Smaller Share Size for Evolving Secret Sharing: General Thresholds and Threshold Three

Xiaozheng Wang

Department of Mathematics
Ludwig-Maximilians-Universität München
Munich, Germany

Xiaozheng.Wang@campus.lmu.de

Abstract

Evolving secret sharing allows participants to join indefinitely without modifying previously distributed shares. We study the share size of perfectly secure evolving threshold secret sharing schemes and obtain two results.

For general thresholds, we introduce a polynomial sharing method that shares two secrets with adjacent reconstruction thresholds using one polynomial. Combining this method with the evolving scheme of Cheng et al. (ASIACRYPT 2025), we obtain an evolving k-threshold scheme whose t-th share has size

$$\left\lfloor \frac{k}{2} \right\rfloor \log_2 t + O_k(\ell + \log_2 \log_2 t)$$

bits for an ℓ-bit secret. This reduces the leading coefficient of their general construction from $k-1$ to $\lfloor k/2 \rfloor$.

For threshold three, we give a separate construction that reduces the lower-order terms of the scheme of Cheng et al. We mask the short shares in all generations with the same random ℓ-bit value R, which is shared through an evolving 2-threshold scheme, we obtain

$$\log_2 t + (2 + o(1)) \log_2 \log_2 t$$

bits per share for fixed ℓ. Both constructions satisfy correctness and perfect information-theoretic security.

Keywords: Evolving secret sharing; Threshold secret sharing; Perfect secrecy; Share size; Polynomial secret sharing.

1 Introduction

Secret sharing is a protocol distributing a secret into many shares. Threshold secret sharing is introduced independently by Shamir [1] and Blakley [2], it distributes a secret so that any k participants can recover it, whereas fewer than k participants obtain no information about it. Classical constructions typically require a predetermined number of participants or an upper bound on that number. For example, Shamir's scheme requires a finite field with sufficiently many distinct evaluation points. Therefore, each share is an element of F_q, which requires $\lceil \lg p \rceil$ bits. The secret is reconstructed by any k shares using Langrange interpolation. Komargodski, Naor, and Yogev [**?**] introduced evolving secret sharing, in which the number of participants can increase without a determined upper bound. Shares are assigned to additional participants without modifying previously distributed shares. In a perfectly secure evolving k-threshold scheme, any k participants can recover the secret, while any fewer than k participants obtain

no information about it. while every smaller coalition must learn nothing about it. A central question is how the bit length L_t of the t-th share grows with the participant index t.

For general thresholds, Komargodski et al. [**?**] gave constructions with leading share size term $(k-1)\log_2 t$. Their work also established a connection between evolving 2-threshold secret sharing and prefix codes. D'Arco et al. [7] gave an alternative approach to this connection based on the tree structure underlying a prefix code. Okamura and Koga [8] subsequently developed constructions based on binary and D-ary prefix codes, supporting secrets of arbitrary length.

Algebraic approaches were developed by Xing and Yuan [9], who presented evolving secret sharing schemes based on polynomial evaluations and algebraic geometry codes. Their results include a direct construction for fixed thresholds with share size logarithmic in t, providing an alternative to the recursive construction of Komargodski et al. [**?**]. Cheng et al. [4] developed a polynomial ring construction that connects prefix codes with evolving k-threshold secret sharing for every $k \geq 2$. For an ℓ-bit secret, their construction using the Elias δ code achieves

$$L_t = (k-1)\lfloor \log_2 t \rfloor + 2(k-1)\,\lfloor \log_2(\lfloor \log_2 t \rfloor + 1)\rfloor + \ell.$$

This improves the lower-order terms while retaining the leading coefficient $k-1$.

For threshold three, D'Arco et al. [10] proposed a construction based on the Chinese remainder theorem. Their approach divides participants into generations and combines finite secret sharing within each generation with evolving secret sharing across generations. Cheng et al. [6] subsequently showed that the original construction does not satisfy perfect secrecy and presented a revised construction. Within the same overall framework, they also developed a perfectly secure extension-field construction with share size

$$L_t \leq \log_2 t + O_\ell\left(\sqrt{\log_2 t}\right)$$

for fixed secret length ℓ. Thus, threshold three admits a leading coefficient of 1, compared with the coefficient 2 obtained by applying the general-threshold construction. The finite secret sharing component of their extension-field construction consists of polynomial evaluation shares and an additional ℓ-bit share. The secret can be recovered from either three evaluation shares or two evaluation shares together with the ℓ-bit share.

1.1 Our Results

Our first result is a method for sharing two secrets with adjacent reconstruction thresholds using a single polynomial. The secret associated with the higher threshold is embedded in the leading coefficient. The other secret is specified by a linear projection of the next coefficient. With suitable evaluation points, the lower threshold suffices to recover the latter secret, while one additional evaluation recovers both. Thus, one polynomial evaluation per participant serves two reconstruction thresholds.

We divide the participants into generations

$$G_g = \{t \in \mathbb{N} : 2^{g-1} \leq t < 2^g\}, \qquad g \geq 1,$$

and apply this method within each generation. In each generation, these shares are distributed with respective thresholds $1, 2, \ldots, k$. Pairing thresholds $(2,3), (4,5), \ldots$ reduces the number of long polynomial evaluations received by each participant to $\lfloor k/2 \rfloor$. We prove correctness and perfect security for arbitrary distributions of participants among generations and obtain

$$L_t \leq \left\lfloor \frac{k}{2} \right\rfloor \log_2 t + O_k(\ell + \log_2 \log_2 t)\,.$$

For fixed $k \geq 3$, this reduces the leading coefficient of the general construction of Cheng et al. from $k-1$ to $\lfloor k/2 \rfloor$. The explicit bound, including all rounding terms, is given in Section 4.

Our second result is a separate construction for threshold three, based on the finite extension-field scheme of Cheng et al. [6]. We mask the short share of every generation using the same uniform random ℓ-bit mask. An evolving 2-threshold scheme shares this random mask across generations, while an evolving 3-threshold scheme shares the original secret across generations.Three participants in one generation recover the secret from their polynomial evaluation shares. Three participants in distinct generations use the evolving 3-threshold scheme. If exactly two belong to one generation, the two represented generations recover the random key, allowing the pair to obtain its generation's short share and recover the secret. We prove that every pair of participants remains independent of the secret, including pairs that can recover the random key.

The resulting share size satisfies,

$$\begin{aligned} L_t \leq\ & \log_2 t + 2\log_2\log_2 t \\ & + 2(\ell+1)\sqrt{\log_2\log_2 t} + O(\log_2\log_2\log_2 t + \ell)\,. \end{aligned}$$

Consequently, for fixed ℓ,

$$L_t \leq \log_2 t + (2+o(1))\log_2\log_2 t.$$

This retains the leading coefficient of one and improves the lower-order bound from $O_\ell(\sqrt{\log_2 t})$ in the cited construction to $O(\log_2\log_2 t)$. The construction and its analysis are presented in Section 5.

2 Preliminaries

Throughout this paper, let $\mathbb{N}^+$ denote the set of positive integers, and let $[n] = \{1, 2, \ldots, n\}$ for $n \in \mathbb{N}^+$. For a set A, its cardinality and power set are denoted by $|A|$ and 2^A, respectively. All logarithms are taken to base two, and share sizes are measured in bits. We consider an ℓ-bit secret drawn from the secret space $\mathcal{S} = \{0,1\}^\ell$, where $\ell \in \mathbb{N}^+$. For a finite field $\mathbb{F}$, the notation $\mathbb{F}[X]$ denotes the polynomial ring over $\mathbb{F}$. We write $Z_i^{(s)}$ for the random variable representing the share assigned to participant P_i when the secret is s, and use lowercase letters for particular share values. Tuples of shares are ordered according to the public participant indices.

2.1 Secret Sharing

Let $\mathcal{P}_n = \{P_1, P_2, \ldots, P_n\}$ be a set of n participants. An access structure specifies which subsets of participants are authorized to reconstruct the secret. Since adding participants to a qualified set cannot prevent reconstruction, the collection of qualified sets is required to be monotone.

Definition 1 (Access structure). An access structure on $\mathcal{P}_n$ is a family $\mathcal{A} \subseteq 2^{\mathcal{P}_n}$ such that $\emptyset \notin \mathcal{A}$ and, whenever $A \in \mathcal{A}$ and $A \subseteq C \subseteq \mathcal{P}_n$, it follows that $C \in \mathcal{A}$. Sets belonging to $\mathcal{A}$ are called *qualified*, while subsets of $\mathcal{P}_n$ that do not belong to $\mathcal{A}$ are called *unqualified*.

Definition 2 (Threshold access structure). For $k, n \in \mathbb{N}^+$ with $k \leq n$, the (k,n)-threshold access structure consists of all subsets containing at least k participants:

$$\mathcal{A} = \{A \subseteq \mathcal{P}_n : |A| \geq k\}.$$

A (k,n)-threshold secret sharing scheme allows a dealer to distribute a secret among n participants so that any set of at least k participants can reconstruct it, whereas the joint shares of fewer than k participants reveal no information about it. These requirements are formalized by correctness and perfect security.

Definition 3 (Threshold secret sharing scheme). A (k,n)-threshold secret sharing scheme over the secret space $\mathcal{S}$ consists of a randomized sharing algorithm $\mathcal{E}$ and a reconstruction

algorithm $\mathcal{R}$. Given a secret $s \in \mathcal{S}$, the sharing algorithm generates

$$(Z_1^{(s)}, Z_2^{(s)}, \ldots, Z_n^{(s)}) \leftarrow \mathcal{E}(s),$$

and the dealer privately delivers $Z_i^{(s)}$ to participant P_i. The scheme must satisfy the following two properties.

- **Correctness.** The scheme satisfies correctness if, for every secret $s \in \mathcal{S}$ and every set $A \subseteq \mathcal{P}_n$ with $|A| \geq k$, the reconstruction algorithm recovers the secret from the shares held by A with probability one:

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

  The probability is taken over the randomness of the sharing algorithm and, if applicable, the reconstruction algorithm.

- **Perfect security.** The scheme satisfies perfect security if, for every set $C \subseteq \mathcal{P}_n$ with $|C| < k$ and every pair of secrets $s_0, s_1 \in \mathcal{S}$, the joint distributions of the shares held by C are identical under the two secrets. Specifically, for every tuple of share values $(z_i)_{P_i \in C}$,

  $$\Pr\Big[(Z_i^{(s_0)})_{P_i \in C} = (z_i)_{P_i \in C}\Big] = \Pr\Big[(Z_i^{(s_1)})_{P_i \in C} = (z_i)_{P_i \in C}\Big].$$

  Thus, an unqualified set obtains no information about the secret, even with unlimited computational power. This requirement applies to its entire joint collection of shares.

Let $B(Z_i^{(s)})$ denote the bit length of the share assigned to P_i. All share-size bounds in this paper hold uniformly over the choice of the secret and every possible outcome of the sharing randomness. Public participant identifiers are not counted as part of the shares. In Shamir's construction, the dealer chooses a polynomial of degree at most $k-1$ over a finite field, places the secret in its constant coefficient, and samples the remaining coefficients independently and uniformly. Each participant receives an evaluation at a distinct nonzero field element. Any k evaluations determine the polynomial and hence the secret, while fewer than k evaluations have a joint distribution independent of the constant coefficient. For an ℓ-bit secret, choosing a binary extension field large enough to contain the secret and n distinct nonzero evaluation points gives

$$B(Z_i^{(s)}) = \max\{\ell, \lceil \log_2(n+1) \rceil\}, \qquad i \in [n].$$

2.2 Evolving Secret Sharing

In conventional threshold secret sharing, the number of participants is fixed or bounded when the scheme is initialized. Evolving secret sharing allows participants to arrive sequentially without requiring a predetermined upper bound. The dealer assigns a share to each new participant while leaving all previously distributed shares unchanged. Let $\mathcal{P} = \{P_1, P_2, \ldots\}$ be a countably infinite sequence of potential participants, indexed by their order of arrival.After t participants have joined, the participants present in the system form the set $\mathcal{P}_t = \{P_1, \ldots, P_t\}$. Throughout the execution, the reconstruction threshold k remains fixed.

Definition 4 (Evolving access structure). An evolving access structure on $\mathcal{P}$ is a monotone family $\mathcal{A} \subseteq 2^{\mathcal{P}}$ that does not contain the empty set. For every $t \in \mathbb{N}^+$, Its restriction to the first t participants is

$$\mathcal{A}_t = \mathcal{A} \cap 2^{\mathcal{P}_t}.$$

The family $\mathcal{A}_t$ specifies the qualified sets among the first t participants and may be empty if none of their subsets is qualified.

Definition 5 (Evolving threshold access structure). For $k \in \mathbb{N}^+$, the evolving k-threshold access structure consists of all subsets of $\mathcal{P}$ containing at least k participants:

$$\mathcal{A} = \{A \subseteq \mathcal{P} : |A| \geq k\}.$$

After t participants have joined, the restricted access structure is

$$\mathcal{A}_t = \{A \subseteq \mathcal{P}_t : |A| \geq k\}.$$

Definition 6 (Evolving threshold secret sharing scheme). An evolving k-threshold secret sharing scheme over $\mathcal{S}$ consists of a sharing algorithm $\mathcal{E}$ and a reconstruction algorithm $\mathcal{R}$. Given a secret $s \in \mathcal{S}$, the dealer generates a share for each participant upon arrival. When P_t joins, its share is generated as

$$Z_t^{(s)} \leftarrow \mathcal{E}\Big(s, (Z_1^{(s)}, \ldots, Z_{t-1}^{(s)})\Big).$$

For $t = 1$, the tuple of previous shares is empty. The sharing algorithm may retain private internal state between invocations; this state is implicit in the notation. The dealer does not require an upper bound on the eventual number of participants, and generating a new share does not modify any previously distributed share. The scheme must satisfy the following properties after any finite number of participants have joined.

- **Correctness.** For every secret $s \in \mathcal{S}$, every $t \in \mathbb{N}^+$, and every qualified set $A \in \mathcal{A}_t$, the reconstruction algorithm satisfies

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

  All shares in this expression are generated within the same ongoing execution. The probability is taken over the randomness of the sharing and reconstruction algorithms.

- **Perfect security.** For every $t \in \mathbb{N}^+$, every set $C \subseteq \mathcal{P}_t$ with $|C| < k$, every pair of secrets $s_0, s_1 \in \mathcal{S}$, and every tuple of share values $(z_i)_{P_i \in C}$, it holds that

  $$\Pr\Big[(Z_i^{(s_0)})_{P_i \in C} = (z_i)_{P_i \in C}\Big] = \Pr\Big[(Z_i^{(s_1)})_{P_i \in C} = (z_i)_{P_i \in C}\Big].$$

  Hence, the joint shares of any set of fewer than k participants reveal no information about the secret, regardless of their arrival times.

The efficiency of an evolving scheme is measured by the bit length $B(Z_t^{(s)})$ of the share assigned to the t-th participant, expressed in terms of k, t, and ℓ. This length may grow with the arrival index t, while every previously issued share remains valid and unchanged.

3 Sharing Two Secrets at Adjacent Thresholds Using One Polynomial

We share two ℓ-bit secrets $P, Q \in \mathbb{F}_{2^\ell}$ using one field element per participant. Any k shares recover P, and any $k+1$ shares recover both P and Q. Fewer than k shares reveal no information about (P, Q); k shares reveal no information about Q beyond P.

3.1 Description of the Proposed Scheme

Let $2 \leq k < n$. Let r be the degree of a finite extension of $\mathbb{F}_{2^\ell}$. Choose a monic irreducible polynomial $\psi(y) \in \mathbb{F}_{2^\ell}[y]$ of degree r, and set

$$K = \mathbb{F}_{2^\ell}[y]/(\psi(y)), \qquad \theta = y + (\psi(y)), \qquad [K : \mathbb{F}_{2^\ell}] = r. \tag{1}$$

Define the $\mathbb{F}_{2^\ell}$-linear projection

$$\tau : K \longrightarrow \mathbb{F}_{2^\ell}, \qquad \tau\left(\sum_{j=0}^{r-1} a_j \theta^j\right) = a_0, \quad a_j \in \mathbb{F}_{2^\ell}. \tag{2}$$

Choose r large enough to admit n distinct evaluation points

$$\alpha_1, \ldots, \alpha_n \in \ker \tau \setminus \{0\}. \tag{3}$$

Independently sample

$$Y \xleftarrow{\$} \tau^{-1}(P) \qquad R_0, \ldots, R_{k-2} \xleftarrow{\$} K,$$

Define

$$F(X) = QX^k + YX^{k-1} + \sum_{j=0}^{k-2} R_j X^j, \qquad W_i = F(\alpha_i), \quad i \in [n]. \tag{4}$$

Participant i receives $W_i \in K$, represented by ℓr bits.

Remark (The extension degree). The space $\ker \tau$ has dimension $r-1$ over $\mathbb{F}_{2^\ell}$. The requirement in (3) is therefore

$$|\ker \tau \setminus \{0\}| = 2^{\ell(r-1)} - 1 \geq n \quad \Longleftrightarrow \quad \ell(r-1) \geq \log_2(n+1).$$

The smallest admissible degree and the resulting share length are

$$r = 1 + \left\lceil \frac{\log_2(n+1)}{\ell} \right\rceil, \qquad |W_i| = \ell\left(1 + \left\lceil \frac{\log_2(n+1)}{\ell} \right\rceil\right). \tag{5}$$

3.2 Correctness and Perfect Secrecy

For a polynomial $f(X)$, $[X^j]f(X)$ denotes the coefficient of X^j.

Proof of correctness.

Case 1. Recovery from k shares.

Let $A \subseteq [n]$ with $|A| = k$. By Lagrange interpolation,

$$\sum_{i \in A} W_i \prod_{j \in A \setminus \{i\}} \frac{X - \alpha_j}{\alpha_i - \alpha_j} = F(X) - Q \prod_{j \in A} (X - \alpha_j). \tag{6}$$

To verify this identity, observe that both sides are polynomials of degree at most $k-1$, since the leading term QX^k of $F(X)$ is canceled on the right-hand side. For every $i \in A$, substituting $X = \alpha_i$ gives

$$\sum_{h \in A} W_h \prod_{j \in A \setminus \{h\}} \frac{\alpha_i - \alpha_j}{\alpha_h - \alpha_j} = W_i = F(\alpha_i) - Q \prod_{j \in A} (\alpha_i - \alpha_j).$$

Since the α_i are pairwise distinct, these k values uniquely determine a polynomial of degree at most $k-1$. Hence the identity follows.

Since

$$[X^{k-1}] \prod_{j \in A \setminus \{i\}} (X - \alpha_j) = 1, \qquad [X^{k-1}] \prod_{j \in A} (X - \alpha_j) = -\sum_{j \in A} \alpha_j,$$

comparison of the X^{k-1} coefficients in (6) yields

$$\sum_{i \in A} \frac{W_i}{\prod_{j \in A \setminus \{i\}} (\alpha_i - \alpha_j)} = Y + Q \sum_{j \in A} \alpha_j. \tag{7}$$

By $\mathbb{F}_{2^\ell}$-linearity of τ and $\tau(\alpha_j) = 0$,

$$\tau\left(\sum_{i\in A} \frac{W_i}{\prod_{j\in A\setminus\{i\}} (\alpha_i - \alpha_j)}\right) = \tau(Y) + Q\sum_{j\in A}\tau(\alpha_j) = P. \tag{8}$$

Case 2. Recovery from $k+1$ shares.

Let $A = \{i_1, \ldots, i_{k+1}\} \subseteq [n]$. Than there is a system of $k+1$ equations with $k+1$ variables.

$$\begin{cases} \sum_{j=0}^{k-2} R_j \alpha_{i_1}^j + Y\alpha_{i_1}^{k-1} + Q\alpha_{i_1}^k = W_{i_1}, \\ \sum_{j=0}^{k-2} R_j \alpha_{i_2}^j + Y\alpha_{i_2}^{k-1} + Q\alpha_{i_2}^k = W_{i_2}, \\ \qquad\qquad \vdots \\ \sum_{j=0}^{k-2} R_j \alpha_{i_{k+1}}^j + Y\alpha_{i_{k+1}}^{k-1} + Q\alpha_{i_{k+1}}^k = W_{i_{k+1}}. \end{cases} \tag{9}$$

The coefficient matrix is a Vandermonde matrix, with

$$\det\left(\alpha_{i_a}^{b-1}\right)_{1\le a,b\le k+1} = \prod_{1\le a<b\le k+1} (\alpha_{i_b} - \alpha_{i_a}) \neq 0.$$

Thus (9) uniquely determines Y, Q, and $P = \tau(Y)$.

Proof of perfect secrecy.

We fix $q \in \mathbb{F}_{2^\ell}$ and consider

$$Q = q, \qquad Y, R_0, \ldots, R_{k-2} \xleftarrow{\$} K, \qquad P = \tau(Y),$$

where the coefficients are sampled independently and uniformly.When $P = p$, the coefficient distribution is exactly that of the original scheme for inputs (p, q).

For a participant set $A \subseteq [n]$, write

$$W_i = q\alpha_i^k + Y\alpha_i^{k-1} + \sum_{j=0}^{k-2} R_j\alpha_i^j, \qquad W_A = (W_i)_{i\in A}.$$

Since τ is surjective, each $p \in \mathbb{F}_{2^\ell}$ has exactly $|\ker\tau|$ preimages in K. Among the $|K|^k$ equally likely coefficient tuples, $|\ker\tau|\,|K|^{k-1}$ satisfy $\tau(Y) = p$. Therefore,

$$\begin{aligned} \Pr(P = p \mid Q = q) &= \Pr(\tau(Y) = p \mid Q = q) \\ &= \frac{|\ker\tau|\,|K|^{k-1}}{|K|^k} \\ &= \frac{|\ker\tau|}{|K|} \\ &= 2^{-\ell}. \end{aligned}$$

For $w \in K^{|A|}$, Bayes' formula gives

$$\begin{aligned} &\Pr(W_A = w \mid P = p, Q = q) \\ &= \frac{\Pr(W_A = w, P = p \mid Q = q)}{\Pr(P = p \mid Q = q)} \\ &= \frac{\Pr(P = p \mid W_A = w, Q = q)\Pr(W_A = w \mid Q = q)}{\Pr(P = p \mid Q = q)}. \end{aligned}$$

Case 1. $|A| < k$.

Let $A = \{i_1, \ldots, i_m\}$ with $1 \le m < k$, and fix $w = (w_i)_{i \in A} \in K^m$.

For every choice of

$$Y \in K, \qquad R_m, \ldots, R_{k-2} \in K,$$

the constraints $W_A = w$ give

$$\sum_{j=0}^{m-1} R_j \alpha_i^j = w_i - q\alpha_i^k - Y\alpha_i^{k-1} - \sum_{j=m}^{k-2} R_j \alpha_i^j, \qquad i \in A.$$

Empty sums are zero. The coefficient matrix satisfies

$$\det\left(\alpha_{i_a}^{b-1}\right)_{1 \le a,b \le m} = \prod_{1 \le a < b \le m} (\alpha_{i_b} - \alpha_{i_a}) \neq 0.$$

Thus, for each fixed choice of $Y, R_m, \ldots, R_{k-2}$, these m independent equations uniquely determine $R_0, \ldots, R_{m-1}$. There are $|K|^{k-m}$ such choices, so

$$\begin{aligned} \Pr(W_A = w \mid Q = q) &= \frac{|K|^{k-m}}{|K|^k} \\ &= |K|^{-m}. \end{aligned}$$

Next, the additional condition $P = p$ restricts Y to $\tau^{-1}(p)$, which contains $|\ker \tau|$ elements. For every such Y, the remaining $k - 1 - m$ coefficients $R_m, \ldots, R_{k-2}$ are unrestricted, while $R_0, \ldots, R_{m-1}$ are uniquely determined by the same equations. Hence,

$$\begin{aligned} &\Pr(P = p, W_A = w \mid Q = q) \\ &= \frac{|\ker \tau|\,|K|^{k-1-m}}{|K|^k}. \end{aligned}$$

By the definition of conditional probability,

$$\begin{aligned} &\Pr(P = p \mid W_A = w, Q = q) \\ &= \frac{\Pr(P = p, W_A = w \mid Q = q)}{\Pr(W_A = w \mid Q = q)} \\ &= \frac{|\ker \tau|\,|K|^{k-1-m}/|K|^k}{|K|^{k-m}/|K|^k} \\ &= \frac{|\ker \tau|}{|K|} \\ &= 2^{-\ell}. \end{aligned}$$

By the Bayes' formula, we obtain,

$$\begin{aligned} &\Pr(W_A = w \mid P = p, Q = q) \\ &= \frac{\Pr(P = p \mid W_A = w, Q = q)\Pr(W_A = w \mid Q = q)}{\Pr(P = p \mid Q = q)} \\ &= \frac{\dfrac{|\ker \tau|\,|K|^{k-1-m}}{|K|^{k-m}} \cdot \dfrac{|K|^{k-m}}{|K|^k}}{\dfrac{|\ker \tau|\,|K|^{k-1}}{|K|^k}} \\ &= \frac{|\ker \tau|\,|K|^{k-1-m}}{|\ker \tau|\,|K|^{k-1}} \\ &= |K|^{-m}. \end{aligned} \tag{10}$$

This probability is independent of both p and q. The case $A = \varnothing$ is immediate.

Case 2. $|A| = k$**.**

Let $A = \{i_1, \ldots, i_k\}$, and let w be any share tuple that the original scheme can produce with first secret p for some value of the second secret.

By correctness,

$$\tau\left(\sum_{i\in A} \frac{w_i}{\prod\limits_{j\in A\setminus\{i\}} (\alpha_i - \alpha_j)}\right) = p. \tag{11}$$

For any $q \in \mathbb{F}_{2^\ell}$, the equations

$$\sum_{j=0}^{k-2} R_j \alpha_i^j + Y\alpha_i^{k-1} = w_i - q\alpha_i^k, \qquad i \in A,$$

have a unique solution $(R_0, \ldots, R_{k-2}, Y) \in K^k$, since

$$\det\left(\alpha_{i_a}^{b-1}\right)_{1\le a,b\le k} = \prod_{1\le a<b\le k} (\alpha_{i_b} - \alpha_{i_a}) \neq 0.$$

Thus, for each fixed q, exactly one of the $|K|^k$ equally likely coefficient tuples produces $W_A = w$. Consequently,

$$\begin{aligned}\Pr(W_A = w \mid Q = q) &= \frac{1}{|K|^k} \\ &= |K|^{-k}.\end{aligned}$$

The coefficient identity in the correctness proof gives

$$Y = \sum_{i\in A} \frac{w_i}{\prod\limits_{j\in A\setminus\{i\}} (\alpha_i - \alpha_j)} - q\sum_{i\in A} \alpha_i.$$

Using $\mathbb{F}_{2^\ell}$-linearity of τ, $\tau(\alpha_i) = 0$, and (11), we obtain

$$\begin{aligned}\tau(Y) &= \tau\left(\sum_{i\in A} \frac{w_i}{\prod\limits_{j\in A\setminus\{i\}} (\alpha_i - \alpha_j)}\right) - q\sum_{i\in A} \tau(\alpha_i) \\ &= p.\end{aligned}$$

Therefore, the unique coefficient tuple determined by $W_A = w$ and $Q = q$ also satisfies $P = p$. It follows that

$$\begin{aligned}&\Pr(P = p, W_A = w \mid Q = q) \\ &= \frac{1}{|K|^k}.\end{aligned}$$

By the definition of conditional probability,

$$\begin{aligned}&\Pr(P = p \mid W_A = w, Q = q) \\ &= \frac{\Pr(P = p, W_A = w \mid Q = q)}{\Pr(W_A = w \mid Q = q)} \\ &= \frac{|K|^{-k}}{|K|^{-k}} \\ &= 1.\end{aligned}$$

By the Bayes' formula,

$$\begin{aligned}
&\Pr(W_A = w \mid P = p, Q = q) \\
&= \frac{\Pr(P = p \mid W_A = w, Q = q)\Pr(W_A = w \mid Q = q)}{\Pr(P = p \mid Q = q)} \\
&= \frac{\dfrac{|K|^{-k}}{|K|^{-k}} \cdot \dfrac{1}{|K|^k}}{\dfrac{|\ker\tau|\,|K|^{k-1}}{|K|^k}} \\
&= \frac{|K|^{-k}}{|\ker\tau|/|K|} \\
&= \frac{1}{|\ker\tau|\,|K|^{k-1}}.
\end{aligned} \tag{12}$$

If w does not satisfy (11), its conditional probability is zero for every q.

Every admissible w occurs for every q with the same probability. Hence both the set of possible share tuples and their probabilities depend only on p, so k shares reveal no information about Q beyond P.

These conclusions hold for any joint distribution of the original secrets P, Q.

3.3 Example: Thresholds Two and Three

For $k = 2$,

$$F(X) = QX^2 + YX + R_0, \qquad \tau(Y) = P.$$

Case 1. Recovery from two shares.

For distinct i, j, Lagrange interpolation gives

$$W_i\frac{X-\alpha_j}{\alpha_i-\alpha_j} + W_j\frac{X-\alpha_i}{\alpha_j-\alpha_i} = F(X) - Q(X-\alpha_i)(X-\alpha_j).$$

Comparing the coefficients of X,

$$\frac{W_i - W_j}{\alpha_i - \alpha_j} = Y + Q(\alpha_i + \alpha_j), \qquad P = \tau\left(\frac{W_i - W_j}{\alpha_i - \alpha_j}\right).$$

Case 2. Recovery from three shares.

For distinct i, j, h,

$$\begin{pmatrix} 1 & \alpha_i & \alpha_i^2 \\ 1 & \alpha_j & \alpha_j^2 \\ 1 & \alpha_h & \alpha_h^2 \end{pmatrix} \begin{pmatrix} R_0 \\ Y \\ Q \end{pmatrix} = \begin{pmatrix} W_i \\ W_j \\ W_h \end{pmatrix}.$$

Since $(\alpha_j - \alpha_i)(\alpha_h - \alpha_i)(\alpha_h - \alpha_j) \neq 0$, the system determines Q and $P = \tau(Y)$. Perfect secrecy follows from (10) and (12).

4 The Proposed Scheme

Let $k \geq 3$ and let $S \in \mathbb{F}_{2^\ell}$ be an ℓ-bit secret. We combine the method of Section 3 with the polynomial-ring evolving k-threshold scheme of Cheng et al. (ASIACRYPT 2025).

4.1 Description of the Proposed Scheme

shares across generations.

We use one instance of the evolving k-threshold scheme for secret sharing across generations. The bit length of its v-th share is at most

$$\begin{aligned} L_{\text{out}}(v) = (k-1)\lfloor \log_2 v \rfloor \\ + 2(k-1)\left\lfloor \log_2(\lfloor \log_2 v \rfloor + 1)\right\rfloor + \ell. \end{aligned} \tag{13}$$

Any k distinct shares of this scheme recover S, whereas fewer than k reveal no information about S.

Partition the participants into generations

$$G_g = \{P_t : 2^{g-1} \le t < 2^g\}, \qquad |G_g| = 2^{g-1}, \qquad g \ge 1. \tag{14}$$

For $P_t \in G_g$, its generation number and index within the generation are

$$g = \lfloor \log_2 t \rfloor + 1, \qquad i = t - 2^{g-1} + 1.$$

Generation G_g is assigned the k consecutive shares across generations indexed by $k(g-1)+1, \ldots, kg$.

Secret sharing within each generation.

Let m_g be the extension degree of $\mathbb{F}_{2^{\ell m_g}}$ over $\mathbb{F}_{2^\ell}$, chosen so that

$$[\mathbb{F}_{2^{\ell m_g}} : \mathbb{F}_{2^\ell}] = m_g, \qquad \ell m_g \ge L_{\text{out}}(kg).$$

Let $U_{g,j} \in \mathbb{F}_{2^{\ell m_g}}$ denote the j-th share across generations assigned to G_g, represented as a field element through a fixed injective encoding, for $j = 1, \ldots, k$.

Let r_g be the degree of a further extension of $\mathbb{F}_{2^{\ell m_g}}$. Choose a monic irreducible polynomial $\psi_g(y) \in \mathbb{F}_{2^{\ell m_g}}[y]$ of degree r_g, and define

$$\begin{aligned} \mathbb{F}_g = \mathbb{F}_{2^{\ell m_g}}[y]/(\psi_g(y)), \qquad [\mathbb{F}_g : \mathbb{F}_{2^{\ell m_g}}] = r_g, \\ \tau_g : \mathbb{F}_g \longrightarrow \mathbb{F}_{2^{\ell m_g}}, \qquad \tau_g\left(\sum_{j=0}^{r_g-1} a_j y^j\right) = a_0, \quad a_j \in \mathbb{F}_{2^{\ell m_g}}. \end{aligned} \tag{15}$$

Choose r_g large enough to admit 2^{g-1} distinct points

$$\alpha_{g,1}, \ldots, \alpha_{g,2^{g-1}} \in \ker \tau_g \setminus \{0\}. \tag{16}$$

Each participant in G_g receives $U_{g,1}$ directly. For every even a with $2 \le a < k$, independently sample

$$Y_g^{(a)} \xleftarrow{\$} \tau_g^{-1}(U_{g,a}), \qquad R_{g,0}^{(a)}, \ldots, R_{g,a-2}^{(a)} \xleftarrow{\$} \mathbb{F}_g,$$

and set

$$\begin{aligned} F_g^{(a)}(X) = U_{g,a+1}X^a + Y_g^{(a)}X^{a-1} + \sum_{j=0}^{a-2} R_{g,j}^{(a)} X^j, \\ W_{g,i}^{(a)} = F_g^{(a)}(\alpha_{g,i}). \end{aligned} \tag{17}$$

These are the formulas of Section 3 with base field $\mathbb{F}_{2^{\ell m_g}}$ and threshold a. They also apply when $|G_g| < a+1$; a recovery requirement is used only when enough shares exist.

Case 1. $k = 2p+1$ **is odd.**

For $P_t \in G_g$, assign

$$Z_t = (U_{g,1}, W_{g,i}^{(2)}, W_{g,i}^{(4)}, \ldots, W_{g,i}^{(2p)}). \tag{18}$$

Case 2. $k = 2p$ **is even.**

Independently sample $T_{g,1}, \ldots, T_{g,k-1} \xleftarrow{\$} \mathbb{F}_g$ and define

$$F_g^{(k)}(X) = U_{g,k} + \sum_{j=1}^{k-1} T_{g,j} X^j. \tag{19}$$

For $P_t \in G_g$, assign

$$Z_t = (U_{g,1}, W_{g,i}^{(2)}, W_{g,i}^{(4)}, \ldots, W_{g,i}^{(2p-2)}, F_g^{(k)}(\alpha_{g,i})). \tag{20}$$

The polynomials are sampled using independent randomness, also independent of the evolving scheme. When the first participant in G_g arrives, the dealer generates the shares and polynomials for that generation. Each participant then receives Z_t upon arrival, using these fixed polynomials.

Remark (The extension degrees). An element of $\mathbb{F}_{2^{\ell m_g}}$ represents ℓm_g bits, so the smallest choice satisfying the common length bound is

$$\begin{aligned} m_g &= \left\lceil \frac{L_{\text{out}}(kg)}{\ell} \right\rceil \\ &= 1 + \left\lceil \frac{k-1}{\ell} \left(\lfloor \log_2(kg) \rfloor + 2 \left\lfloor \log_2\big(\lfloor \log_2(kg) \rfloor + 1 \big) \right\rfloor \right) \right\rceil. \end{aligned} \tag{21}$$

The 2^{g-1} nonzero evaluation points in (16) require

$$2^{\ell m_g (r_g - 1)} - 1 \geq 2^{g-1}.$$

Since $\ell m_g(r_g - 1)$ is an integer,

$$2^{\ell m_g (r_g - 1)} - 1 \geq 2^{g-1} \quad \Longleftrightarrow \quad \ell m_g (r_g - 1) \geq g.$$

Thus the smallest admissible choice is

$$r_g = 1 + \left\lceil \frac{g}{\ell m_g} \right\rceil, \qquad |\mathbb{F}_g| = 2^{\ell m_g r_g}. \tag{22}$$

We use (21) and (22) throughout the analysis.

4.2 Correctness and Perfect Secrecy

Proof of correctness.

Let A be a set of k participants, and put

$$s_g = |A \cap G_g|, \qquad \sum_g s_g = k.$$

For every generation with $s_g > 0$, Section 3.2 and polynomial evaluation polynomial interpolation give

$$(Z_t)_{P_t \in A \cap G_g} \quad \Longrightarrow \quad U_{g,1}, \ldots, U_{g,s_g}. \tag{23}$$

Indeed, $U_{g,1}$ is included directly; a pair $(a, a+1)$ supplies $U_{g,a}$ when $s_g \geq a$ and $U_{g,a+1}$ when $s_g \geq a+1$. For even k, $s_g = k$ also determines the constant coefficient $U_{g,k}$ of (19).

Case 1. All k **participants belong to one generation.**

If $A \subseteq G_g$, then $s_g = k$. By (23), the k participants in G_g recover all k shares across generations assigned to this generation,

$$U_{g,1}, \ldots, U_{g,k}.$$

Thus, the evolving k-threshold scheme directly recovers S.

Case 2. The participants belong to more than one generation.

For each generation G_g, let $s_g = |A \cap G_g|$. Since A intersects more than one generation, we have $s_g < k$ for every g.

In each generation G_g with $s_g > 0$, the s_g participants recover s_g shares across generations,

$$U_{g,1}, \ldots, U_{g,s_g}.$$

Indeed, $U_{g,1}$ is included directly, while the remaining elements are recovered using the adjacent-threshold recovery formulas of Section 3.2. For each pair $(a, a+1)$, $s_g \geq a$ allows the recovery of $U_{g,a}$, and $s_g \geq a+1$ also allows the recovery of $U_{g,a+1}$.

Since different generations are assigned disjoint sets of shares across generations and

$$\sum_{g:s_g>0} s_g = k,$$

the participants in A recover k distinct shares across generations. By correctness of the evolving k-threshold scheme, these shares recover S.

Proof of perfect secrecy. Let C be a nonempty set of fewer than k participants. For each P_t, let Z_t denote its assigned share. Define

$$s_g = |C \cap G_g|, \qquad U_C = (U_{g,j})_{\substack{g:s_g>0 \\ 1\leq j\leq s_g}}, \qquad Z_C = (Z_t)_{P_t \in C}.$$

Thus, U_C consists of the corresponding shares across generations, while Z_C denotes the joint shares held by the participants in C.

For each pair $(a, a+1)$, equations (10) and (12) imply that the observed evaluations are independent of both inputs when $s_g < a$, and depend only on $U_{g,a}$ when $s_g = a$. For $s_g \geq a+1$, both inputs belong to U_C.

For even k, the $s_g < k$ evaluations of (19) are independent of $U_{g,k}$, as verified below.

Since the random choices for distinct polynomials are independent, the conditional distribution of Z_C depends only on U_C. For fixed u, let $q_C(z \mid u)$ denote the probability that the local sharing procedures produce $Z_C = z$ when $U_C = u$. Hence,

$$\Pr(Z_C = z \mid U_C = u, S = s) = q_C(z \mid u), \tag{24}$$

whenever the conditional probability is defined.

Since

$$\sum_g s_g = |C| < k,$$

the components of U_C encode fewer than k distinct shares across generations. By perfect secrecy of the evolving scheme,

$$\Pr(U_C = u \mid S = s) = \Pr(U_C = u \mid S = s') \tag{25}$$

for any secret values s, s'.

By the total probability formula,

$$\begin{aligned} \Pr(Z_C = z \mid S = s) &= \sum_u q_C(z \mid u) \Pr(U_C = u \mid S = s) \\ &= \sum_u q_C(z \mid u) \Pr(U_C = u \mid S = s') \\ &= \Pr(Z_C = z \mid S = s'). \end{aligned} \tag{26}$$

It remains to verify the claim for even k. Recall that

$$F_g^{(k)}(X) = U_{g,k} + \sum_{j=1}^{k-1} T_{g,j} X^j,$$

where $T_{g,1}, \ldots, T_{g,k-1}$ are chosen independently and uniformly from $\mathbb{F}_g$.

Let

$$C \cap G_g = \{P_{t_1}, \ldots, P_{t_{s_g}}\},$$

where i_h is the index of P_{t_h} within generation G_g. Consider the matrix

$$M = \begin{pmatrix} \alpha_{g,i_1} & \alpha_{g,i_1}^2 & \cdots & \alpha_{g,i_1}^{s_g} \\ \alpha_{g,i_2} & \alpha_{g,i_2}^2 & \cdots & \alpha_{g,i_2}^{s_g} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g,i_{s_g}} & \alpha_{g,i_{s_g}}^2 & \cdots & \alpha_{g,i_{s_g}}^{s_g} \end{pmatrix}.$$

We have $M = DH$, where

$$D = \begin{pmatrix} \alpha_{g,i_1} & & \\ & \ddots & \\ & & \alpha_{g,i_{s_g}} \end{pmatrix}$$

and

$$H = \begin{pmatrix} 1 & \alpha_{g,i_1} & \cdots & \alpha_{g,i_1}^{s_g-1} \\ 1 & \alpha_{g,i_2} & \cdots & \alpha_{g,i_2}^{s_g-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{g,i_{s_g}} & \cdots & \alpha_{g,i_{s_g}}^{s_g-1} \end{pmatrix}.$$

Since the evaluation points are nonzero and pairwise distinct,

$$\det D = \prod_{h=1}^{s_g} \alpha_{g,i_h} \neq 0$$

and

$$\det H = \prod_{1 \leq h < r \leq s_g} (\alpha_{g,i_r} - \alpha_{g,i_h}) \neq 0.$$

Therefore,

$$\det M = \det D \det H \neq 0,$$

so M is invertible.

For fixed $U_{g,k}$ and $T_{g,s_g+1}, \ldots, T_{g,k-1}$, we have

$$\begin{pmatrix} F_g^{(k)}(\alpha_{g,i_1}) \\ \vdots \\ F_g^{(k)}(\alpha_{g,i_{s_g}}) \end{pmatrix} = M \begin{pmatrix} T_{g,1} \\ \vdots \\ T_{g,s_g} \end{pmatrix} + \begin{pmatrix} U_{g,k} + \sum_{j=s_g+1}^{k-1} T_{g,j} \alpha_{g,i_1}^j \\ \vdots \\ U_{g,k} + \sum_{j=s_g+1}^{k-1} T_{g,j} \alpha_{g,i_{s_g}}^j \end{pmatrix}.$$

Since M is invertible, every evaluation tuple corresponds to exactly one choice of $(T_{g,1}, \ldots, T_{g,s_g})$. These coefficients are independent and uniformly distributed over $\mathbb{F}_g$. Consequently, for every $w \in \mathbb{F}_g^{s_g}$ and u,

$$\Pr\left(\left(F_g^{(k)}(\alpha_{g,i_h}) \right)_{h=1}^{s_g} = w \,\middle|\, U_{g,k} = u \right) = |\mathbb{F}_g|^{-s_g}.$$

Thus, any $s_g < k$ evaluations of $F_g^{(k)}$ are uniformly distributed, independently of $U_{g,k}$.

The argument applies to participants from the same or different generations and does not require independence of the shares across generations. The empty set is immediate. Hence the proposed scheme satisfies perfect secrecy.

4.3 Analysis of Share Size

Let L_t be the bit length of Z_t, and let $g = \lfloor \log_2 t \rfloor + 1$. Z_t contains one element of $\mathbb{F}_{2^{\ell m_g}}$ and $\lfloor k/2 \rfloor$ elements of $\mathbb{F}_g$. Therefore

$$\begin{aligned} L_t &= \ell m_g \left(1 + \left\lfloor \frac{k}{2} \right\rfloor r_g\right) \\ &= \ell m_g \left[1 + \left\lfloor \frac{k}{2} \right\rfloor \left(1 + \left\lceil \frac{g}{\ell m_g} \right\rceil\right)\right]. \end{aligned} \tag{27}$$

Recall that

$$m_g = \left\lceil \frac{L_{\text{out}}(kg)}{\ell} \right\rceil.$$

For positive integers a, b, we have

$$\left\lceil \frac{a}{b} \right\rceil = \left\lfloor \frac{a-1}{b} \right\rfloor + 1.$$

Since g, ℓ, and m_g are positive integers,

$$\begin{aligned} \ell m_g \left\lceil \frac{g}{\ell m_g} \right\rceil &= \ell m_g \left(\left\lfloor \frac{g-1}{\ell m_g} \right\rfloor + 1\right) \\ &\le g + \ell m_g - 1. \end{aligned}$$

Similarly, by the definition of m_g,

$$\begin{aligned} \ell m_g &= \ell \left\lceil \frac{L_{\text{out}}(kg)}{\ell} \right\rceil \\ &= \ell \left(\left\lfloor \frac{L_{\text{out}}(kg) - 1}{\ell} \right\rfloor + 1\right) \\ &\le L_{\text{out}}(kg) + \ell - 1. \end{aligned}$$

Consequently,

$$\begin{aligned} L_t &\le \left\lfloor \frac{k}{2} \right\rfloor (g-1) + \left(2\left\lfloor \frac{k}{2} \right\rfloor + 1\right) \ell m_g \\ &\le \left\lfloor \frac{k}{2} \right\rfloor \lfloor \log_2 t \rfloor + \left(2\left\lfloor \frac{k}{2} \right\rfloor + 1\right) \left(L_{\text{out}}(kg) + \ell - 1\right). \end{aligned} \tag{28}$$

Substituting (13) yields

$$\begin{aligned} L_t \le\ & \left\lfloor \frac{k}{2} \right\rfloor \lfloor \log_2 t \rfloor \\ & + \left(2\left\lfloor \frac{k}{2} \right\rfloor + 1\right) \Big[2\ell - 1 + (k-1)\lfloor \log_2(kg) \rfloor \\ & \qquad + 2(k-1)\left\lfloor \log_2\big(\lfloor \log_2(kg) \rfloor + 1\big) \right\rfloor\Big], \\ g &= \lfloor \log_2 t \rfloor + 1. \end{aligned} \tag{29}$$

For fixed k, this gives

$$L_t \le \left\lfloor \frac{k}{2} \right\rfloor \log_2 t + O_k(\ell + \log_2 \log_2(t+2)).$$

5 Smaller Shares for Evolving Three-Threshold Secret Sharing

We now consider the case $k = 3$. The construction of Cheng et al. [**?**] has leading share-size term $\log_2 t$. In this section, we reduce its lower-order terms by using one random ℓ-bit mask R across all generations. An evolving 2-threshold scheme shares R, while an evolving 3-threshold scheme shares the original secret across generations.

5.1 Proposed Scheme

Let $S \in \mathbb{F}_2^\ell$ be the secret. We use the same generation partition as in Section 4:

$$G_g = \{P_t : 2^{g-1} \le t < 2^g\}, \qquad g \ge 1. \tag{30}$$

For $P_t \in G_g$, write

$$g = \lfloor \log_2 t \rfloor + 1, \qquad i = t - 2^{g-1} + 1. \tag{31}$$

Thus $|G_g| = 2^{g-1}$ and $1 \le i \le 2^{g-1}$.

Secret Sharing within Each Generation and ℓ bits share

We use the finite 3-threshold scheme of [**?**, Section 4.1], including its proved correctness and perfect security. To provide sufficiently many distinct evaluation points for the participants in G_g, we use an extension field $\mathbb{F}_{2^{\ell r_g}}$ of $\mathbb{F}_{2^\ell}$. Here r_g is the extension degree, chosen so that the evaluation points allowed by the cited construction suffice for all participants in G_g. Its value is determined in Section 5.3.

Over $\mathbb{F}_{2^{\ell r_g}}$, the cited construction provides $2^{\ell r_g - 1}$ polynomial evaluation evaluation shares and one ℓ-bit short share. We retain 2^{g-1} polynomial evaluation shares at distinct, nonzero evaluation points $\alpha_{g,i}$ allowed by that construction. Denote the retained polynomial evaluation shares by

$$W_{g,1}, \ldots, W_{g,2^{g-1}} \in \mathbb{F}_{2^{\ell r_g}},$$

and the short share by $Q_g \in \mathbb{F}_2^\ell$. The properties needed below are precisely the following:

1. Any three distinct polynomial evaluation shares from G_g recover S.
2. Any two distinct polynomial evaluation shares from G_g, together with Q_g, recover S.
3. For $i \ne j$, the distribution of $(W_{g,i}, W_{g,j})$ is independent of S; the distribution of $(W_{g,i}, Q_g)$ is also independent of S.

These are restrictions of the correctness and perfect security properties proved in [**?**, Section 4.1.2]. The local scheme in every generation shares the same secret S, using independent randomness.

Secret sharing across generations and random mask R.

Choose ℓ independent uniform bits $r_0, \ldots, r_{\ell-1} \in \mathbb{F}_2$, independently of S, and set

$$R = (r_0, \ldots, r_{\ell-1}) \in \mathbb{F}_2^\ell, \qquad R(x) = \sum_{j=0}^{\ell-1} r_j x^j. \tag{32}$$

Thus R is uniform on $\mathbb{F}_2^\ell$; $R(x)$ is its polynomial form.

We share R by the polynomial ring evolving 2-threshold scheme of [**?**]. Let d_g be the length of the Elias δ codeword of g. Write the codeword and its polynomial form as

$$c_g = (c_{g,0}, \ldots, c_{g,d_g-1}), \qquad c_g(x) = \sum_{j=0}^{d_g-1} c_{g,j} x^j.$$

Independently choose uniform bits $a_0, a_1, \ldots \in \mathbb{F}_2$ as they are needed. The g-th share of R is

$$U_g^{(2)} = \left(\sum_{j=0}^{d_g+\ell-2} a_j x^j + R(x) c_g(x) \right) \bmod x^{d_g+\ell-1}. \tag{33}$$

The same coefficients a_j are retained across generations; new coefficients are sampled only when a longer share is required. We identify the resulting polynomial with its coefficient vector. By

the correctness and perfect security of the cited scheme, any two shares with distinct generation indices recover R, whereas a single share $U_g^{(2)}$ is independent of R.

Independently, use the evolving 3-threshold scheme of [**?**, Section 4.2] to share S, and denote its g-th share by $U_g^{(3)}$. Any three shares with distinct generation indices recover S, whereas the joint distribution of any two such shares is independent of S. Here the input index of each outer scheme is g, rather than t.

The random choices in all schemes are mutually independent; the schemes are connected only through the specified inputs S and R. Shares generated by the same evolving scheme need not be independent.

The four components of a share.

For $P_t \in G_g$ with index i within that generation, define

$$\begin{aligned} \mathcal{C}_1 &= U_g^{(3)}, & \mathcal{C}_2 &= W_{g,i}, \\ \mathcal{C}_3 &= Q_g \oplus R, & \mathcal{C}_4 &= U_g^{(2)}. \end{aligned} \tag{34}$$

Here $\oplus$ denotes bitwise XOR on $\mathbb{F}_2^\ell$. The dealer gives P_t the share

$$Z_t = (\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4) = (U_g^{(3)}, W_{g,i}, Q_g \oplus R, U_g^{(2)}). \tag{35}$$

Participants in the same generation receive the same first, third, and fourth components, and different polynomial evaluation local shares in the second component. The short share Q_g depends on the generation; the random mask R is sampled once for the entire scheme.

When the first participant in G_g arrives, the dealer generates $U_g^{(2)}$, $U_g^{(3)}$, and the local polynomial specified by the cited finite scheme, and fixes $Q_g \oplus R$. Each subsequent participant in G_g receives its own evaluation of that polynomial and the same three common components.

5.2 Correctness and Perfect Security

Proof of correctness.

It suffices to consider a set of exactly three participants. There are three possible distributions among generations.

Case 1. The three participants belong to distinct generations.
Let the three participants belong to $G_{g_1}, G_{g_2}, G_{g_3}$, respectively, where g_1, g_2, g_3 are pairwise distinct. The first component of the share held by the participant in G_{g_j} is $U_{g_j}^{(3)}$, for $j = 1, 2, 3$. They therefore obtain

$$U_{g_1}^{(3)}, \qquad U_{g_2}^{(3)}, \qquad U_{g_3}^{(3)}.$$

These are the shares assigned to three distinct generation indices by the evolving 3-threshold scheme of Cheng et al., used to share S across generations. Applying the reconstruction procedure of that scheme to these three shares recovers S.

Case 2. The three participants belong to the same generation.
Suppose all three participants belong to G_g, with pairwise distinct indices i_1, i_2, i_3 within that generation. The second components of their shares are

$$W_{g,i_1}, \qquad W_{g,i_2}, \qquad W_{g,i_3}.$$

These are evaluations of the same polynomial at the distinct points $\alpha_{g,i_1}, \alpha_{g,i_2}, \alpha_{g,i_3}$, generated by the finite 3-threshold scheme of Cheng et al. used to share S within G_g. By the correctness of that finite scheme, any three distinct polynomial evaluation shares recover S. Thus, applying its reconstruction procedure to $W_{g,i_1}, W_{g,i_2}, W_{g,i_3}$ recovers S.

Case 3. Exactly two participants belong to the same generation.
Suppose two participants belong to G_g, with distinct indices i_1, i_2 within that generation, and the third belongs to G_h, where $g \neq h$. The fourth component of each share in G_g is $U_g^{(2)}$, while that of the share in G_h is $U_h^{(2)}$. They therefore obtain

$$U_g^{(2)}, \qquad U_h^{(2)}.$$

These are the shares assigned to two distinct generation indices by the polynomial-ring evolving 2-threshold scheme of Cheng et al., used to share R across generations. Applying its reconstruction procedure to these two shares recovers R.

The third component of each share in G_g is $Q_g \oplus R$. Using the recovered value of R, the participants obtain the short share

$$Q_g = (Q_g \oplus R) \oplus R.$$

The second components of the two shares in G_g provide

$$W_{g,i_1}, \qquad W_{g,i_2}.$$

These are evaluations of the same polynomial at the distinct points α_{g,i_1} and α_{g,i_2}, generated by the finite 3-threshold scheme of Cheng et al. used to share S within G_g. By the correctness of that finite scheme, two distinct polynomial evaluation shares together with its short share recover S. Thus, applying its reconstruction procedure to $W_{g,i_1}, W_{g,i_2}, Q_g$ recovers S. The argument requires only $g \neq h$ and applies regardless of the order of the two generations.

Every set of three participants falls into one of the three cases above and can therefore recover S. Since every set of at least three participants contains a subset of exactly three participants, the scheme satisfies correctness.

Proof of perfect security.

It suffices to consider any two distinct participants. We distinguish whether they belong to the same generation or different generations.

Case 1. The two participants belong to the same generation.
Let their local indices be $i \neq j$ in G_g. Their four components provide

$\mathcal{C}_1$	$U_g^{(3)}$
$\mathcal{C}_2$	$W_{g,i},\ W_{g,j}$
$\mathcal{C}_3$	$Q_g \oplus R$
$\mathcal{C}_4$	$U_g^{(2)}$

The first component contains only one share of the evolving 3-threshold scheme, and the second contains only two polynomial evaluation shares of the same local scheme. Each of these two groups has a distribution independent of S.

The fourth component contains only one share of R. By the perfect security of the evolving 2-threshold scheme, R remains uniform when this share is fixed. The random mask and its sharing randomness are independent of the local scheme and the evolving 3-threshold scheme. Consequently, even after fixing S, $U_g^{(2)}$, $U_g^{(3)}$, and all local shares, $Q_g \oplus R$ is uniform on $\mathbb{F}_2^\ell$. Thus the third component is a uniform string independent of the other components and S.

For any fixed S, the first, second, and fourth components use independent randomness, and each has a distribution independent of S. Their joint distribution, together with the independent uniform third component, is therefore independent of S.

Case 2. The two participants belong to different generations.
Let their generations be G_g and G_h, where $g \neq h$, and let their local indices be i and j. Their components provide

$$\begin{array}{c|c} \mathcal{C}_1 & U_g^{(3)},\ U_h^{(3)} \\ \mathcal{C}_2 & W_{g,i},\ W_{h,j} \\ \mathcal{C}_3 & Q_g \oplus R,\ Q_h \oplus R \\ \mathcal{C}_4 & U_g^{(2)},\ U_h^{(2)} \end{array}$$

The two shares in the fourth component recover R. The participants can therefore obtain

$$Q_g = (Q_g \oplus R) \oplus R, \qquad Q_h = (Q_h \oplus R) \oplus R.$$

Their complete information can equivalently be written as the following four groups:

$$(U_g^{(3)}, U_h^{(3)}), \qquad (W_{g,i}, Q_g), \qquad (W_{h,j}, Q_h), \qquad (U_g^{(2)}, U_h^{(2)}).$$

The first group consists of two shares of the evolving 3-threshold scheme, so its distribution is independent of S. The second and third groups each consist of one polynomial evaluation share and the short share of a local scheme. Their distributions are independent of S by the cited local perfect security property. The last group shares a random mask chosen independently of S, and is also independent of S.

For any fixed S, these four groups use mutually independent randomness. Since each group's distribution is independent of S, their joint distribution is independent of S as well. Thus the two participants obtain no information about S, even though they can recover R.

Both cases satisfy perfect security. Security for a single participant follows by considering a pair containing that participant.

5.3 Analysis of Share Size

Let L_t denote the bit length of Z_t, and let $L_t^{(j)}$ denote the length of its component $\mathcal{C}_j$, for $1 \leq j \leq 4$. For $P_t \in G_g$, where $g = \lfloor \log_2 t \rfloor + 1$, we have

$$L_t = L_t^{(1)} + L_t^{(2)} + L_t^{(3)} + L_t^{(4)}. \tag{36}$$

We first determine the extension degree r_g. The cited finite scheme has $2^{\ell r_g - 1} - 1$ admissible nonzero evaluation points. To assign one to each participant in G_g, it suffices that

$$2^{\ell r_g - 1} - 1 \geq 2^{g-1}.$$

We therefore choose

$$r_g = \left\lceil \frac{g+1}{\ell} \right\rceil, \tag{37}$$

which gives

$$2^{\ell r_g - 1} - 1 \geq 2^g - 1 \geq 2^{g-1}.$$

The polynomial evaluation local share occupies ℓr_g bits, while $Q_g \oplus R$ occupies ℓ bits. Hence

$$L_t^{(2)} = \ell \left\lceil \frac{g+1}{\ell} \right\rceil, \qquad L_t^{(3)} = \ell. \tag{38}$$

For the fourth component, the Elias δ code instantiation of [**?**] gives

$$L_t^{(4)} = d_g + \ell - 1 = \ell + \lfloor \log_2 g \rfloor + 2 \left\lfloor \log_2 \left(\lfloor \log_2 g \rfloor + 1 \right) \right\rfloor. \tag{39}$$

Using the share-size bound in [**?**, Section 4.2], we obtain

$$h = \max\left\{1, \left\lceil \sqrt{\log_2 g} \right\rceil \right\}. \tag{40}$$

This is the generation index used internally by that scheme across generations. Its current generation has at most 2^{h^2} participants, so a local extension degree $\lceil (h^2+1)/\ell \rceil$ suffices. Its short shares, masked copies, and random string together contribute $(2h-1)\ell$ bits. Its own polynomial ring 3-threshold share has length at most

$$\ell + 2\lfloor \log_2 h \rfloor + 4\left\lfloor \log_2\left(\lfloor \log_2 h \rfloor + 1\right)\right\rfloor.$$

Adding these contributions gives

$$\begin{aligned} L_t^{(1)} \le \ell \left\lceil \frac{h^2+1}{\ell} \right\rceil + 2h\ell + 2\lfloor \log_2 h \rfloor \\ + 4\left\lfloor \log_2\left(\lfloor \log_2 h \rfloor + 1\right)\right\rfloor. \end{aligned} \tag{41}$$

Consequently, for every $t \ge 1$, the complete share length satisfies

$$\boxed{\begin{aligned} L_t \le \ell \left\lceil \frac{g+1}{\ell} \right\rceil + \ell \left\lceil \frac{h^2+1}{\ell} \right\rceil + 2\ell(h+1) + \lfloor \log_2 g \rfloor \\ + 2\left\lfloor \log_2\left(\lfloor \log_2 g \rfloor + 1\right)\right\rfloor + 2\lfloor \log_2 h \rfloor \\ + 4\left\lfloor \log_2\left(\lfloor \log_2 h \rfloor + 1\right)\right\rfloor, \end{aligned}} \tag{42}$$

where g and h are given by (31) and (40), respectively.

To express the asymptotic improvement, observe that

$$\ell \left\lceil \frac{g+1}{\ell} \right\rceil \le g + \ell, \qquad \ell \left\lceil \frac{h^2+1}{\ell} \right\rceil \le h^2 + \ell.$$

As $g \to \infty$, we have $h \le \sqrt{\log_2 g} + 1$. Therefore,

$$L_t \le g + 2\log_2 g + 2(\ell+1)\sqrt{\log_2 g} + O(\log_2 \log_2 g + \ell). \tag{43}$$

Using $g = \lfloor \log_2 t \rfloor + 1$, we obtain,

$$\boxed{\begin{aligned} L_t \le\ & \log_2 t + 2\log_2 \log_2 t + 2(\ell+1)\sqrt{\log_2 \log_2 t} \\ & + O(\log_2 \log_2 \log_2 t + \ell). \end{aligned}} \tag{44}$$

In particular, for fixed ℓ, this is

$$L_t \le \log_2 t + (2 + o(1)) \log_2 \log_2 t. \tag{45}$$

This improves the lower-order terms compared with the construction of prior work.

6 Conclusion

We presented a polynomial secret sharing method for two adjacent thresholds and applied it to evolving secret sharing. By sharing two secrets with adjacent recovery thresholds through a single polynomial, we reduce the number of polynomial evaluations stored by each participant. Combined with the evolving k-threshold scheme of Cheng et al. [4], this yields

$$L_t \le \left\lfloor \frac{k}{2} \right\rfloor \log_2 t + O_k(\ell + \log_2 \log_2 t).$$

For fixed k and ℓ, the coefficient of the leading term is reduced from $k-1$ to $\lfloor k/2 \rfloor$. The scheme preserves correctness and perfect secrecy.

For threshold three, we further reduced the lower-order terms by using a single random ℓ-bit mask across all generations and sharing this random mask through an evolving 2-threshold scheme. For fixed ℓ, the resulting share-size bound is

$$L_t \leq \log_2 t + (2 + o(1)) \log_2 \log_2 t.$$

Compared with the previous 3-threshold construction, this reduces the additional share length beyond $\log_2 t$ from order $\sqrt{\log_2 t}$ to order $\log_2 \log_2 t$, while retaining perfect secrecy. The following two questions remain open for future research:

(1) Can our method be extended to share three secrets with consecutive recovery thresholds k, $k+1$, and $k+2$ through a single polynomial, while preserving correctness and perfect secrecy at each threshold? If so, can this further reduce the share size of evolving secret sharing schemes?

(2) Is the share-size upper bound of our evolving 3-threshold scheme optimal? If not, can an evolving 3-threshold scheme with perfect secrecy achieve a smaller share size?

References

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

[2] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the 1979 AFIPS National Computer Conference*, volume 48, pages 313–317. AFIPS Press, 1979.

[3] Ilan Komargodski, Moni Naor, and Eylon Yogev. How to Share a Secret, Infinitely. In Michael Hirt and Adam Smith, editors, *Theory of Cryptography—TCC 2016-B, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 485–514. Springer, 2016. https://doi.org/10.1007/978-3-662-53644-5_19.

[4] Qi Cheng, Hongru Cao, Sian-Jheng Lin, Nenghai Yu, Yunghsiang S. Han, and Xianhong Xie. A Construction of Evolving k-Threshold Secret Sharing Scheme over A Polynomial Ring. In Goichiro Hanaoka and Bo-Yin Yang, editors, *Advances in Cryptology—ASIACRYPT 2025, Part VIII*, volume 16252 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2026. https://doi.org/10.1007/978-981-95-5125-5_1.

[5] Peter Elias. 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.

[6] Qi Cheng, Hongru Cao, Leilei Yu, and Sian-Jheng Lin. A construction of evolving 3-threshold secret sharing scheme with perfect security and smaller share size. *Designs, Codes and Cryptography*, 94, Article 128, 2026. https://doi.org/10.1007/s10623-026-01864-4.

[7] P. D'Arco, R. De Prisco, and A. De Santis. On the equivalence of 2-threshold secret sharing schemes and prefix codes. In *Cyberspace Safety and Security (CSS 2018)*, volume 11161 of *Lecture Notes in Computer Science*, pages 157–167. Springer, 2018.

[8] R. Okamura and H. Koga. New constructions of an evolving 2-threshold scheme based on binary or D-ary prefix codes. In *2020 International Symposium on Information Theory and Its Applications (ISITA)*, pages 432–436, 2020.

[9] C. Xing and C. Yuan. Evolving secret sharing schemes based on polynomial evaluations and algebraic geometry codes. *IEEE Transactions on Information Theory*, 70(5):3718–3728, 2024.

[10] P. D'Arco, R. De Prisco, and A. De Santis. Secret sharing schemes for infinite sets of participants: A new design technique. *Theoretical Computer Science*, 859:149–161, 2021.