-1)(\ell_m-1) + w_m\ell$ bits. The proposed scheme saves $\frac{(w_m-1)w_m}{2}(\ell_m-1)$ bits. Crucially, this reduction is significant, especially for participants with a larger weight.

1.2 Technical Overview

We now provide a detailed overview of the main techniques employed to construct our weighted evolving t -threshold scheme. Our approach combines the structure of integer prefix codes with the algebraic properties of Hasse derivative and polynomial quotient rings. Below, we describe the core technical components.

Construction of the Scheme. Our scheme generalizes the standard evolving threshold model by assigning each participant a share composed of multiple sub-shares, the number of which corresponds to its weight. The key technical steps are as follows.

Integer prefix codes for dynamic index. In an evolving scenario, we map each new participant P_i 's index i to a codeword c_i by using binary integer prefix codes, which ensures that even as participants join continuously, each one can always be assigned a unique codeword. Let ℓ_i and y_i denote the codeword length and the corresponding polynomial form of c_i , respectively. The property of prefix codes guarantees that for any two different participants P_i and P_j with $i < j$, $y_i - y_j \neq 0$ always holds in the polynomial quotient ring $\mathbb{F}_2[x]/x^{\ell_i}$, which is crucial for the proof of correctness and security.

Polynomial quotient ring framework with Hasse derivative. Shamir's scheme is based on Lagrange interpolation over a finite field, where the number of participants is bounded by the field size. To support an arbitrary number of participants, we work over the polynomial ring $\mathbb{F}_2[x]$, and choose interpolation nodes via prefix codes to guarantee uniqueness. Specifically, for an ℓ -bit secret s , we construct a polynomial $f(y) = \sum_{m=0}^{t-2} r_m y^m + s y^{t-1}$ over $\mathbb{F}_2[x]$, where the coefficients r_m are randomly chosen from $\mathbb{F}_2[x]$. To achieve weighted sharing, we employ Hermite interpolation, which reconstructs the secret from function values and derivatives at the nodes. However, over $\mathbb{F}_2$, which has characteristic two, ordinary derivatives make even-degree terms vanish. We therefore use Hasse derivatives instead. For a participant P_i with weight w_i , the corresponding share $Z_i^{(s)}$ is a vector of length w_i . The j -th component $Z_{i,j}^{(s)}$ of this vector is computed as the j -th order Hasse derivative of $f(y)$ evaluated at the element y_i derived from a prefix code encoding the integer i , and reduced modulo $x^{(t-j-1)(\ell_i-1)+\ell}$, i.e., $Z_{i,j}^{(s)} = \sum_{m=0}^{t-2} \binom{m}{j} r_m y_i^{m-j} + \binom{t-1}{j} s y_i^{t-1-j} \pmod{x^{(t-j-1)(\ell_i-1)+\ell}}$ for $0 \leq j \leq w_i - 1$. Truncated polynomial rings are used so that each share component retains only the information necessary for Hermite interpolation, ensuring both secret reconstruction and perfect security. Moreover,

using different truncated rings for each share component further reduces share size.

Correctness and Security Proofs. The proof of correctness and security relies on the property of prefix codes, the algebraic property of Hasse derivative and the modular arithmetic in polynomial rings.

Correctness. Proving correctness is the most difficult part of our work from a technical view, which takes much effort. When a set of participants with total weight $\geq t$, their shares form a system of linear equations $\mathbf{V}_y \cdot \mathbf{r} = \mathbf{Z}$ over the corresponding polynomial quotient ring, where $\mathbf{r} = (r_0, r_1, \dots, r_{t-2}, s)^T$ are t unknown variables, $\mathbf{Z}$ contains t known shares, and $\mathbf{V}_y$ is a $t \times t$ confluent Vandermonde matrix and the determinant is not zero based on the property of prefix codes. To reconstruct the secret s , we need to eliminate all unknowns r_m . We first construct a specific column vector $\mathbf{c}$ and left-multiply it by the entire system of equations, then get a new congruence equation $s \cdot \det(\mathbf{V}_y) \equiv \mathbf{c}^T \mathbf{Z} \pmod{x^\xi}$. Next, we prove that $s \cdot \det(\mathbf{V}_y) \equiv \mathbf{c}^T \mathbf{Z} \pmod{x^\xi}$ preserves enough precision to recover s . Specifically, we prove that the maximal extractable power of $\det(\mathbf{V}_y)$ is strictly no more than $\xi - \ell$. This part is very difficult, and we spent a lot of effort to provide a rigorous and elegant proof. A detailed description can be found in Appendix. Finally, we use the known conclusion to recover the unique solution about s in $\mathbb{F}_2[x]/x^\ell$.

Secrecy. When a set of participants with total weight is equal to $t - 1$, we can collect n participants $\{P_{i_u}\}_{u=1}^n$'s $t - 1$ shares. To demonstrate security according to the definition, we choose two distinct secrets s_0 and s_1 , and denote $Z_{i_u}^{(s_0)} = [Z_{i_u,0}^{(s_0)}, \dots, Z_{i_u,w_{i_u}-1}^{(s_0)}]$ and $Z_{i_u}^{(s_1)} = [Z_{i_u,0}^{(s_1)}, \dots, Z_{i_u,w_{i_u}-1}^{(s_1)}]$ the share of the participant P_{i_u} generated under each secret, respectively. Given any fixed $t - 1$ shares $\{\{z_{i_u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$ with each $z_{i_u,j} \in \mathbb{F}_2[x]/x^{(t-j-1)(\ell_{i_u}-1)+\ell}$, we need to prove $P(\{\{Z_{i_u,j}^{(s_0)} = z_{i_u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n) = P(\{\{Z_{i_u,j}^{(s_1)} = z_{i_u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n)$. For given secrets s_0, s_1 , n participants $\{P_{i_u}\}_{u=1}^n$ and $t - 1$ shares $\{\{z_{i_u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$, we construct two systems of $t - 1$ equations, one with $r_{0,0}, r_{0,1}, \dots, r_{0,t-2}$ as the unknown, and the other with $r_{1,0}, r_{1,1}, \dots, r_{1,t-2}$ as the unknown. Then, we prove the equality $P(\{\{Z_{i_u,j}^{(s_0)} = z_{i_u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n) = P(\{\{Z_{i_u,j}^{(s_1)} = z_{i_u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n)$ by demonstrating that the two equation systems possess an equal number of solutions. By leveraging the algebraic structure of polynomial quotient rings and the properties of prefix codes, along with techniques for solving equations, we provide an interesting method to demonstrate that these two equation systems indeed contain the same number of solutions. Therefore, the proposed scheme has perfect security.

1.3 Related Works

The (k, n) secret sharing scheme, first introduced independently by Shamir [1] and Blakley [2] in 1979, enables a dealer to distribute a secret among n participants such that any subset of at least k participants can reconstruct the secret, while any subset of fewer than k participants reveals no information. Shamir's scheme [1] leverages Lagrange interpolation over finite fields, whereas

Blakley’s approach [2] utilizes geometric hyperplane intersections in multidimensional spaces. Subsequent work has explored alternative algebraic structures to enhance flexibility or efficiency. Mignotte [12], Asmuth et al. [13], and Ning et al. [14] respectively proposed new constructions of (k, n) threshold secret sharing schemes based on the Chinese Remainder Theorem for rings. Later, Cramer et al. [15] and Cao et al. [16] generalized schemes to abelian groups and general rings, while Ligeti et al. [17] and Gyarmati et al. [18] employed finite geometry to construct new secret sharing schemes. These works have laid the foundation for practical applications [19–23] of secret sharing.

However, conventional secret sharing schemes require the dealer to determine the total number of participants n in advance, which cannot adapt to scenarios where new participants dynamically join. To meet practical needs, Komargodski et al. [3] introduced the evolving k -threshold secret sharing scheme, which allows the total number of participants to dynamically increase. Specifically, Komargodski et al. [3] first gave the construction of evolving 2-threshold secret sharing schemes based on binary prefix codes, which establishes a connection between prefix codes and 2-threshold schemes. The results indicate that given a set of binary integer prefix codes [24], there necessarily exists a corresponding construction for the evolving 2-threshold scheme, and vice versa. This breakthrough discovery has stimulated extensive research interest. Subsequently, many works [25–27] have been proposed to research evolving 2-threshold schemes based on integer prefix codes.

Komargodski et al. [3] also proposed the construction of an evolving k -threshold secret sharing scheme and analyzed the corresponding share size, where $k > 2$. The scheme is designed based on the idea of distributing shares on a generational basis and uses an evolving scheme once and Shamir’s scheme multiple times. However, the construction will become increasingly complex and even difficult to construct as k increases, and the corresponding share size is not optimal. To obtain a simpler construction method for evolving k -threshold scheme, Xing and Yuan [28] proposed a novel scheme based on algebraic geometry codes. Cheng et al. [4] further introduced a new construction method based on polynomial rings. Their construction works over the polynomial ring $\mathbb{F}_2[x]$, where the secret s serves as the leading coefficient of a polynomial $f(y) = \sum_{j=0}^{k-2} r_j y^j + s y^{k-1}$. Each participant P_i is assigned a point y_i derived from a prefix code of the integer i , and the share is computed as the evaluation $f(y_i)$ modulo $x^{(k-1)(\ell_i-1)+\ell}$, where ℓ_i denotes the length of a binary prefix code for encoding the integer i . Although both methods achieve simplification in construction, an analysis of share size shows that the dominant term of the m -th share size remains $(k-1) \lg m$, which is consistent with the result in [3] and is not optimal. To achieve a smaller share size, D’Arco et al. [29] proposed a new evolving 3-threshold scheme based on the Chinese Remainder Theorem, reducing the dominant term of share size from $2 \lg t$ to $\frac{4}{3} \lg t$.

Weighted secret sharing schemes aim to assign different weights to participants. Shamir [1] first proposed a weighted (t, n) secret sharing scheme. Harn and Miao [30] proposed a weighted scheme based on the Chinese Remainder The-

orem, establishing a fundamental framework for subsequent research. Dragan and Tiplea [31] later introduced a distributed weighted threshold access structure and proposed an implementation that achieves both asymptotic perfectness and perfect zero-knowledge, thereby significantly enhancing security and privacy preservation. Building upon these works, Benhamouda et al. [32] proposed a (α, β) ramp weighted secret sharing scheme, while Garg et al. [33] formalized the concept of weighted cryptosystems and developed an efficient weighted ramp secret sharing scheme, with successful applications in secure multi-party computation, threshold encryption, and threshold signatures. Most recently, Farrás and Guiot [34] employed Chow parameter approximation techniques to design a highly efficient secret sharing scheme with reduced share sizes, substantially optimizing both storage requirements and communication overhead. Collectively, these research efforts have systematically advanced the development of weighted secret sharing. However, for weighted (t, n) secret sharing schemes, the number of participants n is known in advance. When n is uncertain or even ever-growing, traditional weighted (t, n) schemes are unable to be applied in dynamic scenarios.

1.4 Organization

The rest of the paper is organized as follows. In Section 2, we introduce the conventional weighted secret sharing scheme and the evolving secret sharing scheme. In Section 3, we first propose the concept of weighted evolving threshold secret sharing, then present a construction of the weighted evolving 3-threshold scheme and prove its security and correctness. In Section 4, we extend the scheme to the case of t -threshold, where $t \geq 3$. Finally, Section 5 concludes the work and discusses the unresolved problems.

2 Models and Notations

We first introduce the notation used in this paper. Let $\mathbb{N}^+$ denote the set of positive integers. Let $|A|$ denote the cardinality of the set A . Denote $\{A\}^n$ as the direct sum of n sets A for any $n \in \mathbb{N}^+$. For any two sets A and B , where B is a proper subset of A , the set difference $A \setminus B$ denotes the collection of elements remaining in A after the removal of all elements belonging to B . For any $n \in \mathbb{N}^+$, $p \in \mathbb{N}^+$ being a prime, let $\mathbb{F}_p$ denote the finite field with p elements. Let $\mathbb{F}_p[x] = \{\sum_{j=0}^N a_j x^j | a_j \in \mathbb{F}_p\}$ be the polynomial ring, where N is a finite positive integer. Given any $f(x), g(x) \in \mathbb{F}_p[x]$, if $g(x)$ divides $f(x)$, it can be expressed as $g(x) \mid f(x)$, the result of $g(x)$ dividing $f(x)$ is denoted as *quotient*, which is written as $\frac{f(x)}{g(x)}$. For any $i, a \in \mathbb{N}^+$, $f(x) \in \mathbb{F}_p[x]$, if $x^i \mid f(x)$ with any $i \leq a$ and $x^{a+1} \nmid f(x)$, then a is denoted as *the maximal extractable power* of $f(x)$, which is written as $p_x(f(x)) = a$. For any $d \in \mathbb{N}^+$, let $\mathbb{F}_p[x]/x^d$ be a polynomial quotient ring, which is composed of polynomials $f(x) \in \mathbb{F}_p[x]$ with the degree less than d . For any $f(x) \in \mathbb{F}_p[x]/x^d$, if there exists a polynomial $g(x) \in \mathbb{F}_p[x]/x^d$ such that $f(x)g(x) = 1 \in \mathbb{F}_p[x]/x^d$, then $f(x)$ is called to be invertible, which is represented as $f^{-1}(x)$. Let $\mathbb{F}_p[[x]] = \{\sum_{j=0}^{\infty} a_j x^j | a_j \in \mathbb{F}_p\}$ be the ring of

Laurent series. Let $\mathbb{F}_p(x)$ denote the field of rational functions over $\mathbb{F}_p$. For any $f(x) \in \mathbb{F}_p(x)$, we can uniquely write $f(x) = \frac{P(x)}{Q(x)}$ where $P(x), Q(x) \in \mathbb{F}_p[x]$ are coprime, and $Q(x) \neq 0$. The difference between the maximal extractable power of $P(x)$ and $Q(x)$ is defined as the maximal extractable power of $f(x)$, i.e., $p_x(f(x)) = p_x(P(x)) - p_x(Q(x))$.

2.1 Weighted Secret Sharing Scheme

Let $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ represent the set of n participants, w_i denote the corresponding weight of P_i with $w_i \in \mathbb{N}^+$. $2^{\mathcal{P}_n}$ represents the power set of $\mathcal{P}_n$. The collection $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$ is monotone if for arbitrary $A \in \mathcal{A}$ and $A \subseteq C$, it holds that $C \in \mathcal{A}$. The access structure is defined as follows.

Definition 1. An access structure $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$ is a monotone collection of non-empty sets. The set in $\mathcal{A}$ is called qualified, the set not in $\mathcal{A}$ is called unqualified.

Definition 2. For $t, n \in \mathbb{N}^+$ with $t \leq n$, P_i 's weight w_i satisfies $1 \leq w_i \leq t-1$. The weighted (t, n) threshold access structure $\mathcal{A}$ satisfies that for each element A of $\mathcal{A}$, the weight sum of all participants in A is no less than t .

Actually, a weighted (t, n) -threshold secret sharing scheme requires a dealer, a set of n participants, a weighted (t, n) access structure $\mathcal{A}$ and a secret $s \in S$, where S is the domain of the secret. The dealer distributes the share to every participant according to their corresponding weights, such that the shares of any element in $\mathcal{A}$ can correctly recover the secret, while the shares of any element not in $\mathcal{A}$ cannot gain any information about the secret. We denote by $Z_i^{(s)}$ the share respective to secrete s of the i -th participant. The formal definition is given as follows.

Definition 3. A weighted (t, n) -threshold secret sharing scheme consists of a pair of algorithms $(\mathcal{E}, \mathcal{R})$, where $\mathcal{E}$ is used to encode the secret s into shares, and $\mathcal{R}$ is used to reconstruct the secret from a subset of shares $H \in 2^{\mathcal{P}_n}$. The following requirements shall be satisfied.

- **Correctness.** For any qualified set $A \in \mathcal{A}$, the algorithm $\mathcal{R}$ can correctly recover s from the shares of the participants in A , that is

$$P[\mathcal{R}(\{Z_i^{(s)}\}_{P_i \in A}, A) = s] = 1.$$

- **Secrecy.** For any unqualified set $C \notin \mathcal{A}$, there is no information about s leaking to the participants in C , that is, for any two different secrets $s_0, s_1 \in S$ and every possible vector of shares $\{z_i\}_{P_i \in C}$, $P(\{Z_i^{(s_0)} = z_i\}_{P_i \in C}) = P(\{Z_i^{(s_1)} = z_i\}_{P_i \in C})$.

2.2 Evolving Secret Sharing Scheme

When the maximum number of n cannot be determined in advance and can even be infinite, conventional secret sharing schemes cannot be applied directly. In this case, evolving secret sharing schemes are developed. We denote $\mathcal{P} = \{P_1, P_2, \dots, P_n, \dots\}$ as the set of participants, where $\mathcal{P}$ is possibly infinite. Then we give some definitions of the evolving secret sharing scheme.

Definition 4. A collection of sets $\mathcal{A} \subseteq 2^{\mathcal{P}}$ is an evolving access structure if for every $m \in \mathbb{N}^+$, $\mathcal{A}_m := \mathcal{A} \cap 2^{\{P_1, P_2, \dots, P_m\}}$ is an access structure as defined in Definition 1.

Definition 5. For $k \in \mathbb{N}^+$, the evolving k -threshold access structure $\mathcal{A}$ refers to the set consisting only of all elements in $2^{\mathcal{P}}$ of size at least k , i.e.,

$$\mathcal{A} = \{A \in 2^{\mathcal{P}} \mid |A| \geq k\}.$$

Similarly, constructing an evolving k -threshold secret sharing scheme requires a dealer, a secret $s \in S$, a set of participants, and an evolving k -threshold access structure $\mathcal{A}$. The dealer distributes the shares to all participants such that the shares of any set in $\mathcal{A}$ can correctly reconstruct the secret, whereas the shares of any set not in $\mathcal{A}$ reveal no information about the secret. The formal definition is given as follows.

Definition 6 ([3]). Let $\mathcal{A}$ be an evolving access structure and S be a domain of secrets, where $|S| \geq 2$. A secret sharing scheme for $\mathcal{A}$ and S consists of a pair of algorithms $(\mathcal{E}, \mathcal{R})$, where the sharing procedure $\mathcal{E}$ and the reconstruction procedure $\mathcal{R}$ satisfy the following requirements.

- **Share procedure.** $\mathcal{E}(s, \{Z_1^{(s)}, Z_2^{(s)}, \dots, Z_{j-1}^{(s)}\})$ gets as input a secret $s \in S$ and the secret shares of participants $P_1, P_2, \dots, P_{j-1}$. It outputs a share for the j -th party. For $j \in \mathbb{N}^+$ and secret shares $Z_1^{(s)}, Z_2^{(s)}, \dots, Z_{j-1}^{(s)}$ generated for participants $\{P_1, P_2, \dots, P_{j-1}\}$, respectively, we let

$$Z_j^{(s)} \leftarrow \mathcal{E}(s, \{Z_1^{(s)}, Z_2^{(s)}, \dots, Z_{j-1}^{(s)}\})$$

be the secret share of participant P_j .

We abuse notation and sometimes denote by $Z_j^{(s)}$ the random variable that corresponds to the secret share of participant P_j generated as above.

- **Correctness.** For every $s \in S$ and every $m \in \mathbb{N}^+$, every qualified set in $\mathcal{A}_m$ can reconstruct the secret. That is, for $s \in S$, $m \in \mathbb{N}^+$ and $A \in \mathcal{A}_m$, it holds that

$$P[\mathcal{R}(\{Z_i^{(s)}\}_{P_i \in A}, A) = s] = 1,$$

where the probability is over the randomness of the sharing and reconstruction procedures.

- **Secrecy.** For every $m \in \mathbb{N}^+$, every unqualified set $C \notin \mathcal{A}_m$, and every two secrets $s_0, s_1 \in S$, the distribution of the secret shares of participants in C generated with secret s_0 and the distribution of the shares of participants in C generated with secret s_1 are identical. Namely, the distributions $(\{Z_i^{(s_0)} = z_i\}_{P_i \in C})$ and $(\{Z_i^{(s_1)} = z_i\}_{P_i \in C})$ are identical.

3 Construction of Weighted Evolving 3-Threshold Scheme over Polynomial Quotient Rings

When the total number of participants is unknown, and participants have different weights, conventional secret sharing schemes are inapplicable. To address this problem, we propose a novel concept of weighted evolving threshold secret sharing.

Definition 7. Let $t \in \mathbb{N}^+$ and $\mathcal{P} = \{P_1, P_2, \dots, P_n, \dots\}$ be the set of participants. For each $P_i \in \mathcal{P}$, let w_i denote its weight satisfying $1 \leq w_i \leq t - 1$. The weighted evolving t -threshold access structure $\mathcal{A}$ is a collection of subsets such that for any $A \in \mathcal{A}$, the sum of the weights of participants in A is no less than t . The set in $\mathcal{A}$ is called qualified, and the set not in $\mathcal{A}$ is called unqualified.

For a given secret $s \in S$, a set of participants $\mathcal{P}$ and a weighted evolving t -threshold access structure $\mathcal{A}$, in the weighted evolving t -threshold secret sharing scheme, the secret can be recovered from any subset of participants if the sum of their weights is no less than t , and any subset of participants when the sum of weights is less than t , cannot deduce any information about the secret. The formal definition is given as follows.

Definition 8. Let $\mathcal{A}$ be a weighted evolving access structure and S be a domain of secrets, where $|S| \geq 2$. A weighted evolving secret sharing scheme for $\mathcal{A}$ and S consists of a pair of algorithms $(\mathcal{E}, \mathcal{R})$, where the sharing procedure $\mathcal{E}$ and the reconstruction procedure $\mathcal{R}$ satisfy the following requirements.

- **Share procedure.** $\mathcal{E}(s, \{Z_1^{(s)}, Z_2^{(s)}, \dots, Z_{j-1}^{(s)}\})$ gets as input a secret $s \in S$ and the secret shares of participants $P_1, P_2, \dots, P_{j-1}$. It outputs a share for the j -th party with the corresponding weight w_j . For $j \in \mathbb{N}^+$ and secret shares $Z_1^{(s)}, Z_2^{(s)}, \dots, Z_{j-1}^{(s)}$ generated for participants $\{P_1, P_2, \dots, P_{j-1}\}$, respectively, we let

$$Z_j^{(s)} \leftarrow \mathcal{E}(s, w_j, \{Z_1^{(s)}, Z_2^{(s)}, \dots, Z_{j-1}^{(s)}\}).$$

be the secret share of participant P_j .

We abuse notation and sometimes denote by $Z_j^{(s)}$ the random variable that corresponds to the secret share of participant P_j generated as above.

- **Correctness.** For every $s \in S$, every set in $\mathcal{A}$ can reconstruct the secret. That is, for $s \in S$ and $A \in \mathcal{A}$, it holds that

$$P[\mathcal{R}(\{Z_i^{(s)}\}_{P_i \in A}, A) = s] = 1,$$

where the probability is over the randomness of the sharing and reconstruction procedures.

- **Secrecy.** For every unqualified set $C \notin \mathcal{A}$, and every two secrets $s_0, s_1 \in S$, the distribution of the secret shares of participants in C generated with secret s_0 and the distribution of the shares of participants in C generated with secret s_1 are identical. Namely, the distributions $(\{Z_i^{(s_0)} = z_i\}_{P_i \in C})$ and $(\{Z_i^{(s_1)} = z_i\}_{P_i \in C})$ are identical.

In a weighted evolving t -threshold secret sharing scheme for any $t \in \mathbb{N}^+$, each participant P_i holds a weight w_i satisfying $1 \leq w_i \leq t - 1$. When constructing such schemes, we observe that for the minimal threshold $t = 2$, the weighted evolving 2-threshold scheme coincides with the conventional evolving 2-threshold scheme. Consequently, our analysis focuses on the $t = 3$ case as the first non-trivial scenario.

To construct a weighted evolving 3-threshold secret sharing scheme, a natural idea is to distribute multiple shares to participants according to their weights, by using the known evolving 3-threshold schemes [3, 4]. Specifically, this entails allocating 1 share to the participants with weight 1 and 2 shares to the participants with weight 2. However, the direct extension faces two critical challenges. First, since each participant P_i 's share in known schemes [3, 4] is generated based on a unique index i . If we simply assign multiple indices to participants with higher weights, it can easily cause duplicates with indices used by others. Second, these additionally assigned indices must be communicated to the corresponding participants, which creates additional storage overhead. To solve these problems, we propose a novel construction for a weighted evolving 3-threshold secret sharing scheme.

3.1 Proposed Scheme

Before describing the proposed scheme, we first introduce the definition of prefix codes.

Definition 9. *A prefix (or more precisely, prefix-free) code is a code in which no codeword is a prefix of any other codeword. A prefix code for the integers is an infinite prefix code $C = \{c_1, c_2, \dots\}$, where c_i is the codeword of encoding integer i .*

We now begin to describe our scheme in detail. For a given ℓ -bit secret s , its binary sequence is denoted as $s^0 s^1 \dots s^{\ell-1}$, we first construct a polynomial $f(y)$ defined as

$$f(y) = r_0 + r_1 y + s y^2, \quad (1)$$

where r_0, r_1 are randomly chosen in $\mathbb{F}_2[[x]]$. In (1), the secret s is used as the polynomial form $\sum_{j=0}^{\ell-1} s^j x^j \in \mathbb{F}_2[x]$, which would be the default form throughout this paper.

Let $\mathcal{P} = \{P_1, P_2, \dots, P_n, \dots\}$ denote the set of participants, and w_i represent the corresponding weight of participant P_i with $0 < w_i < 3$. Given a set of prefix codes for integers, the codeword of the positive integer i is denoted as $c_i = c_{i,0} c_{i,1} \dots c_{i,\ell_i-1}$, where ℓ_i represents the codeword length. The polynomial form of c_i is defined as $y_i = \sum_{j=0}^{\ell_i-1} c_{i,j} x^j \in \mathbb{F}_2[x]$. For the i -th participant P_i , the algorithm $\mathcal{E}$ generates and distributes the share $Z_i^{(s)}$ depending on weight w_i .

When $w_i = 1$, the corresponding share is

$$Z_i^{(s)} = r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}. \quad (2)$$

Although r_0 and r_1 are theoretically selected from the ring $\mathbb{F}_2[[x]]$, which implies potentially infinite degree terms in (2), practical implementation limits the polynomials to finite degrees. In fact, since the actual computation occurs in the quotient ring $\mathbb{F}_2[x]/x^{2(\ell_i-1)+\ell}$ in (2), it suffices for the dealer to generate only the polynomial segments of r_0 and r_1 with degrees strictly less than $2(\ell_i-1)+\ell$.

When $w_i = 2$, the corresponding share of the i -th participant consists of two parts, i.e.,

$$Z_i^{(s)} = [Z_{i,0}^{(s)}, Z_{i,1}^{(s)}], \quad (3)$$

where $Z_{i,j}^{(s)}$ with $j \in \{0, 1\}$ denotes the j -th order Hasse derivative of $f(y)$ with respect to y , evaluated at $y = y_i$, and reduced modulo $x^{(2-j)(\ell_i-1)+\ell}$. i.e.,

$$Z_i^{(s)} = [r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, \quad r_1 \pmod{x^{\ell_i+\ell-1}}]. \quad (4)$$

Notably, when constructing the corresponding share $Z_i^{(s)}$, though r_0, r_1 are defined randomly chosen in $\mathbb{F}_2[[x]]$ for (4), the calculations for $Z_{i,0}^{(s)}$ and $Z_{i,1}^{(s)}$ are performed in quotient rings with different moduli in (4). Since the ring for calculating $Z_{i,1}^{(s)}$ is contained within that for calculating $Z_{i,0}^{(s)}$, we can simply select r_0 and r_1 from the larger ring $\mathbb{F}_2[x]/x^{2(\ell_i-1)+\ell}$ for calculating $Z_{i,1}^{(s)}$ and $Z_{i,0}^{(s)}$. Consequently, the dealer only needs to choose the parts of r_0 and r_1 with the degree less than $2(\ell_i-1)+\ell$.

Depending on the participant's weight value, equations (2) and (3) provide two distinct methods for generating shares. Regardless of the approach used to construct the i -th share, selecting appropriate polynomials r_0 and r_1 remains essential. We now detail the procedure for updating r_0 and r_1 for the subsequent participant.

Suppose that the dealer has already distributed shares to the first i participants. At this stage, the dealer retains the corresponding r_0 and r_1 used to construct each j -th share, where $1 \leq j \leq i$. Note that for the i -th share, r_0 and r_1 belong to $\mathbb{F}_2[x]/x^{2(\ell_i-1)+\ell}$. To generate the corresponding r_0 and r_1 for constructing the $(i+1)$ -th share, which belong to $\mathbb{F}_2[x]/x^{2(\ell_{i+1}-1)+\ell}$, the dealer extends the current r_0 and r_1 . Specifically, the dealer randomly selects $2(\ell_{i+1}-\ell_i)$ new coefficients in $\mathbb{F}_2$ respectively such that r_0 and r_1 are updated from $\mathbb{F}_2[x]/x^{2(\ell_i-1)+\ell}$ to $\mathbb{F}_2[x]/x^{2(\ell_{i+1}-1)+\ell}$. Then, the corresponding r_0 and r_1 are generated.

3.2 Proofs of Correctness and Security

In this subsection, we will prove the correctness and secrecy of the proposed scheme. Before that, we first present two important conclusions that provide useful results for the proofs.

Lemma 1 ([4]). *For any $n, k \in \mathbb{N}^+$, let $h(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{F}_p[x]$. If $a_0 \neq 0$, then $h(x)$ is invertible over $\mathbb{F}_p[x]/x^k$.*

Lemma 2 ([4]). *For any $d_1, d_2, k \in \mathbb{N}^+$ with $d_1 \leq k$ and $d_2 \leq k$, given $a(x), h(x) \in \mathbb{F}_p[x]$ with $a(x) \neq 0$, let d_1 denote the maximal extractable power of $a(x)$. Let $b(x) \in \mathbb{F}_p[x]$ be an unknown polynomial with the degree less than d_2 , and $b(x)$ satisfy the congruence equation $a(x)b(x) \equiv h(x) \pmod{x^k}$. Then if $d_1 + d_2 \leq k$, there exists a unique solution $b(x)$ with the degree less than d_2 .*

The Proof of Correctness According to the definition, our goal is to prove that the ℓ -bit secret s can be correctly reconstructed from the participants' shares when the sum of their weights is at least 3. It suffices to prove the boundary case where the total weight equals 3, and then other cases can be proven naturally. Since this boundary case itself includes various subcases, we focus on proving the following two fundamental cases. All other subcases can be viewed as adding new shares based on any of these two cases, and thus can be proven. Consequently, the proof for the boundary case is complete, which proves the corresponding correctness of the scheme.

Case 1. There exist three participants, each with weight 1.

Case 2. There exist two participants: one has weight 1 and the other has weight 2.

To reconstruct the secret s , the proof of each of the two cases proceeds according to the following steps. First, using the shares provided by the corresponding participants, we derive a system of equations with unknowns $\{r_0, r_1, s\}$ in the polynomial quotient ring $\mathbb{F}_2[x]$. Then, we apply the elimination method to eliminate the unknowns r_0 and r_1 , resulting in a congruence equation of the form $a(x)s \equiv b(x) \pmod{x^\phi}$, where $a(x)$ and $b(x)$ are known polynomials. Finally, we verify that the value of ℓ , adding the maximal extractable power of $a(x)$, is no more than ϕ . Consequently, by Lemma 2, we obtain the unique solution for s of $a(x)s \equiv b(x) \pmod{x^\phi}$ in $\mathbb{F}_2[x]/x^\ell$. The specific proofs for Case 1 and Case 2 are provided below.

Proof of Case 1. Without loss of generality, we denote three participants as P_i, P_j and P_k with $i < j < k$. Let c_i, c_j and c_k be the corresponding binary prefix codes of i, j and k , y_i, y_j and y_k be the polynomial forms of c_i, c_j and c_k , respectively. Let ℓ_i, ℓ_j and ℓ_k be the code length of i, j and k , thus we have $\ell_i \leq \ell_j \leq \ell_k$. Since the weight of each participant is 1, according to the algorithm $\mathcal{E}$, the corresponding shares from (2) are

$$\begin{cases} Z_i^{(s)} = r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, \\ Z_j^{(s)} = r_0 + r_1 y_j + s y_j^2 \pmod{x^{2(\ell_j-1)+\ell}}, \\ Z_k^{(s)} = r_0 + r_1 y_k + s y_k^2 \pmod{x^{2(\ell_k-1)+\ell}}. \end{cases} \quad (5)$$

Let $a, b \in \{i, j, k\}$ with $a \neq b$, as c_a is not a prefix of c_b , then $(y_a - y_b) \neq 0 \pmod{x^{\ell_a}}$. Denote $\ell_{a,b}$ as the maximal extractable power of $(y_a - y_b)$, then $0 \leq \ell_{a,b} < \min\{\ell_a, \ell_b\} - 1$. For (5), we multiply both sides of $Z_i^{(s)} = r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}$ by $y_j - y_k$, multiply both sides of $Z_j^{(s)} = r_0 + r_1 y_j + s y_j^2 \pmod{x^{2(\ell_j-1)+\ell}}$ by $y_i - y_k$, multiply both sides of $Z_k^{(s)} = r_0 + r_1 y_k + s y_k^2$

$(\text{mod } x^{2(\ell_k-1)+\ell})$ by $y_i - y_j$, respectively. Then, we can get

$$\begin{cases} Z_i^{(s)}(y_j - y_k) \equiv (r_0 + r_1 y_i + s y_i^2)(y_j - y_k) \pmod{x^{2(\ell_i-1)+\ell+\ell_{j,k}}}, \\ Z_j^{(s)}(y_i - y_k) \equiv (r_0 + r_1 y_j + s y_j^2)(y_i - y_k) \pmod{x^{2(\ell_j-1)+\ell+\ell_{i,k}}}, \\ Z_k^{(s)}(y_i - y_j) \equiv (r_0 + r_1 y_k + s y_k^2)(y_i - y_j) \pmod{x^{2(\ell_k-1)+\ell+\ell_{i,j}}}. \end{cases} \quad (6)$$

Summing all congruent equations in (6), we have

$$\begin{aligned} & s(y_j - y_k)(y_i - y_k)(y_i - y_j) \\ & \equiv Z_i^{(s)}(y_j - y_k) + Z_j^{(s)}(y_i - y_k) + Z_k^{(s)}(y_i - y_j) \pmod{x^\alpha}, \end{aligned} \quad (7)$$

where $\alpha = \min\{2(\ell_i - 1) + \ell + \ell_{j,k}, 2(\ell_j - 1) + \ell + \ell_{i,k}, 2(\ell_k - 1) + \ell + \ell_{i,j}\}$.

For the above equation (7), we find that $(y_j - y_k)(y_i - y_k)(y_i - y_j)$'s maximal extractable power is $\ell_{j,k} + \ell_{i,k} + \ell_{i,j}$, and $\ell_{j,k} + \ell_{i,k} + \ell_{i,j} + \ell \leq \alpha$. Let $Z = Z_i^{(s)}(y_j - y_k) + Z_j^{(s)}(y_i - y_k) + Z_k^{(s)}(y_i - y_j)$, using the conclusion of Lemma 2, there exists a unique s with degree less than ℓ satisfying (7), given by

$$s = \frac{Z}{x^{\ell_{j,k} + \ell_{i,k} + \ell_{i,j}}} \left(\frac{(y_j - y_k)(y_i - y_k)(y_i - y_j)}{x^{\ell_{j,k} + \ell_{i,k} + \ell_{i,j}}} \right)^{-1} \pmod{x^\ell}. \quad (8)$$

Thus, we can calculate s .

Proof of Case 2. We denote two participants as P_i and P_j with $i < j$. Without loss of generality, we assume that the weight of P_i is 1, and the weight of P_j is 2. The algorithm $\mathcal{E}$ constructs the corresponding shares $Z_i^{(s)}$ and $Z_j^{(s)} = [Z_{j,0}^{(s)}, Z_{j,1}^{(s)}]$ by (2) and (4) as

$$\begin{cases} Z_i^{(s)} = r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, \\ Z_{j,0}^{(s)} = r_0 + r_1 y_j + s y_j^2 \pmod{x^{2(\ell_j-1)+\ell}}, \\ Z_{j,1}^{(s)} = r_1 \pmod{x^{\ell_j+\ell-1}}. \end{cases} \quad (9)$$

Let $\ell_{i,j}$ be the maximal extractable power of $(y_i + y_j)$. We multiply $Z_{j,1}^{(s)}$ by $(y_i + y_j)$ and get

$$Z_{j,1}^{(s)}(y_i + y_j) \equiv r_1(y_i + y_j) \pmod{x^{\ell_i + \ell_{i,j} + \ell - 1}}. \quad (10)$$

As $\ell_{i,j} < \ell_i - 1 \leq \ell_j - 1$, then $\ell_i + \ell_{i,j} + \ell - 1 \leq 2(\ell_i - 1) + \ell \leq 2(\ell_j - 1) + \ell$, summing the values of (10), $Z_i^{(s)}$ and $Z_{j,0}^{(s)}$ in $\mathbb{F}_2[x]$, we get

$$s(y_i + y_j)^2 \equiv Z_i^{(s)} + Z_{j,0}^{(s)} + r_1(y_i + y_j) \pmod{x^{\ell_i + \ell_{i,j} + \ell - 1}}. \quad (11)$$

As $(y_i + y_j)^2$'s the maximal extractable power is $2\ell_{i,j}$, the bit length of s is ℓ , and $\ell_{i,j} < \ell_i - 1$, then $2\ell_{i,j} + \ell \leq \ell_i + \ell_{i,j} + \ell - 1$. According to the conclusion of Lemma 2, there exists a unique s with degree less than ℓ satisfying (11), which is given by

$$s = \frac{Z_i^{(s)} + Z_{j,0}^{(s)} + Z_{j,1}^{(s)}(y_i + y_j)}{x^{2\ell_{i,j}}} \left(\frac{(y_i + y_j)^2}{x^{2\ell_{i,j}}} \right)^{-1} \pmod{x^\ell}.$$

Combining the two cases above, we prove that the secret is reconstructed.

The Proof of Security To prove security, we need to demonstrate that any set of participants whose total weight is less than 3 cannot obtain any information about the secret s . We only prove the case where the sum of the weights is 2, the other cases can be verified naturally.

When the sum of the weights of these participants is 2, there are only the following two cases.

Case 1. There exists one participant with weight 2.

Case 2. There exist two participants, each with weight 1.

Proof of Case 1. We denote the participant as P_i and its weight is 2. According to the algorithm $\mathcal{E}$, the corresponding share is

$$Z_i^{(s)} = [Z_{i,0}^{(s)}, Z_{i,1}^{(s)}] = [r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, r_1 \pmod{x^{\ell_i+\ell-1}}].$$

Let d_i denote the maximal extractable power of y_i . Although r_1 is known in the polynomial ring $\mathbb{F}_2[x]/x^{\ell_i+\ell-1}$, the term $r_1 y_i$ is known in the polynomial ring $\mathbb{F}_2[x]/x^{\ell_i+d_i+\ell-1}$. By substituting this value $r_1 y_i$ into the expression $r_0 + r_1 y_i + s y_i^2$, we obtain the value of $r_0 + s y_i^2 \pmod{x^{\ell_i+d_i+\ell-1}}$. As $d_i < \ell_i$ and r_0 is the random variables uniformly distributed in $\mathbb{F}_2[x]/x^{2(\ell_i-1)+\ell}$, r_0 is the random variables uniformly distributed in $\mathbb{F}_2[x]/x^{\ell_i+d_i+\ell-1}$, $r_0 + s y_i^2$ is uniformly random in $\mathbb{F}_2[x]/x^{\ell_i+d_i+\ell-1}$. Hence, $Z_i^{(s)}$ is uniformly random in $\mathbb{F}_2[x]$ for each selection of s .

Proof of Case 2. We take two participants as P_i and P_j with $i < j$ and the weight of each participant is 1. For given the secret s , the algorithm $\mathcal{E}$ constructs the corresponding shares as

$$\begin{cases} Z_i^{(s)} = r_0 + r_1 y_i + s y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, \\ Z_j^{(s)} = r_0 + r_1 y_j + s y_j^2 \pmod{x^{2(\ell_j-1)+\ell}}. \end{cases} \quad (12)$$

According to the definition of secrecy, we choose two distinct secrets s_0 and s_1 , then denote $Z_k^{(s_0)}$ and $Z_k^{(s_1)}$ as the corresponding shares for P_k , respectively. For any given $z_i \in \mathbb{F}_2[x]/x^{2(\ell_i-1)+\ell}$ and $z_j \in \mathbb{F}_2[x]/x^{2(\ell_j-1)+\ell}$, we need to prove that the following two probabilities are equal, i.e.,

$$P(\{Z_i^{(s_0)} = z_i, Z_j^{(s_0)} = z_j\}) = P(\{Z_i^{(s_1)} = z_i, Z_j^{(s_1)} = z_j\}). \quad (13)$$

Considering $P(\{Z_i^{(s_0)} = z_i, Z_j^{(s_0)} = z_j\})$, when the secret is selected as s_0 and $Z_i^{(s_0)} = z_i, Z_j^{(s_0)} = z_j$, we have

$$\begin{cases} z_i = r_0 + r_1 y_i + s_0 y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, \\ z_j = r_0 + r_1 y_j + s_0 y_j^2 \pmod{x^{2(\ell_j-1)+\ell}}, \end{cases} \quad (14)$$

where the random variables (r_0, r_1) are unknown.

For $P(\{Z_i^{(s_1)} = z_i, Z_j^{(s_1)} = z_j\})$, when the secret is s_1 and $Z_i^{(s_1)} = z_i, Z_j^{(s_1)} = z_j$, we get

$$\begin{cases} z_i = r_0 + r_1 y_i + s_1 y_i^2 \pmod{x^{2(\ell_i-1)+\ell}}, \\ z_j = r_0 + r_1 y_j + s_1 y_j^2 \pmod{x^{2(\ell_j-1)+\ell}}, \end{cases} \quad (15)$$

where the random variables (r_0, r_1) are also unknown.

To avoid confusion of (r_0, r_1) in (14) and (r_0, r_1) in (15), we denote the corresponding variables in (14) and (15) as $(r_{0,0}, r_{0,1})$ and $(r_{1,0}, r_{1,1})$, respectively. Substituting these variables into (14) and (15), respectively, then (14) and (15) respectively are written as

$$\begin{cases} z_i = r_{0,0} + r_{0,1}y_i + s_0y_i^2 & (\text{mod } x^{2(\ell_i-1)+\ell}), \\ z_j = r_{0,0} + r_{0,1}y_j + s_0y_j^2 & (\text{mod } x^{2(\ell_j-1)+\ell}), \end{cases} \quad (16)$$

and

$$\begin{cases} z_i = r_{1,0} + r_{1,1}y_i + s_1y_i^2 & (\text{mod } x^{2(\ell_i-1)+\ell}), \\ z_j = r_{1,0} + r_{1,1}y_j + s_1y_j^2 & (\text{mod } x^{2(\ell_j-1)+\ell}). \end{cases} \quad (17)$$

Observing that (16) and (17), the calculation is performed on $\mathbb{F}_2[x]/x^{2(\ell_j-1)+\ell}$, thus the space of the solution vector $(r_{0,0}, r_{0,1})$ and $(r_{1,0}, r_{1,1})$ can be regarded as $\{\mathbb{F}_2[x]/x^{2(\ell_j-1)+\ell}\}^2$, denoted by U . Then the value of $P(\{Z_i^{(s_0)} = z_i, Z_j^{(s_0)} = z_j\})$ is equal to the ratio of the number of solutions $(r_{0,0}, r_{0,1})$ for (16) in the whole space U . And the value of $P(\{Z_i^{(s_1)} = z_i, Z_j^{(s_1)} = z_j\})$ is equal to the ratio of the number of solutions $(r_{1,0}, r_{1,1})$ for (17) in the whole space U .

Next, we show that the number of solutions $(r_{0,0}, r_{0,1})$ in (16) and $(r_{1,0}, r_{1,1})$ in (17) is equal, to prove that (13) holds. Without loss of generality, we assume that (16) has N_0 solutions and (17) has N_1 solutions with $N_0 > N_1$. Let $\mathbb{R}_0$ and $\mathbb{R}_1$ respectively be the solution sets of (16) and (17).

For (16) and (17), we subtract the first equation in (16) from the first equation in (17), and subtract the second equation in (16) from the second equation in (17), then obtain

$$\begin{cases} (r_{1,0} - r_{0,0}) + (r_{1,1} - r_{0,1})y_i + (s_1 - s_0)y_i^2 = 0 & (\text{mod } x^{2(\ell_i-1)+\ell}), \\ (r_{1,0} - r_{0,0}) + (r_{1,1} - r_{0,1})y_j + (s_1 - s_0)y_j^2 = 0 & (\text{mod } x^{2(\ell_j-1)+\ell}). \end{cases} \quad (18)$$

Let $\Delta_s = s_0 - s_1$, $\Delta_{r_0} = r_{1,0} - r_{0,0}$ and $\Delta_{r_1} = r_{1,1} - r_{0,1}$, where $\Delta_s \in \mathbb{F}_2[x]/x^\ell$, $\Delta_{r_0}, \Delta_{r_1} \in \mathbb{F}_2[x]/x^{2(\ell_j-1)+\ell}$. Substitute the above variables into (18) and simplify it as

$$\begin{cases} \Delta_{r_0} + \Delta_{r_1}y_i = \Delta_s y_i^2 & (\text{mod } x^{2(\ell_i-1)+\ell}), \\ \Delta_{r_0} + \Delta_{r_1}y_j = \Delta_s y_j^2 & (\text{mod } x^{2(\ell_j-1)+\ell}). \end{cases} \quad (19)$$

Subtracting the first equation from the second equation in (19), we can get

$$\Delta_{r_1}(y_j - y_i) = \Delta_s(y_j - y_i)^2 \quad (\text{mod } x^{2(\ell_i-1)+\ell}). \quad (20)$$

As c_i is not a prefix of c_j , we have $y_j - y_i \neq 0 \pmod{x^{\ell_i}}$. Since $\ell_{i,j}$ denotes the maximal extractable power of $(y_j - y_i)$ and $0 \leq \ell_{i,j} < \ell_i - 1$, we have

$$\Delta_{r_1} = \Delta_s(y_j - y_i) \quad (\text{mod } x^{2(\ell_i-1)+\ell-\ell_{i,j}}). \quad (21)$$

Taking the value of Δ_{r_1} into (19), we can also compute

$$\Delta_{r_0} = \Delta_s y_j y_i \quad (\text{mod } x^{2(\ell_i-1)+\ell-\ell_{i,j}}), \quad (22)$$

then we denote $\Delta^* = (\Delta_s y_j y_i, \Delta_s (y_j - y_i))$ from (21) and (22), and Δ^* is one of solutions of (19).

According to the assumptions, (16) has N_0 solutions. As $\mathbb{R}_0$ is the solution set of (16), we choose one of the solutions in $\mathbb{R}_0$ and denote it as $r = (r_{0,0}, r_{0,1})$, then $r + \Delta^* = (r_{0,0} + \Delta_s y_j y_i, r_{0,1} + \Delta_s (y_j - y_i))$ is a solution of (17) by summing (16) and (19). When r is taken across the whole solution set $\mathbb{R}_0$, (17) has at least N_0 different solutions, which contradicts that (17) has N_1 solutions. Therefore, (16) and (17) have the same number of solutions. Thus, we can derive $P(\{Z_i^{(s_0)} = z_i, Z_j^{(s_0)} = z_j\}) = P(\{Z_i^{(s_1)} = z_i, Z_j^{(s_1)} = z_j\})$. Using the definition of secrecy, we have proven the security of the proposed scheme.

3.3 Share Size

In this part, we will analyze the share size of the proposed scheme. For the m -th participant P_m with the corresponding weight w_m satisfying $1 \leq w_m \leq 2$, from (2), (3) and (4), the corresponding share $Z_m^{(s)}$ is

$$Z_m^{(s)} = [Z_{m,0}^{(s)}, \dots, Z_{m,w_m-1}^{(s)}],$$

where $Z_{m,j}^{(s)}$ with $j \in \{0, \dots, w_m - 1\}$ denotes the j -th order Hasse derivative of $f(y)$ with respect to y , evaluated at $y = y_m$, and reduced modulo $x^{(2-j)(\ell_m-1)+\ell}$. Thus, each $Z_{m,j}^{(s)}$ can be regarded as a polynomial of x in $\mathbb{F}_2$ with the degree less than $(2-j)(\ell_m-1) + \ell$, where ℓ_m is the length of the binary prefix code for the positive integer m . Then, the size of the corresponding share is

$$B(Z_m^{(s)}) = \sum_{j=0}^{w_m-1} ((2-j)(\ell_m-1) + \ell) = w_m(2 - \frac{w_m-1}{2})(\ell_m-1) + w_m\ell. \quad (23)$$

By analyzing the above result, if we directly use the conventional scheme proposed in [4] to distribute w_m shares to participant P_m , since the size of each share is $2(\ell_m-1) + \ell$, then we have

$$B(Z_m^{(s)}) = 2w_m(\ell_m-1) + w_m\ell. \quad (24)$$

Comparing (23) and (24), the value of (23) is significantly smaller than the value of (24) for $1 \leq w_m \leq 2$, our proposed scheme saves $\frac{w_m(w_m-1)}{2}(\ell_m-1)$ bits, thus achieves a significantly smaller share size.

Observing (23), we find that $B(Z_m^{(s)})$ may be different when choosing different binary prefix codes. Next, we show the corresponding share size by using several binary prefix codes. We denote by $L(\cdot)$ the codeword length for encoding m for $m \in \mathbb{N}^+$. Considering γ code [24], a widely used integer universal code, the codeword length of $\gamma(m)$ is given by

$$L(\gamma(m)) = 2\lceil \lg m \rceil + 1.$$

Therefore, when using γ code as the binary prefix code, the size of the m -th share satisfies

$$B(Z_m^{(s)}) = 2w_m(2 - \frac{w_m - 1}{2})\lfloor \lg m \rfloor + w_m\ell. \quad (25)$$

Except for the γ code, we also consider another binary prefix code, the δ code [24]. The codeword length of $\delta(m)$ is given by

$$L(\delta(m)) = \lfloor \lg m \rfloor + 2\lfloor \lg(\lfloor \lg m \rfloor + 1) \rfloor + 1.$$

Therefore, if using δ code as the binary prefix code, the share size of the m -th satisfies

$$B(Z_m^{(s)}) = w_m(2 - \frac{w_m - 1}{2})(\lfloor \lg m \rfloor + 2\lfloor \lg(\lfloor \lg m \rfloor + 1) \rfloor) + w_m\ell. \quad (26)$$

4 The Extension of A Weighted Evolving t -Threshold Scheme

As shown in the previous section, we have completed the construction of the framework for a weighted evolving 3-threshold secret sharing scheme. Notably, the proposed scheme is extensible, allowing natural generalization to higher threshold cases. In this section, we extend the prior scheme to the evolving t -threshold scheme, where $t \geq 3$. We will give the construction of the weighted evolving t -threshold scheme over $\mathbb{F}_2[x]$ for an ℓ -bit secret s . The scheme allows the dealer to distribute the share to each participant according to its weight, such that the secret can be recovered from the set of participants when the sum of weights is no less than t , and any set of participants when the sum of weights is less than t , cannot deduce any information about the secret.

4.1 Proposed t -Threshold Scheme

For a given ℓ -bit secret s , we first construct a polynomial $f(y)$, defined as

$$f(y) = \sum_{m=0}^{t-2} r_m y^m + s y^{t-1}, \quad (27)$$

where each coefficient r_m is randomly chosen from $\mathbb{F}_2[[x]]$ for $0 \leq m \leq t-2$. Let $\mathcal{P} = \{P_1, P_2, \dots, P_n, \dots\}$ denote the set of participants. For any participant $P_i \in \mathcal{P}$, let w_i represent the corresponding weight of participant P_i with $0 < w_i < t$. Given a set of prefix codes for integers, c_i denotes the codeword of the positive integer i , ℓ_i represents the bit length, and $y_i \in \mathbb{F}_2[x]$ denotes the polynomial form of c_i . For the i -th participant P_i with weight w_i , the algorithm $\mathcal{E}$ constructs the corresponding share $Z_i^{(s)}$, which consists of w_i parts, i.e.,

$$Z_i^{(s)} = [Z_{i,0}^{(s)}, Z_{i,1}^{(s)}, \dots, Z_{i,w_i-1}^{(s)}], \quad (28)$$

where $Z_{i,j}^{(s)}$ with $j \in \{0, 1, \dots, w_i - 1\}$ is calculated below

$$Z_{i,j}^{(s)} = D^j f(y_i) \pmod{x^{(t-j-1)(\ell_i-1)+\ell}}. \quad (29)$$

Here $D^j f(y_i)$ denotes the j -th order Hasse derivative of $f(y)$ with respect to y , evaluated at $y = y_i$, i.e.,

$$D^j f(y_i) = \sum_{m=0}^{t-2} \binom{m}{j} r_m y_i^{m-j} + \binom{t-1}{j} s y_i^{t-1-j}. \quad (30)$$

Notably, when constructing the corresponding share $Z_i^{(s)}$, though $\{r_m\}_{m=0}^{t-2}$ are defined randomly chosen in $\mathbb{F}_2[[x]]$ for (27), as the operation of calculating each $Z_{i,j}^{(s)}$ is performed over $\mathbb{F}_2[x]/x^k$ where k is at most $(t-1)(\ell_i-1)+\ell$ as in (29), the dealer only needs to choose the parts of $\{r_m\}_{m=0}^{t-2}$ such that each $r_m \in \mathbb{F}_2[x]/x^{(t-1)(\ell_i-1)+\ell}$ in (29). The construction method for updating $\{r_m\}_{m=0}^{t-2}$ has been similarly described in Section 3.2, and thus will not be repeated here.

4.2 Proofs of Correctness and Security

We prove the correctness and secrecy of the proposed scheme in this subsection.

The Proof of Correctness We need to prove that if the sum of the participants' weights is at least t , then their combined shares can reconstruct the ℓ -bit secret. By analyzing, we only need to prove the boundary case that these participants can reconstruct s when the sum of their weights equals t . Then other cases can be proven naturally.

In Section 3.2, we gave the corresponding proof of correctness when the threshold t equals to 3. To facilitate understanding, we employed a case-by-case analysis to prove the correctness. Specifically, we first demonstrated that proving the boundary case suffices to establish correctness. Through analysis, we observed that the boundary case itself includes various subcases. It suffices to prove the two most fundamental ones, and then all other subcases are proven naturally. Therefore, we provided detailed proofs for each of two fundamental cases. However, for an arbitrary threshold t , the boundary case will be classified into more subcases, and the classification becomes increasingly complex as the threshold t grows. Therefore, it is infeasible to use a case-by-case analysis to prove the corresponding boundary case for the general threshold t . Consequently, we employ a unified approach to prove the corresponding boundary case, thereby establishing the correctness of the proposed t -threshold scheme.

The proof proceeds as follows. First, using the shares from the corresponding participants, we derive a system of equations with t equations and t unknowns $\{r_0, \dots, r_{t-2}, s\}$ in $\mathbb{F}_2[x]$. Then, we apply the elimination method to eliminate $t-1$ unknowns $\{r_0, \dots, r_{t-2}\}$ and get a congruence equation of the form $a_1(x)s \equiv b_1(x) \pmod{x^\ell}$, where $a_1(x)$ and $b_1(x)$ are known polynomials. Finally, we prove that the value of ℓ adding the maximal extractable power of $a_1(x)$ is no more than

χ . Consequently, by Lemma 2, we obtain the unique solution for s of $a_1(x)s \equiv b_1(x) \pmod{x^\chi}$ in $\mathbb{F}_2[x]/x^\ell$. The specific proof is described below.

We assume that there are n participants, and the sum of their weights is t . Denote the n participants as $P_{i_1}, P_{i_2}, \dots, P_{i_n}$ with $i_1 < \dots < i_n$. For any $u \in \{1, \dots, n\}$, since c_{i_u} is the prefix code of i_u , y_{i_u} is the polynomial form of c_{i_u} and ℓ_{i_u} is the code length of i_u . By the properties of prefix codes, ℓ_{i_u} is non-decreasing with respect to u . Let w_{i_u} denote the weight of participant P_{i_u} . Without loss of generality, we assume the weights are ordered such that $0 < w_{i_1} \leq w_{i_2} \leq \dots \leq w_{i_n} < t$, satisfying the threshold condition $\sum_{u=1}^n w_{i_u} = t$. For the participant P_{i_u} , $\mathcal{E}$ constructs the share $Z_{i_u}^{(s)}$ according to (28) as

$$Z_{i_u}^{(s)} = [Z_{i_u,0}^{(s)}, Z_{i_u,1}^{(s)}, \dots, Z_{i_u,w_{i_u}-1}^{(s)}], \quad (31)$$

where each component $Z_{i_u,j}^{(s)}$ for $j \in \{0, 1, \dots, w_{i_u} - 1\}$ is computed as

$$\begin{aligned} Z_{i_u,j}^{(s)} &= D^j f(y_{i_u}) \pmod{x^{(t-j-1)(\ell_{i_u}-1)+\ell}} \\ &= \sum_{m=0}^{t-2} \binom{m}{j} r_m y_{i_u}^{m-j} + \binom{t-1}{j} s y_{i_u}^{t-1-j} \pmod{x^{(t-j-1)(\ell_{i_u}-1)+\ell}}. \end{aligned} \quad (32)$$

Consequently, collecting the shares from all n participants $\{P_{i_u}\}_{u=1}^n$ forms a system of t linear equations as follows

$$\left\{ \begin{array}{l} Z_{i_1,0}^{(s)} = \sum_{m=0}^{t-2} r_m y_{i_1}^m + s y_{i_1}^{t-1} \pmod{x^{L_{i_1,0}}}, \\ Z_{i_1,1}^{(s)} = \sum_{m=0}^{t-2} \binom{m}{1} r_m y_{i_1}^{m-1} + \binom{t-1}{1} s y_{i_1}^{t-2} \pmod{x^{L_{i_1,1}}}, \\ \dots \\ Z_{i_1,w_{i_1}-1}^{(s)} = \sum_{m=0}^{t-2} \binom{m}{w_{i_1}-1} r_m y_{i_1}^{m-w_{i_1}+1} + \binom{t-1}{w_{i_1}-1} s y_{i_1}^{t-w_{i_1}} \pmod{x^{L_{i_1,w_{i_1}-1}}}, \\ \vdots \\ Z_{i_n,0}^{(s)} = \sum_{m=0}^{t-2} r_m y_{i_n}^m + s y_{i_n}^{t-1} \pmod{x^{L_{i_n,0}}}, \\ Z_{i_n,1}^{(s)} = \sum_{m=0}^{t-2} \binom{m}{1} r_m y_{i_n}^{m-1} + \binom{t-1}{1} s y_{i_n}^{t-2} \pmod{x^{L_{i_n,1}}}, \\ \dots \\ Z_{i_n,w_{i_n}-1}^{(s)} = \sum_{m=0}^{t-2} \binom{m}{w_{i_n}-1} r_m y_{i_n}^{m-w_{i_n}+1} + \binom{t-1}{w_{i_n}-1} s y_{i_n}^{t-w_{i_n}} \pmod{x^{L_{i_n,w_{i_n}-1}}}, \end{array} \right. \quad (33)$$

where $L_{i_u,j} = (t-1-j)(\ell_{i_u}-1) + \ell$ for $0 \leq j \leq w_{i_u} - 1$ and $1 \leq u \leq n$.

The above system of congruence equations can be compactly expressed in matrix form as

$$\mathbf{V}_y \cdot \mathbf{r} \equiv \mathbf{Z} \quad (34)$$

modulo the corresponding power of x , where $\mathbf{r} = (r_0, r_1, \dots, r_{t-2}, s)^T$ and $\mathbf{Z} = (Z_{i_1,0}^{(s)}, \dots, Z_{i_1,w_{i_1}-1}^{(s)}, \dots, Z_{i_n,0}^{(s)}, \dots, Z_{i_n,w_{i_n}-1}^{(s)})^T$ is the concatenated vector of shares.

The matrix $\mathbf{V}_y$ is a $t \times t$ confluent Vandermonde matrix composed of n blocks, where the u -th block V_u is structured as

$$V_u = \begin{pmatrix} 1 & y_{i_u} & y_{i_u}^2 & \cdots & y_{i_u}^{t-1} \\ 0 & 1 & \binom{2}{1}y_{i_u} & \cdots & \binom{t-1}{1}y_{i_u}^{t-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{t-1}{w_{i_u}-1}y_{i_u}^{t-w_{i_u}} \end{pmatrix}.$$

Therefore, the matrix $\mathbf{V}_y$ takes the form

$$\mathbf{V}_y = \begin{pmatrix} 1 & y_{i_1} & y_{i_1}^2 & \cdots & y_{i_1}^{t-1} \\ 0 & 1 & \binom{2}{1}y_{i_1} & \cdots & \binom{t-1}{1}y_{i_1}^{t-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{t-1}{w_{i_1}-1}y_{i_1}^{t-w_{i_1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & y_{i_n} & y_{i_n}^2 & \cdots & y_{i_n}^{t-1} \\ 0 & 1 & \binom{2}{1}y_{i_n} & \cdots & \binom{t-1}{1}y_{i_n}^{t-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{t-1}{w_{i_n}-1}y_{i_n}^{t-w_{i_n}} \end{pmatrix}, \quad (35)$$

and the determinant is

$$\det(\mathbf{V}_y) = \prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}. \quad (36)$$

For any $u \neq v$ with $1 \leq u, v \leq n$, since $y_{i_u} - y_{i_v} \neq 0$, then $\det(\mathbf{V}_y) \neq 0$.

In order to calculate s , we need to eliminate these elements $r_0, \dots, r_{t-2}$. Let $\mathbf{G}_t$ be the new matrix obtained by replacing the t -th column of matrix $\mathbf{V}_y$ with the vector $\mathbf{Z}$. For $1 \leq u \leq n$, $0 \leq j \leq w_{i_u}-1$ with $\sum_{u=1}^n w_{i_u} = t$, let $\mathbf{G}_{t,u,j}$ denote the submatrix of $\mathbf{G}_t$ obtained by deleting the row and the column containing the element $Z_{i_u,j}^{(s)}$ of the t -th column. Let $\mathbf{c}$ be a column vector comprising t elements $\{\{\det(\mathbf{G}_{t,u,j})\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$. For the column vector $\mathbf{Z}$ in (34), we left multiply $\mathbf{Z}$ by the transpose of $\mathbf{c}$, then we have

$$\mathbf{c}^T \mathbf{Z} = \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \det(\mathbf{G}_{t,u,j}) \cdot Z_{i_u,j}^{(s)}. \quad (37)$$

Substituting $\mathbf{Z} \equiv \mathbf{V}_y \cdot \mathbf{r}$ into this expression and expanding based on (33), then we have

$$\begin{aligned} \mathbf{c}^T \mathbf{Z} &\equiv \mathbf{c}^T \cdot \mathbf{V}_y \mathbf{r} \\ &\equiv \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \det(\mathbf{G}_{t,u,j}) \cdot \left(\sum_{m=0}^{t-2} \binom{m}{j} r_m y_{i_u}^{m-j} + \binom{t-1}{j} s y_{i_u}^{t-1-j} \right) \pmod{x^\xi}, \end{aligned} \quad (38)$$

where $\xi = \min_{u,j} \{p_x(\det(\mathbf{G}_{t,u,j})) + L_{i_u,j}\}$, $p_x(\det(\mathbf{G}_{t,u,j}))$ is the maximal extractable power of $\det(\mathbf{G}_{t,u,j})$ and $L_{i_u,j} = (t-1-j)(\ell_{i_u} - 1) + \ell$ with $u \in \{1, 2, \dots, n\}$ and $j \in \{0, 1, \dots, w_{i_u} - 1\}$.

In $\mathbb{F}_2[x]$, observing the right-hand side of (38), the coefficient of each parameter r_m for $0 \leq m \leq t-2$ is

$$\sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \binom{m}{j} y_{i_u}^{m-j} \cdot \det(\mathbf{G}_{t,u,j}),$$

denoted as b_m .

Let $\mathbf{v}_m$ be a column vector comprising t elements $\{\{\binom{m}{j} y_{i_u}^{m-j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$, then $\mathbf{v}_m$ is identical to the $(m+1)$ -th column of matrix $\mathbf{V}_y$. Let $\mathbf{G}_{\mathbf{v}_m}$ be the new matrix obtained by replacing the t -th column of matrix $\mathbf{V}_y$ with the vector $\mathbf{v}_m$. According to the definition of $\mathbf{G}_{t,u,j}$, we find that it equals to the submatrix of $\mathbf{V}_y$ obtained by deleting the row and the column containing the element $\binom{t-1}{j} y_{i_u}^{t-1-j}$ of the t -th column, then it is identical to the submatrix of $\mathbf{G}_{\mathbf{v}_m}$ obtained by deleting the row and the column containing the element $\binom{m}{j} y_{i_u}^{m-j}$ of the t -th column. Therefore, the value of b_m is equal to the determinant of matrix $\mathbf{G}_{\mathbf{v}_m}$ expanded along its t -column. As the matrix $\mathbf{G}_{\mathbf{v}_m}$'s t -th column is the same as its $(m+1)$ -th column for $0 \leq m \leq t-2$, then

$$b_m = \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \binom{m}{j} y_{i_u}^{m-j} \cdot \det(\mathbf{G}_{t,u,j}) = \det(\mathbf{G}_{\mathbf{v}_m}) = 0. \quad (39)$$

Thus, we derive $b_m = 0$ for $0 \leq m \leq t-2$.

We proceed to observe the right-hand side of (38), and then find that the coefficient of s is

$$\sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \binom{t-1}{j} y_{i_u}^{t-1-j} \cdot \det(\mathbf{G}_{t,u,j}),$$

denoted as b_t .

Let $\mathbf{v}_t$ be a column vector comprising t elements $\{\{\binom{t-1}{j} y_{i_u}^{t-1-j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$, then $\mathbf{v}_t$ is equal to the last column of the matrix $\mathbf{V}_y$. As $\mathbf{G}_{t,u,j}$ is the same as the submatrix of $\mathbf{V}_y$ obtained by deleting the row and the column containing the element $\binom{t-1}{j} y_{i_u}^{t-1-j}$ of the t -th column, then we derive that the value of b_t is equal to the determinant of matrix $\mathbf{V}_y$ expanded along its last column. Thus, we have

$$b_t = \det(\mathbf{V}_y) = \prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}. \quad (40)$$

Substituting the results of (39) and (40) into (38), we obtain

$$\mathbf{c}^T \mathbf{Z} = \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \det(\mathbf{G}_{t,u,j}) \cdot Z_{i_u,j}^{(s)}$$

$$\begin{aligned}
 &\equiv \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \det(\mathbf{G}_{t,u,j}) \cdot \left(\sum_{m=0}^{t-2} \binom{m}{j} r_m y_{i_u}^{m-j} + \binom{t-1}{j} s y_{i_u}^{t-1-j} \right) \pmod{x^\xi} \\
 &\equiv \sum_{m=0}^{t-2} r_m \cdot \left(\sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \binom{m}{j} y_{i_u}^{m-j} \cdot \det(\mathbf{G}_{t,u,j}) \right) \\
 &\quad + s \cdot \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \binom{t-1}{j} y_{i_u}^{t-1-j} \cdot \det(\mathbf{G}_{t,u,j}) \pmod{x^\xi} \\
 &\equiv \sum_{m=0}^{t-2} r_m b_m + s b_t \pmod{x^\xi} \\
 &\equiv s \cdot \prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}} \pmod{x^\xi}. \tag{41}
 \end{aligned}$$

To ensure that s can be recovered modulo x^ℓ , according to the conclusion of Lemma 2, we must prove that $\xi \geq p_x\left(\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}\right) + \ell$. The following theorem provides a useful result to verify it.

Theorem 1. *Let t, n, i_u, w_{i_u}, j be positive integers with $t \geq 2$, and let $1 \leq u, v \leq n$. For $1 \leq u \leq n$, they satisfy $1 \leq w_{i_u} \leq t-1$, $0 \leq j \leq w_{i_u}-1$, and $\sum_{u=1}^n w_{i_u} = t$. Given a set of prefix codes for integers, c_{i_u} denotes the codeword of the positive integer i_u , ℓ_{i_u} represents the bit length, and $y_{i_u} \in \mathbb{F}_2[x]$ denotes the polynomial form of c_{i_u} . For any polynomial $a(x) \in \mathbb{F}_2[x]$, let $p_x(a(x))$ denote the maximal extractable power of $a(x)$. Let $\mu = \max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\}$ and $\eta = p_x\left(\prod_{v \neq u} (y_{i_u} - y_{i_v})^{w_{i_v}}\right)$. Then we have*

$$p_x(\det(\mathbf{V}_y)) - p_x(\det(\mathbf{G}_{t,u,j})) \leq \eta + (w_{i_u} - j - 1)\mu. \tag{42}$$

Proof. The detailed proof is provided in Appendix because of space limitations.

Next, we begin to prove the inequality $\xi \geq p_x\left(\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}\right) + \ell$. As $\xi = \min_{u,j} \{p_x(\det(\mathbf{G}_{t,u,j})) + L_{i_u,j}\}$, where $L_{i_u,j} = (t-1-j)(\ell_{i_u}-1) + \ell$ for $1 \leq u \leq n$, $0 \leq j \leq w_{i_u}-1$ and $\det(\mathbf{V}_y) = \prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}$, combining the conclusion of Theorem 1, we get

$$\begin{aligned}
 &\xi - p_x\left(\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}\right) - \ell \\
 &= \min_{u,j} \{p_x(\det(\mathbf{G}_{t,u,j})) + L_{i_u,j}\} - p_x(\det(\mathbf{V}_y)) - \ell \\
 &= \min_{u,j} \{p_x(\det(\mathbf{G}_{t,u,j})) + (t-1-j)(\ell_{i_u}-1) + \ell\} - p_x(\det(\mathbf{V}_y)) - \ell \\
 &= \min_{u,j} \{p_x(\det(\mathbf{G}_{t,u,j})) + (t-1-j)(\ell_{i_u}-1)\} - p_x(\det(\mathbf{V}_y))
 \end{aligned}$$

$$\begin{aligned}
&= \min_{u,j} \{p_x(\det(\mathbf{G}_{t,u,j})) - p_x(\det(\mathbf{V}_y)) + (t-1-j)(\ell_{i_u} - 1)\} \\
&= p_x(\det(\mathbf{G}_{t,u^*,j^*})) - p_x(\det(\mathbf{V}_y)) + (t-1-j^*)(\ell_{i_{u^*}} - 1),
\end{aligned}$$

where (u^*, j^*) is the pair of indices that attains the minimum in the last expression. For notational simplicity, we write $u = u^*$ and $j = j^*$ in the following derivation. Then, we have

$$\begin{aligned}
& p_x(\det(\mathbf{G}_{t,u,j})) - p_x(\det(\mathbf{V}_y)) + (t-1-j)(\ell_{i_u} - 1) \\
& \geq -\eta - (w_{i_u} - j - 1)\mu + (t-1-j)(\ell_{i_u} - 1) \\
& = -p_x\left(\prod_{v \neq u} (y_{i_u} - y_{i_v})^{w_{i_v}}\right) - (w_{i_u} - j - 1) \max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\} \\
& \quad + (t-1-j)(\ell_{i_u} - 1) \\
& \stackrel{(a)}{\geq} -\sum_{v \neq u} (w_{i_v}(\ell_{i_u} - 1)) - (w_{i_u} - j - 1)(\ell_{i_u} - 1) + (t-1-j)(\ell_{i_u} - 1) \\
& = (t-1-j-w_{i_u}+j+1-\sum_{v \neq u} w_{i_v})(\ell_{i_u} - 1) = 0, \tag{43}
\end{aligned}$$

where (a) holds because $-p_x\left(\prod_{v \neq u} (y_{i_u} - y_{i_v})^{w_{i_v}}\right) = -\sum_{v \neq u} w_{i_v} p_x(y_{i_u} - y_{i_v}) \geq -\sum_{v \neq u} w_{i_v}(\ell_{i_u} - 1)$ and $-\max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\} \geq -(\ell_{i_u} - 1)$ according to the properties of prefix codes for $1 \leq u \leq n$. Thus $p_x\left(\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}\right) + \ell \leq \xi$.

Consider the congruence equation mentioned in (41) as

$$s \cdot \prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}} \equiv \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \det(\mathbf{G}_{t,u,j}) \cdot Z_{i_u,j}^{(s)} \pmod{x^\xi}.$$

For any $u \neq v$ with $1 \leq u, v \leq n$, since $y_{i_u} - y_{i_v} \neq 0$, let L_{i_u, i_v} be the maximal extractable power of $y_{i_u} - y_{i_v}$, then the maximal extractable power of $\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}$ is $\sum_{1 \leq u < v \leq n} w_{i_v} w_{i_u} \cdot L_{i_u, i_v}$, i.e., we have $\sum_{1 \leq u < v \leq n} w_{i_v} w_{i_u} \cdot L_{i_u, i_v} = p_x\left(\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}\right)$. Combining the result $p_x\left(\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}\right) + \ell \leq \xi$ of (43) and the conclusion of Lemma 2, we can recover the unique solution about s of (41) in $\mathbb{F}_2[x]/x^\ell$ as

$$s = \frac{\sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} \det(\mathbf{G}_{t,u,j}) \cdot Z_{i_u,j}^{(s)}}{x^{\sum_{1 \leq u < v \leq n} w_{i_v} w_{i_u} \cdot L_{i_u, i_v}}} \left(\frac{\prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_v} w_{i_u}}}{x^{\sum_{1 \leq u < v \leq n} w_{i_v} w_{i_u} \cdot L_{i_u, i_v}}} \right)^{-1} \pmod{x^\ell}. \tag{44}$$

Therefore, the correctness of the proposed scheme has been proved completely.

Remark 1. It is worth noting that, for the specific threshold, such as $t = 3$, we employed a case-by-case analysis to establish correctness, as described in

Section 3.2. Specifically, we first demonstrated that proving the boundary case is sufficient to establish the scheme's correctness. We then classify this boundary case into two fundamental subcases and provide detailed proofs for each. For a general threshold t , we similarly established that proving the boundary case is sufficient to show correctness, while we did not use case-by-case analysis to prove the boundary case. Instead, we proposed a unified approach to handle the boundary case. The proof step of this unified approach is the same as that for each of the two cases for $t = 3$. Therefore, this unified approach serves as a natural generalization of our earlier reasoning in Section 3.2. Through the unified approach, we conduct the constructive proof more concisely and universally.

The Proof of Security To prove security, we need to show that the shares of participants whose sum of weights is less than t cannot reconstruct the ℓ -bit secret s . Through analysis, we only need to prove the boundary case, in which these participants with the sum of weights as $t-1$, cannot reveal any information about the secret s . Then other cases can be verified naturally.

We assume there exist n participants whose weights equal $t-1$. Denote the n participants as $P_{i_1}, P_{i_2}, \dots, P_{i_n}$ with $i_1 < \dots < i_n$. For any $u \in \{1, \dots, n\}$, recall that c_{i_u} is the prefix code of i_u , y_{i_u} is the polynomial form of c_{i_u} and ℓ_{i_u} is the code length of i_u , thus ℓ_{i_u} is increasing on u . Let w_{i_u} denote the participant P_{i_u} 's weight, without loss of generality, we suppose that the weight w_{i_u} is increasing on u , i.e., $0 < w_{i_1} \leq w_{i_2} \leq \dots \leq w_{i_n} < t$, satisfying $\sum_{u=1}^n w_{i_u} = t-1$.

According to the definition of secrecy, we choose any two distinct secrets s_0 and s_1 , let $Z_{i_u}^{(s_0)}$ and $Z_{i_u}^{(s_1)}$ be the corresponding shares of P_{i_u} . We need to prove that for any n vectors $\{z_{i_u}\}_{u=1}^n$, where $z_{i_u} = [z_{i_u,0}, \dots, z_{i_u,w_{i_u}-1}]$ with each $z_{i_u,j} \in \mathbb{F}_2[x]/x^{(t-j-1)(\ell_{i_u}-1)+\ell}$ for $0 \leq j \leq w_{i_u}-1$, the following two probabilities are equal, i.e.,

$$P(\{Z_{i_u}^{(s_0)} = z_{i_u}\}_{u=1}^n) = P(\{Z_{i_u}^{(s_1)} = z_{i_u}\}_{u=1}^n). \quad (45)$$

We first analyze the value of $P(\{Z_{i_u}^{(s_0)} = z_{i_u}\}_{u=1}^n)$. For a given secret s_0 , n participants $\{P_{i_u}\}_{u=1}^n$, the corresponding weight $\{w_{i_u}\}_{u=1}^n$ and given shares $\{z_{i_u}\}_{u=1}^n$, we construct the following congruence system of $t-1$ linear equations

$$\begin{cases} z_{i_1,0} = \sum_{m=0}^{t-2} r_{0,m} y_{i_1}^m + s_0 y_{i_1}^{t-1} \pmod{x^{L_{i_1,0}}}, \\ \dots \\ z_{i_1,w_{i_1}-1} = \sum_{m=0}^{t-2} \binom{m}{w_{i_1}-1} r_{0,m} y_{i_1}^{m-w_{i_1}+1} + \binom{t-1}{w_{i_1}-1} s_0 y_{i_1}^{t-w_{i_1}} \pmod{x^{L_{i_1,w_{i_1}-1}}}, \\ \vdots \\ z_{i_n,0} = \sum_{m=0}^{t-2} r_{0,m} y_{i_n}^m + s_0 y_{i_n}^{t-1} \pmod{x^{L_{i_n,0}}}, \\ \dots \\ z_{i_n,w_{i_n}-1} = \sum_{m=0}^{t-2} \binom{m}{w_{i_n}-1} r_{0,m} y_{i_n}^{m-w_{i_n}+1} + \binom{t-1}{w_{i_n}-1} s_0 y_{i_n}^{t-w_{i_n}} \pmod{x^{L_{i_n,w_{i_n}-1}}}, \end{cases} \quad (46)$$

where $L_{i_u,j} = (t-1-j)(\ell_{i_u}-1) + \ell$ for $0 \leq j \leq w_{i_u}-1$ and $1 \leq u \leq n$. Though $r_{0,m} \in \mathbb{F}_2[[x]]$, only the part with degree less than $L_{i_n,0} = (t-1)(\ell_{i_n}-1) + \ell$ participates in the above calculation. Hence, we only need to consider the part of $r_{0,m}$ modulo $x^{L_{i_n,0}}$. Therefore, the whole space of the solution vector $(r_{0,0}, r_{0,1}, \dots, r_{0,t-2})$ can be regarded as $\{\mathbb{F}_2[x]/x^{L_{i_n,0}}\}^{t-1}$. Thus, the value of $P(\{Z_{i_u}^{(s_0)} = z_{i_u}\}_{u=1}^n)$ is equal to the ratio of the number of solutions $(r_{0,0}, r_{0,1}, \dots, r_{0,t-2})$ of (46) in the whole space $\{\mathbb{F}_2[x]/x^{L_{i_n,0}}\}^{t-1}$.

Similarly, the value of $P(\{Z_{i_u}^{(s_1)} = z_{i_u}\}_{u=1}^n)$ is equal to the ratio of the number of solutions $(r_{1,0}, r_{1,1}, \dots, r_{1,t-2})$ of (47) in the whole space $\{\mathbb{F}_2[x]/x^{L_{i_n,0}}\}^{t-1}$.

$$\left\{ \begin{array}{l} z_{i_1,0} = \sum_{m=0}^{t-2} r_{1,m} y_{i_1}^m + s_1 y_{i_1}^{t-1} \pmod{x^{L_{i_1,0}}}, \\ \qquad \qquad \qquad \dots \\ z_{i_1,w_{i_1}-1} = \sum_{m=0}^{t-2} \binom{m}{w_{i_1}-1} r_{1,m} y_{i_1}^{m-w_{i_1}+1} + \binom{t-1}{w_{i_1}-1} s_1 y_{i_1}^{t-w_{i_1}} \pmod{x^{L_{i_1,w_{i_1}-1}}}, \\ \qquad \qquad \qquad \vdots \\ z_{i_n,0} = \sum_{m=0}^{t-2} r_{1,m} y_{i_n}^m + s_1 y_{i_n}^{t-1} \pmod{x^{L_{i_n,0}}}, \\ \qquad \qquad \qquad \dots \\ z_{i_n,w_{i_n}-1} = \sum_{m=0}^{t-2} \binom{m}{w_{i_n}-1} r_{1,m} y_{i_n}^{m-w_{i_n}+1} + \binom{t-1}{w_{i_n}-1} s_1 y_{i_n}^{t-w_{i_n}} \pmod{x^{L_{i_n,w_{i_n}-1}}}. \end{array} \right. \quad (47)$$

Therefore, we can prove that (46) and (47) have the same number of solutions, to show that (45) holds.

Next, our goal is to prove that (46) and (47) have the same number of solutions. We prove the conclusion by contradiction. Without loss of generality, we assume that (46) has N_0 solutions and (47) has N_1 solutions with $N_0 > N_1$. Let $\mathbb{R}_0$ and $\mathbb{R}_1$ respectively be the solution sets of (46) and (47). Subtracting (47) from (46), then we have

$$\left\{ \begin{array}{l} (s_1 - s_0) y_{i_1}^{t-1} = \sum_{m=0}^{t-2} (r_{0,m} - r_{1,m}) y_{i_1}^m \pmod{x^{L_{i_1,0}}}, \\ \binom{t-1}{1} (s_1 - s_0) y_{i_1}^{t-2} = \sum_{m=0}^{t-2} \binom{m}{1} (r_{0,m} - r_{1,m}) y_{i_1}^{m-1} \pmod{x^{L_{i_1,1}}}, \\ \qquad \qquad \qquad \dots \\ \binom{t-1}{w_{i_1}-1} (s_1 - s_0) y_{i_1}^{t-w_{i_1}} = \sum_{m=0}^{t-2} \binom{m}{w_{i_1}-1} (r_{0,m} - r_{1,m}) y_{i_1}^{m-w_{i_1}+1} \pmod{x^{L_{i_1,w_{i_1}-1}}}, \\ \qquad \qquad \qquad \vdots \\ (s_1 - s_0) y_{i_n}^{t-1} = \sum_{m=0}^{t-2} (r_{0,m} - r_{1,m}) y_{i_n}^m \pmod{x^{L_{i_n,0}}}, \\ \binom{t-1}{1} (s_1 - s_0) y_{i_n}^{t-2} = \sum_{m=0}^{t-2} \binom{m}{1} (r_{0,m} - r_{1,m}) y_{i_n}^{m-1} \pmod{x^{L_{i_n,1}}}, \\ \qquad \qquad \qquad \dots \\ \binom{t-1}{w_{i_n}-1} (s_1 - s_0) y_{i_n}^{t-w_{i_n}} = \sum_{m=0}^{t-2} \binom{m}{w_{i_n}-1} (r_{0,m} - r_{1,m}) y_{i_n}^{m-w_{i_n}+1} \pmod{x^{L_{i_n,w_{i_n}-1}}}. \end{array} \right. \quad (48)$$

Denote $\Delta_s = s_1 - s_0 \in \mathbb{F}_2[x]/x^\ell$ and $\Delta_{r_m} = r_{0,m} - r_{1,m} \in \mathbb{F}_2[x]/x^{L_{i_n,0}}$ for $0 \leq m \leq t-2$. Substituting the above results into (48), we obtain

$$\left\{ \begin{array}{l} \Delta_s y_{i_1}^{t-1} = \sum_{m=0}^{t-2} \Delta_{r_m} y_{i_1}^m \pmod{x^{L_{i_1,0}}}, \\ \binom{t-1}{1} \Delta_s y_{i_1}^{t-2} = \sum_{m=0}^{t-2} \binom{m}{1} \Delta_{r_m} y_{i_1}^{m-1} \pmod{x^{L_{i_1,1}}}, \\ \dots \\ \binom{t-1}{w_{i_1}-1} \Delta_s y_{i_1}^{t-w_{i_1}} = \sum_{m=0}^{t-2} \binom{m}{w_{i_1}-1} \Delta_{r_m} y_{i_1}^{m-w_{i_1}+1} \pmod{x^{L_{i_1,w_{i_1}-1}}}, \\ \vdots \\ \Delta_s y_{i_n}^{t-1} = \sum_{m=0}^{t-2} \Delta_{r_m} y_{i_n}^m \pmod{x^{L_{i_n,0}}}, \\ \binom{t-1}{1} \Delta_s y_{i_n}^{t-2} = \sum_{m=0}^{t-2} \binom{m}{1} \Delta_{r_m} y_{i_n}^{m-1} \pmod{x^{L_{i_n,1}}}, \\ \dots \\ \binom{t-1}{w_{i_n}-1} \Delta_s y_{i_n}^{t-w_{i_n}} = \sum_{m=0}^{t-2} \binom{m}{w_{i_n}-1} \Delta_{r_m} y_{i_n}^{m-w_{i_n}+1} \pmod{x^{L_{i_n,w_{i_n}-1}}}. \end{array} \right. \quad (49)$$

Analyzing the above equation, we conclude that it has solutions. Call that a fact, for given n different values $\{y_{i_u}\}_{u=1}^n$ and n positive integers $\{w_{i_u}\}_{u=1}^n$ with $\sum_{u=1}^n w_{i_u} = t-1$, consider the monic polynomial

$$f_1(y) = \prod_{u=1}^n (y - y_{i_u})^{w_{i_u}}.$$

Thus, y_{i_u} is a root of multiplicity w_{i_u} of the above equation for $1 \leq u \leq n$. On the other hand, $f_1(y)$ can also be expressed as

$$f_1(y) = y^{t-1} + \sum_{m=0}^{t-2} a_m y^m.$$

By the formulas of the relation between roots and coefficients, each coefficient a_m for $0 \leq m \leq t-2$ is uniquely determined as

$$a_m = \sum_{\substack{k_1+k_2+\dots+k_n=t-1-m, \\ 0 \leq k_u \leq w_{i_u}}} \prod_{u=1}^n \binom{w_{i_u}}{k_u} y_{i_u}^{k_u}.$$

Thus, we can construct a solution $\Delta_r = (\Delta_{r_0}, \Delta_{r_1}, \dots, \Delta_{r_{t-2}})$ in (49), i.e.,

$$\begin{aligned} \Delta_{r_m} &= \Delta_s \cdot a_m \\ &= (s_1 - s_0) \sum_{\substack{k_1+k_2+\dots+k_n=t-1-m, \\ 0 \leq k_u \leq w_{i_u}}} \prod_{u=1}^n \binom{w_{i_u}}{k_u} y_{i_u}^{k_u} \end{aligned}$$

for $0 \leq m \leq t - 2$.

Under the assumptions, (46) admits solutions. As $\mathbb{R}_0$ is the solution set of (46), we choose one of solutions in $\mathbb{R}_0$ and denote it as r_0^1 , then $r_0^1 + \Delta_{r_m} = (r_{0,0} + \Delta_{r_0}, \dots, r_{0,t-2} + \Delta_{r_{t-2}})$ is the solution of (47). When r_0^1 is taken across the whole solution set $\mathbb{R}_0$, (47) has at least N_0 different solutions, which contradicts that (47) has N_1 solutions. Therefore, (46) and (47) have the same number of solutions, then (45) holds. Thus, the proof of security is completed.

4.3 Share Size

We now analyze the share size of the proposed t -threshold scheme. For the m -th participant P_m with the corresponding weight w_m satisfying $1 \leq w_m \leq t - 1$, from (29) and (31), the corresponding share $Z_m^{(s)}$ is

$$[Z_{m,0}^{(s)}, Z_{m,1}^{(s)}, \dots, Z_{m,w_m-1}^{(s)}],$$

where $Z_{m,j}^{(s)}$ with $j \in \{0, 1, \dots, w_m - 1\}$ can be regarded as a polynomial of x in $\mathbb{F}_2$ with the degree less than $(t - j - 1)(\ell_m - 1) + \ell$, where ℓ_m is the length of the binary prefix code for the positive integer m . Then, we have

$$B(Z_m^{(s)}) = \sum_{j=0}^{w_m-1} ((t-j-1)(\ell_m-1)+\ell) = w_m(t-1-\frac{w_m-1}{2})(\ell_m-1)+w_m\ell. \quad (50)$$

By analyzing the above result, if we directly use the conventional scheme proposed in [4] to distribute w_m shares to participant P_m , since the size of each share is $(t - 1)(\ell_m - 1) + \ell$, then we have

$$B(Z_m^{(s)}) = w_m(t - 1)(\ell_m - 1) + w_m\ell. \quad (51)$$

Comparing (50) and (51), our proposed scheme can save $\frac{(w_m-1)w_m}{2}(\ell_m - 1)$ bits than the conventional scheme proposed in [4] for $1 \leq w_m \leq t - 1$. Thus, our proposed scheme achieves a significantly smaller share size.

4.4 Discussion

It is worth noting that when the weights of all participants are set to 1, the weighted evolving t -threshold secret sharing scheme over polynomial quotient rings proposed in our work precisely degenerates into the evolving t -threshold secret sharing scheme by Cheng et al. [4] from ASIACRYPT 2025. In other words, the scheme in [4] can be viewed as a special case of our scheme when all participants have equal weight 1.

This observation confirms the correctness and security of our scheme, and also highlights the key difference between the two models. The scheme of Cheng et al. [4] only applies to the setting where every participant has weight 1. In contrast, our weighted evolving model naturally supports participants with different weights. Therefore, our scheme not only retains the ability to allow participants to join dynamically, as in Cheng et al.'s work [4], but also extends applicability to real-world scenarios that require a weighted access structure.

5 Conclusion and Discussion

In this paper, we introduce the concept of weighted evolving threshold secret sharing to address practical scenarios in which the total number of participants is unknown, and participants have different levels of authority over the secret information. As a concrete instantiation, we propose a construction for the 3-threshold case, and subsequently extend it to the more general t -threshold case. Moreover, we prove the corresponding correctness and secrecy, and analyze the share size. The result shows that for the m -th participant with the weight w_m satisfying $1 \leq w_m \leq t - 1$, the size of the corresponding share is $w_m(t - 1 - \frac{w_m - 1}{2})(\ell_m - 1) + w_m \ell$ bits, where ℓ_m denotes the length of a binary prefix code of encoding integer m .

For comparison, a baseline scheme that allocates w_m independent full evolving shares to this participant would require $w_m(t - 1)(\ell_m - 1) + w_m \ell$ bits. Our proposed scheme saves $\frac{(w_m - 1)w_m}{2}(\ell_m - 1)$ bits, thereby achieving a smaller share size. More importantly, the scheme proposed by Cheng et al. [4] at ASIACRYPT 2025 can be regarded as a special case of our scheme when all participants have equal weights of 1. Thus, our scheme can serve as a natural extension of Cheng et al.'s work.

Our analysis reveals that the share size for participant P_m is at least $w_m(t - 1 - \frac{w_m - 1}{2})(\ell_m - 1) + w_m \ell$ bits; we are uncertain whether it is optimal. If so, please prove. If not, we find the share size depends on both the participant's weight w_m and the threshold value t . This raises a critical question: is it possible to design more efficient weighted evolving t -threshold secret sharing schemes that mitigate this dependency w_m and t , thereby achieving significantly reduced share sizes?

We also note that the current work assumes that both weights and threshold are fixed when a participant joins. A natural direction for future work is to study more flexible settings where participants' weights or the threshold may change over time. In particular, allowing both weights and threshold to be dynamic is an interesting open problem. This would make the design and security proof much more challenging, and we leave it for future investigation.

Acknowledgements. This work was supported by the National Natural Science Foundation of China under Grant No. 62602015. We are deeply grateful to Prof. Sian-Jheng Lin and Prof. Yung-Hsiang S. Han for their valuable guidance and for their careful proofreading of the manuscript. We also thank Dr. Guang Hu and Dr. Hongru Cao for their helpful discussions and constructive suggestions throughout this work. Finally, we appreciate the anonymous reviewers for their insightful comments.

References

1. Shamir, A.: How to share a secret. *Communications of the ACM* **22**(11), 612–613 (1979). <https://doi.org/10.1145/359168.359176>

2. Blakley, G.R.: Safeguarding cryptographic keys. 1979 International Workshop on Managing Requirements Knowledge (MARK), 313–313 (1979). <https://doi.org/10.1109/MARK.1979.8817296>
3. Komargodski, I., Naor, M., Yogev, E.: How to share a secret, infinitely. *IEEE Transactions on Information Theory* **64**(6), 4179–4190 (2017). <https://doi.org/10.1109/TIT.2017.2779121>
4. Cheng, Q., Cao, H., Lin, S., Yu, N., Han, Y., Xie, X.: A construction of evolving k -threshold secret sharing scheme over a polynomial ring. In: Hanaoka, G., Yang, B.Y. (eds) *Advances in Cryptology -ASIACRYPT 2025*. ASIACRYPT 2025, LNCS, vol. 16252, pp. 3–33. Springer, Singapore. (2025). https://doi.org/10.1007/978-981-95-5125-5_1
5. Komargodski, I., Paskin-Cherniavsky, A.: Evolving secret sharing: dynamic thresholds and robustness. In: Kalai, Y., Reyzin, L. (eds) *Theory of Cryptography*. TCC 2017, LNCS, vol. 10678, pp.379–393. Springer, Cham. (2017). https://doi.org/10.1007/978-3-319-70503-3_12
6. Beimel, A., Othman, H.: Evolving ramp secret-sharing schemes. In: Catalano, D., De Prisco, R. (eds) *Security and Cryptography for Networks Conference*. SCN 2018, LNCS, vol. 11035, pp.313–332. Springer, Cham. (2018). https://doi.org/10.1007/978-3-319-98113-0_17
7. Desmedt, Y., Dutta, S., Morozov, K.: Evolving perfect hash families: a combinatorial viewpoint of evolving secret sharing. In: Mu, Y., Deng, R., Huang, X. (eds) *Cryptography and Network Security*. CANS 2019, LNCS, vol. 11829, pp.291–307. Springer, Cham. (2019). https://doi.org/10.1007/978-3-030-31578-8_16
8. Beimel, A., Othman, H.: Evolving ramp secret sharing with a small gap. In: Canteaut, A., Ishai, Y. (eds) *Advances in Cryptology -EUROCRYPT 2020*. EUROCRYPT 2020, LNCS, vol. 12105, pp.529–555. Springer, Cham. (2020). https://doi.org/10.1007/978-3-030-45721-1_19
9. Alon, B., Beimel, A., Ben David, T., Omri, E., Paskin-Cherniavsky, A.: New upper bounds for evolving secret sharing via infinite branching programs. In: Boyle, E., Mahmoody, M. (eds) *Theory of Cryptography*. TCC 2024, LNCS, vol. 15367, pp.548–580. Springer, Cham. (2024). https://doi.org/10.1007/978-3-031-78023-3_18
10. Zhang, Y., Kong, J., En, K., Chen, Y., Yang, Y., Qin, X.: A dealer-assisted weighted threshold pointcheval–sanders signature scheme from crt-based weighted ramp secret sharing. *Cybersecurity* **9**(192) (2026). <https://doi.org/10.1186/s42400-026-00627-x>
11. Francati, D., Giammusso, S., Venturi, D.: Beyond the linear barrier: secret sharing for evolving (weighted) threshold access structures with poly-logarithmic share size. *Cryptography ePrint Archive*, Paper 2026/267 (2026). <https://eprint.iacr.org/2026/267>
12. Mignotte, M.: How to share a secret. In: Beth, T. (eds) *EUROCRYPT 1982*, LNCS, vol. 149, pp. 371–375. Springer, Heidelberg. (1982). https://doi.org/10.1007/3-540-39466-4_27
13. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. *IEEE Transactions on Information Theory* **29**(2), 208–210 (1983). <https://doi.org/10.1109/TIT.1983.1056651>
14. Ning, Y., Miao, F., Huang, W., Meng, K., Xiong, Y., Wang, X.: Constructing ideal secret sharing schemes based on Chinese remainder theorem. In: Peyrin, T., Galbraith, S. (eds) *ASIACRYPT 2018*, LNCS, vol. 11274, pp. 310–331. Springer, Cham. (2018). https://doi.org/10.1007/978-3-030-03332-3_12

15. Cramer, R., Fehr, S.: Optimal black-box secret sharing over arbitrary abelian groups. In: Moti, Y. (eds) CRYPTO 2002, LNCS, vol. 2442, pp. 272–287. Springer, Heidelberg. (2002). https://doi.org/10.1007/3-540-45708-9_18
16. Cao, H., Lin, S., Zhang, W., Han, Y.: On the security of secret sharing over a ring and the fast implementation. *IEEE Signal Processing Letters* **26**(5), 705–709 (2019). <https://doi.org/10.1109/LSP.2019.2907010>
17. Ligeti, P., Sziklai, P., Takáts, M.: Generalized threshold secret sharing and finite geometry. *Designs, Codes and Cryptography* **89**(9), 2067–2078 (2021). <https://doi.org/10.1007/s10623-021-00900-9>
18. Gyarmati, M., Ligeti, P., Sziklai, P., Takáts, M.: Conjunctive hierarchical secret sharing by finite geometry. *Designs, Codes and Cryptography* **93**(2), 423–428 (2025). <https://doi.org/10.1007/s10623-024-01496-6>
19. Chen, B., Lu, W., Huang, J., Weng, J., Zhou, Y.: Secret sharing based reversible data hiding in encrypted images with multiple data-hiders. *IEEE Transactions on Dependable and Secure Computing* **19**(2), 978–991 (2020). <https://doi.org/10.1109/TDSC.2020.3011923>
20. Chen, Z., Tian, Y., Peng, C.: An incentive-compatible rational secret sharing scheme using blockchain and smart contract. *Science China Information Sciences* **64**, 1–21 (2021). <https://doi.org/10.1007/s11432-019-2858-8>
21. Lai, J., Susilo, W., Deng, R.H., Guo, F.: Sdss: Sequential data sharing system in iot. *IEEE Transactions on Information Forensics and Security* **19**, 2288–2299 (2024). <https://doi.org/10.1109/TIFS.2023.3348229>
22. Yang, C.-N., Li, P., Cheng, H.-H., Kuo, H.-C., Lu, M.-C., Xiong, L.: A security model of multihospital FHIR database authorization based on secret sharing and blockchain. *IEEE Internet of Things Journal* **11**(6), 10325–10335 (2024). <https://doi.org/10.1109/JIOT.2023.3328989>
23. Lu, Y., Yu, Z., Suri, N.: Privacy-preserving decentralized federated learning over time-varying communication graph. *ACM Transactions on Privacy and Security* **26**(3), 1–39 (2023). <https://doi.org/10.1145/3591354>
24. Elias, P.: Universal codeword sets and representations of the integers. *IEEE Transactions on Information Theory* **21**(2), 194–203 (1975). <https://doi.org/10.1109/TIT.1975.1055349>
25. Okamura, R., Koga, H.: New Constructions of an Evolving 2-Threshold Scheme Based on Binary or D-ary Prefix Codes. 2020 International Symposium on Information Theory and Its Applications, 432–436 (2020).
26. Yan, W., Lin, S.-J., Han, Y.S.: A new metric and the construction for evolving 2- threshold secret sharing schemes based on prefix coding of integers. *IEEE Transactions on Communications* **71**(5), 2906–2915 (2023). <https://doi.org/10.1109/TCOMM.2023.3253720>
27. D’Arco, P., Prisco, R. D., Santis, A. D.: Constructions and lower bounds for evolving 2-threshold secret sharing schemes. *IEEE Transactions on Communications* (2024). <https://doi.org/10.1109/TCOMM.2024.3493802>
28. Xing, C., Yuan, C.: Evolving secret sharing schemes based on polynomial evaluations and algebraic geometry codes. *IEEE Transactions on Information Theory* **70**(5), 3718–3728 (2024). <https://doi.org/10.1109/TIT.2024.3379278>
29. D’Arco, P., De Prisco, R., De Santis, A.: Secret sharing schemes for infinite sets of participants: A new design technique. *Theoretical Computer Science* **859**, 149–161 (2021). <https://doi.org/10.1016/j.tcs.2021.01.019>
30. Harn, L., Miao, F.: Weighted secret sharing based on the Chinese remainder theorem. *International Journal of Network Security* **16**(6), 420–425 (2014). <https://doi.org/10346205>

31. Dragan, C.C., Tiplea, F.L.: Distributive weighted threshold secret sharing schemes. *Information Sciences* **339**(20), 85–97 (2016). <https://doi.org/10.1016/j.ins.2016.01.019>
32. Benhamouda, F., Halevi, S., Stambler, L.: Weighted secret sharing from wiretap channels. *Cryptology ePrint Archive*, Paper 2022/1578, (2022). <https://eprint.iacr.org/2022/1578>
33. Garg, S., Jain, A., Mukherjee, P., Sinha, R., Wang, M., Zhang, Y.: Cryptography with weights: MPC, encryption and signatures. In: Handschuh, H., Lysyanskaya, A. (eds) *Advances in Cryptology -CRYPTO 2023*. CRYPTO 2023, LNCS, vol. 14081, pp. 295–327. Springer, Cham. (2023). https://doi.org/10.1007/978-3-031-38557-5_10
34. Farrás, Ó., Guiot, M.: Reducing the share size of weighted threshold secret sharing schemes via Chow parameters approximation. In: Boyle, E., Mahmoody, M. (eds) *Theory of Cryptography. TCC 2024*, LNCS, vol. 15367, pp. 517–547. Springer, Singapore. (2025). https://doi.org/10.1007/978-3-031-78023-3_17

Appendix

Proof of Theorem 1. Theorem 1 is established based on the polynomial $f(y)$ over the polynomial ring $\mathbb{F}_2[x]$, aiming to prove an inequality $p_x(\det(\mathbf{V}_y)) - p_x(\det(\mathbf{G}_{t,u,j})) \leq \eta + (w_{i_u} - j - 1)\mu$. If one attempts to derive this directly within the structure of the ring $\mathbb{F}_2[x]$, a fundamental algebraic limitation arises. Although the polynomial ring has additive and multiplicative structures, it lacks closure under division, so nonzero elements need not be invertible, which prevents freely applying algebraic transformations as in a field, such as extracting complex factors or eliminating variables. To overcome this structural limitation, we embed the research object $f(y)$ from the restricted polynomial ring $\mathbb{F}_2[x]$ into the fraction field $\mathbb{F}_2(x)$ as $\mathbb{F}_2[x] \subset \mathbb{F}_2(x)$. This transformation is crucial because the fraction field allows the division operation and endows the coefficient field with complete algebraic properties. This enables us to derive some auxiliary results in the fraction field $\mathbb{F}_2(x)$ that will be used to prove the theorem. Therefore, before presenting the proof, we emphasize several lemmas that provide useful results for it.

Next, we introduce some notation used in this part. Consider the given polynomial $f(y) = \sum_{m=0}^{t-2} r_m y^m + s y^{t-1}$ denoted in (27), where these coefficients r_m and s are randomly chosen from $\mathbb{F}_2[x]$ for $0 \leq m \leq t-2$. As $\mathbb{F}_2[x] \subset \mathbb{F}_2(x)$, then $f(y)$ can be viewed as a polynomial over $\mathbb{F}_2(x)$. To not cause misunderstanding, we denote this polynomial $f(y)$ over the field $\mathbb{F}_2(x)$ as

$$g(y) = \sum_{m=0}^{t-1} r_m y^m, \quad r_m \in \mathbb{F}_2(x), \quad (52)$$

where $r_{t-1} = s$.

Recall the definitions associated with the prefix codes. Given a set of prefix codes for integers, c_{i_u} denotes the codeword of the positive integer i_u , ℓ_{i_u} represents the bit length of c_{i_u} , and $y_{i_u} \in \mathbb{F}_2[x] \subset \mathbb{F}_2(x)$ denotes the polynomial

form of c_{i_u} . Given a set of n polynomials $\{y_{i_u}\}_{u=1}^n$ and a corresponding set of n positive integers $\{w_{i_u}\}_{u=1}^n$ satisfying $\sum_{u=1}^n w_{i_u} = t$, $1 \leq w_{i_u} \leq t-1$, and w_{i_u} is increasing on u , we get t values denoted by $\{\{b_{u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$, where each value is calculated as

$$b_{u,j} = D^j g(y_{i_u}) = \sum_{m=0}^{t-1} \binom{m}{j} r_m y_{i_u}^{m-j}. \quad (53)$$

Here $D^j g(y)$ denotes the j -th order Hasse derivative of the polynomial $g(y)$ with respect to y , and $D^j g(y_{i_u})$ represents the evaluation of this derivative at $y = y_{i_u}$.

Therefore, for given the t pairs $\{\{(y_{i_u}, b_{u,j})\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$, we can construct a system of t linear equations in $\mathbb{F}_2(x)$ as follows

$$\mathbf{V} \cdot \mathbf{r} = \mathbf{b}. \quad (54)$$

In (54), $\mathbf{V}$ is a $t \times t$ confluent Vandermonde matrix in the field $\mathbb{F}_2(x)$. It is composed of n blocks of rows, where the u -th block V_{i_u} is uniquely determined by the polynomial y_{i_u} and its multiplicity w_{i_u} . The matrix is structured as

$$V_{i_u} = \begin{pmatrix} 1 & y_{i_u} & y_{i_u}^2 & \cdots & y_{i_u}^{t-1} \\ 0 & 1 & \binom{2}{1} y_{i_u} & \cdots & \binom{t-1}{1} y_{i_u}^{t-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \binom{t-1}{w_{i_u}-1} y_{i_u}^{t-w_{i_u}} \end{pmatrix}.$$

Therefore, the determinant of this confluent Vandermonde matrix $\mathbf{V}$ is given by

$$\det(\mathbf{V}) = \prod_{1 \leq u < v \leq n} (y_{i_v} - y_{i_u})^{w_{i_u} w_{i_v}}. \quad (55)$$

Here, $\mathbf{r} = (r_0, r_1, \dots, r_{t-2}, r_{t-1})^T$ denotes the column vector of unknown coefficients, and $\mathbf{b}$ is the column vector containing t values $\{\{b_{u,j}\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$.

Next, we present two different methods to construct the polynomial $g(y)$ when receiving these t pairs $\{\{(y_{i_u}, b_{u,j})\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$.

Lemma 3. For $1 \leq m \leq t$, let $\mathbf{A}_m$ be the new matrix obtained by replacing the m -th column of matrix $\mathbf{V}$ with the vector $\mathbf{b}$. For $1 \leq u \leq n$, $0 \leq j \leq w_{i_u} - 1$ and $\sum_{u=1}^n w_{i_u} = t$, let $\mathbf{A}_{m,u,j}$ denote the submatrix of $\mathbf{A}_m$ obtained by deleting the row and the column containing the element $b_{u,j}$ of the m -th column. Then, the polynomial $g(y)$ can be expressed as

$$g(y) = \frac{1}{\det(\mathbf{V})} \left(\sum_{u,j} \det(\mathbf{A}_{1,u,j}) b_{u,j} y^0 + \cdots + \sum_{u,j} \det(\mathbf{A}_{t,u,j}) b_{u,j} y^{t-1} \right) \quad (56)$$

Proof. In $\mathbb{F}_2(x)$, let $u, v \in \{1, 2, \dots, n\}$ with $u \neq v$, then $y_{i_u} - y_{i_v} \neq 0$, we have $\det(\mathbf{V}) \neq 0$. Thus, the linear system of equations $\mathbf{V} \cdot \mathbf{r} = \mathbf{b}$ has a unique solution $\mathbf{r} = (r_0, r_1, \dots, r_{t-1})^T$. By Cramer's rule, each coefficient r_{m-1} for $1 \leq m \leq t$ is solved as

$$r_{m-1} = \frac{\det(\mathbf{A}_m)}{\det(\mathbf{V})}.$$

As $\mathbf{A}_m$ is the matrix obtained by replacing the m -th column of matrix $\mathbf{V}$ with the vector $\mathbf{b}$, $\det(\mathbf{A}_m)$ can be calculated by expanding along the m -th column, where the entries are $b_{u,j}$ of $\mathbf{b}$. Then, we have

$$\det(\mathbf{A}_m) = \sum_{u,j} \det(\mathbf{A}_{m,u,j}) b_{u,j}.$$

Therefore, we derive

$$\begin{aligned} g(y) &= \sum_{m=1}^t r_{m-1} y^{m-1} = \sum_{m=1}^t \frac{\det(\mathbf{A}_m)}{\det(\mathbf{V})} y^{m-1} = \sum_{m=1}^t \frac{\sum_{u,j} \det(\mathbf{A}_{m,u,j}) b_{u,j}}{\det(\mathbf{V})} y^{m-1} \\ &= \frac{1}{\det(\mathbf{V})} \left(\sum_{u,j} \det(\mathbf{A}_{1,u,j}) b_{u,j} y^0 + \cdots + \sum_{u,j} \det(\mathbf{A}_{t,u,j}) b_{u,j} y^{t-1} \right). \end{aligned}$$

Lemma 4. For $1 \leq u, v \leq n$, $0 \leq j \leq w_{i_u} - 1$ and $\sum_{u=1}^n w_{i_u} = t$, let $B_{u,j}(y)$ be a polynomial of degree at most $t-1$ in $\mathbb{F}_2(x)[y]$ satisfying the following conditions

$$D^k B_{u,j}(y_{i_v}) = \begin{cases} 0, & \text{if } v \neq u, \quad 0 \leq k \leq w_{i_v} - 1, \\ 0, & \text{if } v = u, \quad 0 \leq k \leq w_{i_v} - 1, k \neq j, \\ 1, & \text{if } v = u, \quad k = j. \end{cases} \quad (57)$$

Then, the polynomial $g(y)$ can be reconstructed as

$$g(y) = \sum_{u,j} B_{u,j}(y) \cdot b_{u,j}, \quad (58)$$

where $B_{u,j}(y)$ is called as the basis polynomial of $g(y)$.

Proof. Let us define the polynomial $H(y)$ as the right-hand side of (58), i.e.,

$$H(y) = \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} B_{u,j}(y) \cdot b_{u,j}.$$

We evaluate the k -th order Hasse derivative of $H(y)$ at an arbitrary point y_{i_v} for $0 \leq k \leq w_{i_v} - 1$ and $1 \leq v \leq n$. By the linearity of the Hasse derivative, we have

$$D^k H(y_{i_v}) = \sum_{u=1}^n \sum_{j=0}^{w_{i_u}-1} b_{u,j} \cdot D^k B_{u,j}(y_{i_v}).$$

According to the defining properties of $B_{u,j}(y)$ in (57), the term $D^k B_{u,j}(y_{i_v})$ is equal to 1 if and only if $v = u$ and $k = j$. For all other pairs (v, k) , the derivative evaluates to 0. Therefore, we have

$$D^j H(y_{i_u}) = b_{u,j} \cdot D^j B_{u,j}(y_{i_u}) = b_{u,j} \cdot 1 = b_{u,j}.$$

This shows that $H(y)$ satisfies the same set of t interpolations as $g(y)$ in (53), i.e., $D^j H(y_{i_u}) = D^j g(y_{i_u}) = b_{u,j}$ for all valid u and j . Since both $H(y)$ and $g(y)$ are polynomials of degree at most $t-1$, then the Hermite interpolation of $g(y)$ over the field $\mathbb{F}_2(x)$ is unique; it follows that $H(y) = g(y)$. Thus, (58) holds.

Lemma 5. *Under the assumptions of Lemma 4, there exist following two crucial results.*

(1) $B_{u,j}(y)$ can be uniquely expressed as

$$B_{u,j}(y) = (y - y_{i_u})^j \cdot P_u(y) \cdot Q_u(y), \quad (59)$$

where $P_u(y) = \prod_{v \neq u} (y - y_{i_v})^{w_{i_v}}$ and $Q_u(y) = \sum_{e=0}^{w_{i_u}-j-1} a_e (y - y_{i_u})^e$. Then the coefficient a_e is determined recursively by

$$a_e = \begin{cases} \frac{1}{P_u(y_{i_u})}, & \text{if } e = 0, \\ \frac{1}{P_u(y_{i_u})} \sum_{m=0}^{e-1} a_m \cdot D^{e-m} P_u(y_{i_u}), & \text{if } 1 \leq e \leq w_{i_u} - j - 1. \end{cases} \quad (60)$$

(2) For any $h(x) \in \mathbb{F}_2(x)$, let $p_x(h(x))$ denote as the maximal extractable power of x in $h(x)$. Let $\mu = \max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\}$ and $\eta = p_x(P_u(y_{i_u}))$. Then we have

$$p_x(a_e) \geq -\eta - e \cdot \mu, \quad \text{for } 0 \leq e \leq w_{i_u} - j - 1. \quad (61)$$

Proof. (1). We first verify that the proposed form $B_{u,j}(y) = (y - y_{i_u})^j P_u(y) Q_u(y)$ satisfies the conditions (57) required by Lemma 4.

Since $P_u(y) = \prod_{v \neq u} (y - y_{i_v})^{w_{i_v}}$ contains the factor $(y - y_{i_v})^{w_{i_v}}$ for every $v \neq u$, the polynomial $B_{u,j}(y)$ has a root of multiplicity at least w_{i_v} at each y_{i_v} . Consequently, by the linearity of the Hasse derivative, $D^k B_{u,j}(y_{i_v}) = 0$ holds for all $0 \leq k \leq w_{i_v} - 1$. Moreover, the factor $(y - y_{i_u})^j$ of $B_{u,j}(y)$ ensures that $D^k B_{u,j}(y_{i_u}) = 0$ for all $0 \leq k < j$.

Thus, the problem reduces to determining each coefficient a_e of $Q_u(y)$ such that the remaining higher-order derivative conditions at y_{i_u} satisfying

$$\begin{cases} D^j B_{u,j}(y_{i_u}) = 1, \\ D^k B_{u,j}(y_{i_u}) = 0, \quad \text{for } j < k \leq w_{i_u} - 1. \end{cases} \quad (62)$$

Since $D^k((y - y_{i_u})^j) = \binom{j}{k} (y - y_{i_u})^{j-k}$, then we have

$$\begin{cases} D^k((y - y_{i_u})^j) \Big|_{y=y_{i_u}} = 0, & \text{if } k \neq j, \\ D^k((y - y_{i_u})^j) \Big|_{y=y_{i_u}} = 1, & \text{if } k = j. \end{cases} \quad (63)$$

To calculate $D^k B_{u,j}(y_{i_u})$, we use the Leibniz rule of Hasse derivative and combine the results of (63), then get

$$\begin{aligned} D^k B_{u,j}(y_{i_u}) &= \sum_{a+b=k} D^a((y - y_{i_u})^j) \cdot D^b(P_u(y) Q_u(y)) \Big|_{y=y_{i_u}} \\ &= D^j((y - y_{i_u})^j) \cdot D^{k-j}(P_u(y) Q_u(y)) \Big|_{y=y_{i_u}} \\ &= 1 \cdot D^{k-j}(P_u(y) Q_u(y)) \Big|_{y=y_{i_u}}. \end{aligned} \quad (64)$$

According to the results of (62), $D^k B_{u,j}(y_{i_u}) = 1$ when $k = j$. From (64), we get

$$D^j B_{u,j}(y_{i_u}) = D^0(P_u(y)Q_u(y)) \Big|_{y=y_{i_u}} = P_u(y_{i_u}) \cdot a_0 = 1.$$

Thus

$$a_0 = \frac{1}{P_u(y_{i_u})}. \quad (65)$$

When $j < k \leq w_{i_u} - 1$, $D^k B_{u,j}(y_{i_u}) = 0$ in (62), let $k - j = e$, then $1 \leq e \leq w_{i_u} - j - 1$. From (64), we get

$$D^k B_{u,j}(y_{i_u}) = D^{j+e} B_{u,j}(y_{i_u}) = D^e(P_u(y)Q_u(y)) \Big|_{y=y_{i_u}} = 0. \quad (66)$$

Using the Leibniz rule of Hasse derivative to (66), we can further derive

$$\begin{aligned} D^e(P_u(y)Q_u(y)) \Big|_{y=y_{i_u}} &= \sum_{m=0}^e D^{e-m} P_u(y_{i_u}) \cdot D^m Q_u(y_{i_u}) \\ &= \sum_{m=0}^e a_m \cdot D^{e-m} P_u(y_{i_u}) \\ &= \sum_{m=0}^{e-1} a_m \cdot D^{e-m} P_u(y_{i_u}) + P_u(y_{i_u}) a_e = 0. \end{aligned}$$

Thus, we can solve a_e as

$$a_e = \frac{1}{P_u(y_{i_u})} \sum_{m=0}^{e-1} a_m \cdot D^{e-m} P_u(y_{i_u}). \quad (67)$$

By combining (65) and (67), it can observe that the value of each coefficient a_e is consistent with the result presented in (60).

(2). Recall that $P_u(y_{i_u}) = \prod_{v \neq u} (y_{i_u} - y_{i_v})^{w_{i_v}}$, $\mu = \max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\}$ and $\eta = p_x(P_u(y_{i_u}))$.

First, for any $k \geq 0$, we estimate the valuation $D^k P_u(y_{i_u})$ of the Hasse derivative of $P_u(y)$ at y_{i_u} as

$$\begin{aligned} D^k P_u(y_{i_u}) &= \sum_{\substack{\sum k_v = k \\ v \neq u}} \left(\prod_{v \neq u} D^{k_v} (y - y_{i_v})^{w_{i_v}} \right) \Big|_{y=y_{i_u}} \\ &= \sum_{\substack{\sum k_v = k \\ v \neq u}} \left(\prod_{v \neq u} \binom{w_{i_v}}{k_v} (y_{i_u} - y_{i_v})^{w_{i_v} - k_v} \right). \end{aligned} \quad (68)$$

Note that in $\mathbb{F}_2(x)$, binomial coefficient $\binom{w_{i_v}}{k_v}$ is element of $\mathbb{F}_2$. Thus, we have

$$p_x \left(\binom{w_{i_v}}{k_v} (y_{i_u} - y_{i_v})^{w_{i_v} - k_v} \right) = \begin{cases} +\infty, & \text{if } \binom{w_{i_v}}{k_v} = 0, \\ 0, & \text{if } \binom{w_{i_v}}{k_v} = 1, \quad w_{i_v} = k_v, \\ (w_{i_v} - k_v)p_x((y_{i_u} - y_{i_v})), & \text{if } \binom{w_{i_v}}{k_v} = 1, \quad w_{i_v} > k_v, \end{cases}$$

which implies that $p_x \left(\binom{w_{i_v}}{k_v} (y_{i_u} - y_{i_v})^{w_{i_v} - k_v} \right) \geq (w_{i_v} - k_v)p_x((y_{i_u} - y_{i_v}))$ always holds. Combining the property $p_x(A + B) \geq \min\{p_x(A), p_x(B)\}$, we obtain

$$\begin{aligned} p_x(D^k P_u(y_{i_u})) &= p_x \left(\sum_{\substack{k_v=k \\ v \neq u}} \left(\prod_{v \neq u} \binom{w_{i_v}}{k_v} (y_{i_u} - y_{i_v})^{w_{i_v} - k_v} \right) \right) \\ &\geq \min_{\{k_v\}} \left\{ p_x \left(\prod_{v \neq u} \binom{w_{i_v}}{k_v} (y_{i_u} - y_{i_v})^{w_{i_v} - k_v} \right) \right\} \\ &= \min_{\{k_v\}} \left\{ \sum_{v \neq u} p_x \left(\binom{w_{i_v}}{k_v} (y_{i_u} - y_{i_v})^{w_{i_v} - k_v} \right) \right\} \\ &\geq \min_{\{k_v\}} \left\{ \sum_{v \neq u} (w_{i_v} - k_v) p_x((y_{i_u} - y_{i_v})) \right\} \\ &\geq \sum_{v \neq u} w_{i_v} \cdot p_x((y_{i_u} - y_{i_v})) - \min_{\{k_v\}} \left\{ \sum_{v \neq u} k_v \cdot p_x((y_{i_u} - y_{i_v})) \right\} \\ &\stackrel{(c)}{\geq} \eta - k\mu, \end{aligned} \tag{69}$$

where (c) holds because $\sum_{v \neq u} w_{i_v} \cdot p_x((y_{i_u} - y_{i_v})) = \eta$, $\max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\} = \mu$

and $\min_{\{k_v\}} \left\{ \sum_{v \neq u} k_v \cdot p_x((y_{i_u} - y_{i_v})) \right\} \leq k \cdot \max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\} = k\mu$. Therefore, $p_x(D^k P_u(y_{i_u}))$ is bounded by $\eta - k\mu$.

Next, we prove by mathematical induction that for all integers e satisfying $0 \leq e \leq w_{i_u} - j - 1$, the inequality $p_x(a_e) \geq -\eta - e \cdot \mu$ holds.

When $e = 0$, we have

$$p_x(a_0) = p_x \left(\frac{1}{P_u(y_{i_u})} \right) = -p_x(P_u(y_{i_u})) = -\eta \geq -\eta - 0 \cdot \mu.$$

Assume that for some e with $1 \leq e \leq w_{i_u} - j - 1$, the inequality $p_x(a_m) \geq -\eta - m\mu$ holds for all $0 \leq m < e$. We need to prove $p_x(a_m) \geq -\eta - m\mu$ holds when $m = e$.

As $a_e = \frac{1}{P_u(y_{i_u})} \sum_{m=0}^{e-1} a_m \cdot D^{e-m} P_u(y_{i_u})$ by (60), using the result of (69) and the above assumption, then we have

$$\begin{aligned}
p_x(a_e) &= p_x \left(\frac{1}{P_u(y_{i_u})} \sum_{m=0}^{e-1} a_m \cdot D^{e-m} P_u(y_{i_u}) \right) \\
&= p_x \left(\sum_{m=0}^{e-1} a_m \cdot D^{e-m} P_u(y_{i_u}) \right) - p_x(P_u(y_{i_u})) \\
&\geq \min_{0 \leq m \leq e-1} \{p_x(a_m) + p_x(D^{e-m} P_u(y_{i_u}))\} - \eta \\
&\geq -\eta + \min_{0 \leq m \leq e-1} \{p_x(a_m) + \eta - (e-m)\mu\} \\
&\geq \min_{0 \leq m \leq e-1} \{p_x(a_m) - (e-m)\mu\} \\
&\geq \min_{0 \leq m \leq e-1} \{-\eta - m \cdot \mu - (e-m)\mu\} \\
&\geq -\eta - e \cdot \mu.
\end{aligned}$$

By the principle of mathematical induction, $p_x(a_e) \geq -\eta - e\mu$ is true for all $0 \leq e \leq w_{i_u} - j - 1$, which completes the proof of (2).

Now, we begin to prove Theorem 1. Recall that $\mathbb{F}_2(x)$ is a field of fractions and $g(y) \in \mathbb{F}_2(x)[y]$ is a polynomial of degree $t-1$ as $g(y) = \sum_{m=0}^{t-1} r_m y^m$, $r_m \in \mathbb{F}_2(x)$. Consider the corresponding system of linear equations $\mathbf{V} \cdot \mathbf{r} = \mathbf{b}$ mentioned in (54). $\mathbf{A}_m$ is the new matrix obtained by replacing the m -th column of matrix $\mathbf{V}$ with the vector $\mathbf{b}$ for $1 \leq m \leq t$. For $1 \leq u \leq n$, $0 \leq j \leq w_{i_u} - 1$ and $\sum_{u=1}^n w_{i_u} = t$, $\mathbf{A}_{m,u,j}$ denotes the submatrix of $\mathbf{A}_m$ obtained by deleting the row and the column containing the element $b_{u,j}$ of the m -th column. For any $h(x) \in \mathbb{F}_2(x)$, $p_x(h(x))$ denotes the maximal extractable power of x in $h(x)$, $\mu = \max_{v \neq u} \{p_x(y_{i_u} - y_{i_v})\}$ and $\eta = p_x(\prod_{v \neq u} (y_{i_u} - y_{i_v})^{w_{i_v}})$. In $\mathbb{F}_2(x)$. Given that Lemma 3 and Lemma 4 provide two distinct methods for constructing $g(y)$, it follows that

$$\begin{aligned}
g(y) &= \frac{1}{\det(\mathbf{V})} \left(\sum_{u,j} \det(\mathbf{A}_{1,u,j}) b_{u,j} y^0 + \cdots + \sum_{u,j} \det(\mathbf{A}_{t,u,j}) b_{u,j} y^{t-1} \right) \\
&= \sum_{u,j} (y - y_{i_u})^j \prod_{v \neq u} (y - y_{i_v})^{w_{i_v}} \cdot \sum_{e=0}^{w_{i_u}-j-1} a_e (y - y_{i_u})^e \cdot b_{u,j},
\end{aligned}$$

where a_e is defined as (60).

By comparing the coefficients of y^{t-1} in the above two equations, we have

$$\sum_{u,j} \frac{\det(\mathbf{A}_{t,u,j})}{\det(\mathbf{V})} \cdot b_{u,j} = \sum_{u,j} a_{w_{i_u}-j-1} \cdot b_{u,j}. \quad (70)$$

By Lemma 3, for arbitrary pairs $\{(y_{i_u}, b_{u,j})\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$, there exists a polynomial $g(y) \in \mathbb{F}_2[x]$ such that $D^j g(y_{i_u}) = b_{u,j}$. Hence, the equation (70) holds for arbitrary pairs $\{(y_{i_u}, b_{u,j})\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$. The coefficients $\frac{\det(\mathbf{A}_{t,u,j})}{\det(\mathbf{V})}$ and $a_{w_{i_u}-j-1}$ are functions of $\{y_{i_u}\}_{u=1}^n$, hence remain unaffected by variations in $b_{u,j}$. By taking $\mathbf{b} = \{(b_{u,j})\}_{j=0}^{w_{i_u}-1}\}_{u=1}^n$ standard basis vectors, we get

$$\frac{\det(\mathbf{A}_{t,u,j})}{\det(\mathbf{V})} = a_{w_{i_u}-j-1} \quad (71)$$

for $1 \leq u \leq n$ and $0 \leq j \leq w_{i_u} - 1$. For (71), using the conclusion of Lemma 5, we have

$$p_x(\det(\mathbf{V})) - p_x(\det(\mathbf{A}_{t,u,j})) = -p_x(a_{w_{i_u}-j-1}) \leq \eta + (w_{i_u} - j - 1)\mu. \quad (72)$$

In fact, the values of $\det(\mathbf{V}_y)$ and $\det(\mathbf{G}_{t,u,j})$ in the ring $\mathbb{F}_2[x]$ are respectively equal to the values of $\det(\mathbf{V})$ and $\det(\mathbf{A}_{t,u,j})$ in the field $\mathbb{F}_2(x)$. According to (72), we can derive

$$p_x(\det(\mathbf{V}_y)) - p_x(\det(\mathbf{G}_{t,u,j})) \leq \eta + (w_{i_u} - j - 1)\mu. \quad (73)$$

Thus, we complete the proof of Theorem 1.