Revisiting Shamir Secret Sharing for Threshold Fully Homomorphic Encryption

Jiseung Kim
Jeonbuk National University
Jeonju, Republic of Korea
jiseungkim@jbnu.ac.kr

Seunghu Kim
Chung-Ang University
Seoul, Republic of Korea
rlatmdgn77@cau.ac.kr

Hyung Tae Lee*
Chung-Ang University
Seoul, Republic of Korea
hyungtaelee@cau.ac.kr

Abstract

Recent advances in lattice-based threshold cryptography, including threshold fully homomorphic encryption (ThFHE) and threshold public key encryption (ThPKE), commonly employ Shamir secret sharing over rings. While conceptually simple, these schemes suffer from rapidly growing denominator-clearing factors required for secret reconstruction as the number of parties N increases, which in turn necessitates larger ciphertext moduli and complex reconstruction procedures.

In this work, we revisit the notion of *subtractive sets* underlying ring-based Shamir secret sharing and present a refined framework for constructing integer-reconstructible sharing over cyclotomic rings. To that end, we introduce a new geometric analysis of Lagrange coefficients and show that the resulting reconstruction factors can be made significantly smaller under specific settings. In particular, our framework enables smaller ciphertext sizes in (t, N)-threshold settings, and yields improved correctness and efficiency when applied to any ring-based threshold construction employing Shamir secret sharing over cyclotomic rings. Specifically, in lattice-based one-round (t, N)-ThFHE schemes, our approach reduces the bit-size of ciphertext moduli from $O(N)$ to $O(t \log(N/t^2))$ while ensuring efficient denominator handling. For lattice-based ThPKE, our method yields a new bound on reconstruction factors that improves upon the recent state-of-the-art result of Pilvi. Moreover, we implement ThFHE schemes over cyclotomic rings based on our framework and demonstrate their practical efficiency. Our experimental results show that each algorithm completes within 0.2 seconds for $N = 64$ and remains scalable for larger configurations with $N \geq 256$.

CCS Concepts

• **Security and privacy → Cryptography**.

Keywords

Shamir secret sharing, threshold fully homomorphic encryption, subtractive sets, geometric analysis

1 Introduction

Threshold cryptography [25, 27, 30] distributes a secret key among multiple parties so that no single party can perform cryptographic operations that require access to the secret key. This paradigm has become a cornerstone of modern distributed security and has led to a wide variety of cryptographic primitives, including threshold public-key encryption (ThPKE) [8, 23, 38, 39], threshold signatures [4, 10, 12, 17, 26, 34], and threshold fully homomorphic encryption (ThFHE) [6, 13, 15, 19, 22, 36, 40–42, 49]. Among these, ThFHE has recently emerged as a fundamental tool for secure distributed computation. By combining homomorphic evaluation with threshold access control, it enables encrypted data to be processed collaboratively without revealing the underlying secret key. This capability has established ThFHE as a central cryptographic primitive supporting privacy-preserving applications such as federated learning [29, 32, 35, 43, 47] and collaborative data analytics [31, 46, 48].

Limitation of Classical Shamir SSS. A straightforward approach to constructing a ThFHE scheme is to apply the Shamir secret sharing scheme (SSS) to distribute shares of the secret key from a traditional fully homomorphic encryption (FHE) scheme among multiple parties. However, this approach faces a fundamental incompatibility: the classical Shamir SSS is defined over a finite field, whereas most efficient FHE schemes are defined over a polynomial ring, such as $R_Q = \mathbb{Z}_Q[X]/(X^n + 1)$. Consequently, a direct adaptation of Shamir SSS to the ring setting requires introducing a *denominator-clearing factor* Δ to eliminate the fractional terms that appear in the Lagrange coefficients. For the classical Shamir SSS, this factor must simultaneously clear all possible denominators arising from every $\binom{N}{t}$ reconstruction subset, resulting in an exponentially growing value, typically $\Delta = (N!)^2$ [3, 11, 45]. Such a large Δ forces the ciphertext modulus Q to increase proportionally, requiring roughly $O(N \log_2 N)$ bits to preserve correctness. This, in turn, becomes a major bottleneck for large-scale threshold systems.

Existing Approaches for ThFHE. To overcome this bottleneck, recent polynomial ring-based threshold systems, including ThFHE, have explored several design strategies that differ in their protocol-level assumptions, particularly in whether decryption operates in a synchronous or fully asynchronous setting.

(i) Asynchronous decryptable schemes. This class of schemes [11, 13, 15, 18, 19, 24] targets the most robust and practical setting, where decryption proceeds asynchronously so that each party produces a single partial decryption message without further interaction. Such a model *requires* the use of a ring-compatible linear secret sharing scheme (LSSS), since the specific t-subset T of responding parties is not known in advance. As a result, correctness cannot rely on additional communication rounds and must instead be ensured through the algebraic structure of the LSSS itself. This is achieved, for example, by tightly bounding the denominator-clearing factor Δ and the geometric norms of the reconstruction coefficients $\lambda_i^{(T)}$. This coefficient-controlled design, adopted by Boneh et al. [11], Brakerski et al. [15], and others [13, 18, 19, 24], directly ties correctness to numerical stability: small reconstruction coefficients not only bound the decryption error term $\sum \lambda_i^{(T)} e_i$ but also reduce the overall ciphertext modulus and size.

*Corresponding author

(ii) Synchronous decryption systems. Another line of research relaxes the asynchronous requirement in order to better control noise. This class includes synchronous schemes that assume a *fixed*, predetermined set T of parties. Such an assumption enables simpler additive secret sharing or precomputation of the Lagrange coefficient $\lambda_i^{(T)}$, but it is not resilient to unpredictable party dropouts. It also encompasses *multi-round* protocols [26, 36, 38–40, 49], which *decompose* the reconstruction process into several interactive linear steps. This design helps keep per-round noise growth small, though at the cost of additional protocol complexity and communication overhead, which single-round schemes can avoid.

Adoption of Asynchronous Decryption. While both synchronous and asynchronous threshold decryption models have been studied in prior work, synchronous designs remain limited in practicality because they depend on fixed participant sets or require multiple rounds of interaction. These constraints reduce robustness and hinder scalability in dynamic or partially available environments. In this work, we focus on the *asynchronous* setting, which enables any t-out-of-N subset of parties to complete decryption independently and without coordination. Our approach builds upon the Shamir SSS adapted to polynomial rings, while introducing an improved analysis that dramatically reduces the denominator-clearing factor. This improvement directly translates into smaller reconstruction errors, reduced ciphertext modulus requirements, and more compact ciphertexts, which result in a more efficient and scalable design for ThFHE.

1.1 Our Contributions

In this paper, we revisit the Shamir SSS and introduce a refined variant over polynomial rings that serves as a generic tool for improving ring-based threshold constructions: it is fully compatible with existing ring-based ThFHE and ThPKE constructions (Section 3). We then provide a detailed theoretical analysis of the resulting denominator-clearing factors and reconstruction errors, establishing tighter bounds than in prior work (Section 3). Building on this foundation, we integrate the refined scheme into ThFHE (Section 4). Finally, we present a comparative evaluation between our refined Shamir SSS and prior constructions when applied to ThFHE, demonstrating clear improvements in both efficiency and parameter sizes (Section 5).

We next elaborate on our main contributions. At a high level, our work comprises three complementary components: (i) a new geometric *analysis* of Lagrange coefficients over cyclotomic rings that yields tighter bounds on the recovery-expansion factor (Section 3); (ii) concrete *instantiations* of lattice-based ThFHE and ThPKE with improved parameters derived from these bounds (Section 4); and (iii) an *integration* of the refined SSS into existing frameworks [11, 15] with a full implementation and experimental evaluation (Section 5).

Refined Shamir SSS over Polynomial Rings. We revisit the analytic bottleneck of Shamir secret sharing when instantiated over polynomial rings, which is a critical subroutine in ring-based ThFHE. Our goal is to tightly control the worst-case growth of Lagrange coefficients induced by the choice of evaluation points. To this end, we exploit the geometric structure of evaluation points on the unit circle, specifically the M-th roots of unity with $M = 2^{\lceil \log_2 N \rceil}$ for a t-out-of-N threshold scheme.

Formally, we consider a *subtractive set* $S = \{\alpha_1, \ldots, \alpha_N\}$ together with a denominator-clearing factor $\Delta(t)$ such that $\Delta(t) \cdot v(x_0)^\top V_T^{-1}$ has coefficients in the underlying ring. Here, V_T denotes the row-style Vandermonde matrix over $T \subseteq S$, where $V_T[\alpha, :] = (1, \alpha, \ldots, \alpha^{t-1})$, and $v(x_0)^\top = (1, x_0, \ldots, x_0^{t-1})$. As [5], we quantify the quality of the evaluation set S via the recovery-expansion factor

$$\rho_{x_0}(t) := \max_{T \subseteq S,\ |T|=t} \left\| \Delta(t) \cdot v(x_0)^\top V_T^{-1} \right\|.$$

Primal Analysis. Prior works [5, 23, 37] derive bounds that scale with the ring dimension. In contrast, our geometric analysis yields bounds that depend only on (N, t) (via M), and reveals an explicit factorial gain. For reconstruction at $x_0 = 0$, letting $\tilde{t} = \lfloor (t-1)/2 \rfloor$, we obtain

$$\rho_0(t) \ \le\ \Delta(t) \cdot \prod_{r=1}^{\tilde{t}} \frac{1}{\sin^2\left(\pi r / M\right)} \ \le\ \frac{\Delta(t)}{(\tilde{t}!)^2} \left(\frac{M}{2}\right)^{t-1}.$$

Dual Analysis. When t approaches N, primal bounds alone may become loose. To address this regime, we introduce a complementary *dual analysis* based on a structural identity that relates the Lagrange coefficients over a reconstruction set T to those over the full set S and a multiplicative correction over the missing set $U := S \setminus T$ of size $k := N - t$. This perspective yields improved worst-case control governed by the number of missing parties rather than the threshold size. For reconstruction at $x_0 = 0$, defining $L_S(0) := \max_{j \in S} \left\| \lambda_j^{(S)}(0) \right\|_\infty$, we derive the combined guarantee

$$\rho_0(t) \ \le\ \Delta(t) \cdot t \cdot \min\left(\left(\frac{M}{2}\right)^{t-1} \frac{1}{(\tilde{t}!)^2},\ 2^{N-t} L_S(0) \right).$$

Furthermore, we prove that $L_S(0) \le \frac{2^{M-N}}{M}$, implying $2^{N-t} L_S(0) \le 2^{M-t}/M$. Overall, this primal-dual viewpoint yields a refined Shamir SSS whose worst-case reconstruction growth is governed by the better of a t-driven primal geometric bound and a $(N-t)$-driven dual bound. As a result, our scheme supports significantly tighter choices across both low- and high-threshold regimes.

Application to ThFHE. We instantiate our improved bounds within the ThFHE framework of [11, 15]. Our refinement applies to arbitrary t-out-of-N ThFHE constructions and significantly improves parameter efficiency. Asymptotically, we achieve $\log_2 Q = O(\log_2 N)$ for $t = O(1)$ and $\log_2 Q = \Theta((\log_2 N)^2)$ for $t = \Theta(\log_2 N)$, while preserving N decryption shares. In contrast, prior constructions require $\log_2 Q = O(\log_2 N)$ [11] or $\log_2 Q = O(N)$ [15] with N decryption shares, and achieving $\log_2 Q = O(\log_2 N)$ previously necessitated a dramatically large number of keys per party (e.g., $N^{4.3}$ keys in [19]).

Concrete estimates (Table 2) confirm substantial savings across both low- and high-threshold regimes. For example, when $N = 64$, ciphertext sizes are reduced by about 107×–290× compared to [11], depending on t. Relative to [15], our refined Shamir SSS consistently improves performance; e.g., for $(N, t) = (512, 5)$, the ciphertext size drops from 1933.31 KB to 104.45 KB (about 18.5×), and even for $(512, 341)$ it is reduced by about 2.9×.

We further validate these gains through an implementation of [11] instantiated with our refined SSS—the first concrete ThFHE implementation supporting one-round asynchronous decryption,

to the best of our knowledge. For instance, at $(N, t) = (64, 6)$, reducing $(n, \log_2 Q)$ from $(2^{16}, 1200)$ to $(2^{12}, 72)$ leads to speedups of about 758× for Setup, 102× for Enc, 47× for PartDec, and 18× for FinDec over [11]. Unlike the classical Shamir-based instantiation of [11], which becomes impractical due to prohibitive runtime for $N \geq 128$, our scheme remains practical even for large N and high thresholds, including $(N, t) = (512, 256)$ and $(512, 341)$.

We additionally compare our one-round ThFHE with the two-round approximate secret sharing-based construction of [18]. While a two-round protocol may naturally be expected to offer better concrete performance due to its smaller noise allowance, our experiments show that, across a range of practically relevant threshold settings, the refined Shamir SSS achieves competitive—and in some cases improved–efficiency, primarily as a result of the reduced modulus and ring dimension. For example, when measuring the combined decryption cost (per-party partial decryption plus final aggregation), our construction attains speedups of approximately 7.4× and 2.9× for $(N, t) = (256, 8)$ and $(256, 170)$, respectively, compared to [18].

Application to ThPKE. Our improved primal-dual analysis is also directly applied to the recent lattice-based ThPKE construction of [23], whose ciphertext modulus depends on the recovery-expansion factor $\rho(t)$. Compared with the worst-case bound underlying [23], our primal estimate satisfies

$$\frac{\rho^{\text{primal}}_{\text{ours}}(t)}{\rho_{\text{Pilvi}}(t)} \lesssim \frac{2^{(t-1)/2}}{t(\tilde{t}!)^2} \cdot \left(\frac{M}{n}\right)^{t-1},$$

which is strictly smaller than 1 and decreases rapidly as t grows for ring dimension $n \geq M$. Substituting our bound into the correctness condition of [23] yields a strictly smaller sufficient ciphertext modulus. For example, with $n = 2^{13}$ and $(N, t) = (64, 21)$, the ratio $(M/n)^{t-1}$ alone contributes a factor of 2^{-20}, which translates to approximately 20 fewer bits in $\log_2 Q$. Moreover, for large thresholds, the dual term dominates the primal term, yielding an even smaller ciphertext modulus.

2 Preliminaries

In this section, we introduce background that will be helpful for understanding our proposed scheme and its applications.

Notations. Let n be a power of two, and let K denote the $2n$-th cyclotomic field of degree n. We denote by R its ring of integers, that is, $R = \mathbb{Z}[X]/(X^n + 1)$. For any integer $q \geq 2$, we write $R_q = R/qR$.

For $a, b \in \mathbb{Z}$, the notation $a \mid b$ indicates that a divides b. For any positive integer a, let $[a]$ denote the set $\{1, 2, \ldots, a\}$. When S is a set, $|S|$ denotes the cardinality of S.

Canonical Embedding and Norms. Let $n = 2^m$ be a power of two, and let ζ denote a primitive $2n$-th root of unity. We define the canonical embedding $\sigma : R \to \mathbb{C}^n$ by $\sigma(g) := \left(g(\zeta^{2j+1})\right)_{j=0}^{n-1}$. We define the Euclidean and supremum norms on the image of σ: $\|g\|_2 := \|\sigma(g)\|_2$ and $\|g\|_\infty := \|\sigma(g)\|_\infty$. We usually omit the subscript 2 for simplicity. We adopt the following conventions for vectors and matrices over R: 1) A vector $v = (v_1, \ldots, v_k) \in R^k$ has Euclidean norm $\|v\|_2^2 = \sum_i \|v_i\|_2^2$, 2) A real or complex matrix A has *spectral norm* $\|A\|$, defined as its largest singular value, and *Frobenius norm* $\|A\|_F = \sqrt{\sum_{i,j} |A_{i,j}|^2}$. These norms satisfy the standard inequality $\|A\| \leq \|A\|_F$, with equality holding only when all singular values of A are equal.

2.1 Subtractive Sets

We revisit the concept of subtractive sets, a foundational notation introduced by Albrecht and Lai [5] and further developed in subsequent works such as [37]. This framework has become a key tool for constructing threshold primitives in lattice-based cryptography.

Definition 2.1 (Subtractive Sets [5]). *Let R be a ring and $S = \{\alpha_1, \ldots, \alpha_N\} \subset R$ a finite set. For any $t \leq N$ and any subset $T \subset S \cup \{0\}$, define V_T as the row-style Vandermonde matrix constructed from the elements of T. The rows of V_T are indexed by $\alpha \in T$, where each row vector is given by $(1, \alpha, \ldots, \alpha^{t-1})$.*

We say that S is Δ-subtractive if for every $t \in [N]$ and every t-subset $T \subset S$, it holds that $\Delta V_T^{-1} \in R^{t \times t}$. To evaluate the quality of S, the following auxiliary metrics are introduced:

- *Recovery-expansion factor $\rho(t) := \max_{T \subset_t S} \|\Delta \cdot v_0^\top \cdot V_T^{-1}\|$ where $v_0^\top$ denotes the row vector indexed by the element 0.*
- *Inverse-expansion factor $\gamma(t) := \max_{T^* \subset_{t-1} S} \|\Delta \cdot V_S \cdot V^{-1}_{\{0\} \cup T^*}\|$.*

Here, the notation $T \subset_t S$ indicates that T is a subset of S with $|T| = t$.

The Vandermonde matrix V_S coincides with the share-generating matrix of the t-out-of-N Shamir SSS, where the evaluation points are taken from S.

Lemma 2.2 (Adapted from [5, Theorem 1]). *Let $R = \mathbb{Z}[\zeta]$ be the cyclotomic ring with power-of-two conductor $n = 2^k$. Then, the canonical set $\{1, \zeta, \ldots, \zeta^{n-1}\}$ is Δ-subtractive with the slack factor $\Delta(t) = 2^{\lceil \log_2 t \rceil}$.*

This lemma implies that for any distinct exponents $i \neq j$, the element $\Delta \cdot (\zeta^i - \zeta^j)^{-1}$ lies in R.

2.2 Shamir Secret Sharing over R

In this subsection, we review the Shamir SSS defined over R. For simplicity, we assume that the Lagrange coefficients are well-defined in R. Since ensuring this property is often nontrivial, a subtractive set can be employed to guarantee the well-definedness of the Lagrange coefficients [5, 15].

Throughout this paper, we restrict our attention to the classical *t-out-of-N* threshold access structure, where any subset of at least t parties can jointly perform reconstruction, while any set of fewer than t learns nothing about the secret. Let $P = \{P_1, \ldots, P_N\}$ denote the set of parties and let $\mathbb{A}$ be the corresponding access structure consisting of all subsets of P with cardinality greater than or equal to t.

Let $R[Y]_{<t}$ be the set of polynomials over R in the variable Y of degree less than t. Fix a public set of N distinct evaluation points (subtractive set) $S = \{\alpha_1, \alpha_2, \ldots, \alpha_N\} \subset R$, where each α_i is assigned to a party P_i for $1 \leq i \leq N$. A (t, N)-threshold Shamir SSS for sharing a secret $s \in R$ consists of the following algorithms:

- **Share Generation** (ShareGen): The dealer samples a random polynomial $f(Y) = \sum_{j=0}^{t-1} f_j Y^j \in R[Y]_{<t}$ such that $f(0) = s$. Each party P_i receives the share $s_i = f(\alpha_i)$.

- **Reconstruction** (Reconstruct): Any subset $T \subset \{\alpha_1, \ldots, \alpha_N\}$ with cardinality at least t can recover the secret s by Lagrange interpolation $s = \sum_{\alpha_i \in T} \lambda_i^{(T)}(0) \cdot s_i$, where $\lambda_i^{(T)}(Y) = \prod_{\alpha_j \neq \alpha_i \in T} \frac{Y - \alpha_j}{\alpha_i - \alpha_j}$. Here, $\lambda_i^{(T)}(Y)$ is called the Lagrange basis polynomial, and $\lambda_i^{(T)}(z)$ is referred to as the Lagrange coefficient at point z.

We omit the details of correctness and privacy, since they are identical to those of the classical Shamir SSS.

2.3 Threshold Fully Homomorphic Encryption

Next, we define the notion of ThFHE schemes, which serve as the primary application of our refined secret sharing framework. (Definitions of standard FHE schemes appear in Appendix A.)

Let $P = \{P_1, P_2, \cdots, P_N\}$ be a set of parties and $\mathcal{S}$ be a class of efficient access structures on P. A ThFHE scheme for $\mathcal{S}$ consists of five probabilistic polynomial-time (PPT) algorithms, ThFHE = (Setup, Enc, Eval, PartDec, FinDec), defined as follows:

- $\mathsf{Setup}(1^\lambda, 1^d, \mathbb{A})$: Given the security parameter λ, a depth bound d, and an access structure $\mathbb{A}$, it outputs a public key pk and a set of secret keys $\mathsf{sk}_1, \mathsf{sk}_2, \ldots, \mathsf{sk}_N$, where sk_i denotes the secret share associated with party P_i.
- $\mathsf{Enc}(\mathsf{pk}, m)$: Given the public key pk and a plaintext m, it outputs a ciphertext ct.
- $\mathsf{Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k)$: Given the public key pk, a circuit C, and a set of ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_k$, it outputs an evaluated ciphertext ct_{out}.
- $\mathsf{PartDec}(\mathsf{pk}, \mathsf{sk}_i, \mathsf{ct})$: Given the public key pk, a secret key share sk_i, and a ciphertext ct, it outputs a partial decryption share p_i.
- $\mathsf{FinDec}(\mathsf{pk}, \mathsf{ct}, \{\mathsf{p}_i\}_{i \in T})$: Given the public key pk, the ciphertext ct, and a set of partial decryption shares $\{\mathsf{p}_i\}_{i \in T}$ from a qualified subset $T \in \mathbb{A}$, it outputs the plaintext m or an error symbol $\perp$.

The correctness and security definitions are given in Appendix A.

3 Revisiting Subtractive Sets for Shamir Secret Sharing over Cyclotomic Rings

We revisit the notion of subtractive sets [5, 37] in the context of lattice-based threshold cryptography, including ThFHE and ThPKE. Our goal is to reformulate the analysis so that the correctness criterion depends primarily on the *number of parties* N and the threshold t, rather than on the cyclotomic ring dimension n. Concretely, we modify the choice of the subtractive set and adapt the Shamir SSS over finite fields [44] to derive a tight bound on $\sum_{j \in T} \left\| \Delta \lambda_j^{(T)}(0) \right\|$ which is equivalent to the recovery-expansion factor

$$\rho(t) = \max_{T \subset_t S} \| \Delta \cdot v_0^\top \cdot V_T^{-1} \|$$

up to a $\sqrt{t}$ factor. Here, V_T denotes the row-style Vandermonde matrix over $T \subseteq S \cup \{0\}$, with rows $V_T[\alpha, :] = (1, \alpha, \ldots, \alpha^{t-1})$, and $v_{x_0}^\top = (1, x_0, \ldots, x_0^{t-1})$. These bounds, in turn, yield direct control over

$$E = \sum_{j \in T} \left\| \Delta \lambda_j^{(T)}(0) e_j \right\|,$$

where $T \subset [N]$ with $|T| = t$, $\lambda_j^{(T)}$ are the (ring) Lagrange basis polynomials, e_j represents the noise generated in the scheme, and Δ is a denominator-clearing factor. A smaller bound on E directly enables the use of a smaller ciphertext modulus q in lattice-based ThFHE and ThPKE schemes.

Before proceeding, we summarize prior results [5, 11, 15, 23] over the power-of-two cyclotomic ring $R = \mathbb{Z}[X]/(X^n + 1)$.

- In [11], $E \approx N \cdot (N!)^2 \cdot \max \|e_j\|$.
- In [15], $E \approx \frac{N^2}{3n} 2^{\frac{3}{4}N} \cdot \max \|e_j\|$.
- In [5, 23], $E \approx t \cdot 2^{\lceil \log_2 t \rceil} \cdot \left(\frac{n}{2\sqrt{2}}\right)^{t-1} \cdot \max \|e_j\|$.

In contrast, our results achieve

$$E \approx t \cdot 2^{\lceil \log_2 t \rceil} \cdot \min \left\{ \left(\frac{M}{2}\right)^{t-1} \frac{1}{(\tilde{t}!)^2},\ 2^{N-t} L_S(0) \right\} \cdot \max \|e_j\|,$$

where $M = 2^{\lceil \log_2 N \rceil}$ satisfying $M \mid 2n$.

3.1 Refined Shamir Secret Sharing over R

Let q be an odd integer and $N \geq 2$ the number of parties. Throughout this section, we assume that $N \leq n/2$[1], where n denotes the dimension of the cyclotomic ring R. This assumption is reasonable in most application scenarios of our proposed scheme. For example, in the fully homomorphic encryption (FHE) setting, most FHE libraries employ parameters with $n \geq 2^{12}$, and in typical lattice-based public-key encryption schemes, it holds that $n \geq 1000$. Since practical threshold deployments typically involve $N \leq 1024$ parties while lattice parameters require $n \geq 2^{12}$, the condition $N \leq n/2$ is easily satisfied and does not restrict the applicability of our framework. Let $M := 2^{\lceil \log_2 N \rceil}$. Since $2n$ is a power-of-two, it follows that $M \mid 2n$ and we can define

$$\omega := X^{2n/M} \in R.$$

Then ω has exact order M; that is, $\omega^M = 1$ and $\omega^k \neq 1$ for all $0 < k < M$ since X is a $2n$-th root of unity. Based on the set $\{\omega^k\}_{k \in \mathbb{Z}_M}$, we adapt the subtractive set construction [5, 23, 37]. Lemma 3.1 supports the well-definedness of the Lagrange polynomial interpolation, as in prior approaches. Indeed, since 2 is invertible in R_q for odd q, it follows that $(\omega^i - \omega^j)^{-1}$ is also invertible in R_q.

Lemma 3.1 ([9, Lemma 3.1]). *Let n be a power of two and let $0 \leq i, j \leq 2n - 1$. Then, $2(X^i - X^j)^{-1}$ has an inverse in R of the form*

$$1 \pm X^{j \bmod n} \pm X^{2j \bmod n} \pm \cdots \pm X^{(k-1)j \bmod n}$$

where $k = 2^{\log_2 n - j'}$ for $j = 2^{j'} j''$ with a positive odd integer j''.

A formal description of the refined Shamir SSS, defined over the set of evaluation points $\{\omega^k\}_{k \in \mathbb{Z}_M}$, is provided in Figure 1. In contrast to prior constructions, our refinement places particular emphasis on how the evaluation points are selected. To capture this aspect clearly, we introduce a dedicated Setup algorithm that specifies how these points are determined.

Correctness and Privacy. Correctness relies on the well-definedness of Lagrange interpolation over the ring R_q. By Lemma 3.1, for any distinct evaluation points $\alpha_i, \alpha_j \in S$, where S is constructed from ω as in the **Setup** algorithm, their difference $(\alpha_i - \alpha_j)$ is an invertible element (a unit) in R_q. Consequently, for any t-subset $T \subset S$, all

[1] In [15], it is assumed that $N < n$.

Refined Shamir Secret Sharing Scheme over R (Setup / ShareGen / Reconstruct)

Setup(n, q, N, t)

Input: n=2^m, odd q, integers $N < n$, $t \le N$.
Output: $S = \{\alpha_1, \ldots, \alpha_N\} \subset R_q$.

(1) Set $M = 2^{\lceil \log_2 N \rceil}$ such that $M | 2n$.
(2) Compute an M-th root of unity $\omega = X^h$, where $Mh = 2n$.
(3) Build a set $\tilde{S} = \{\omega, \omega^2, \ldots, \omega^M\}$.
(4) Publish a subset $S = \{\alpha_1, \ldots, \alpha_N\} \subset \tilde{S}$ with $|S| = N$.

ShareGen(s, S, t)

Input: a secret $s \in R_q$, a public set S, a threshold t.
Output: shares $\{(y_i, \alpha_i)\}_{i \in [N]}$.

(1) For all $i \in \{1, \ldots, t-1\}$, sample a random element c_i from R_q.
(2) Compute a degree $t-1$ polynomial $h(Y) = c_0 + \cdots + c_{t-1} Y^{t-1} \in R_q[Y]$ with $c_0 = s$.
(3) For all $i \in [N]$, evaluate $y_i = h(\alpha_i)$.
(4) Return $\{(y_i, \alpha_i)\}_{i \in [N]}$.

Reconstruct$(T, \{y_i\}_{i \in T})$

Input: $T \subset [N]$ with $|T| = t$, $\{y_i\}_{i \in T}$
Output: $\hat{s} = h(0)$.

(1) For all $j \in T$, compute $\lambda_j^{(T)}$ using Lemma 3.1.
(2) Compute $\hat{s} = \sum_{j \in T} \lambda_j^{(T)} y_j$.
(3) Return $\hat{s}$.

Figure 1: Refined Shamir Secret Sharing Scheme over R

Lagrange basis polynomials $\lambda_j^{(T)}(Y) = \prod_{i \in T \setminus \{j\}} (Y - \alpha_i)(\alpha_j - \alpha_i)^{-1}$ are well-defined over $R_q[Y]$. Therefore, the correctness and privacy properties are essentially identical to those of the classical Shamir SSS.

Compared to Prior Works. Prior studies [5, 23, 37] employ a subtractive set of the form $\{1, \zeta, \ldots, \zeta^{n-1}\}$, where n is the ring dimension and ζ is a primitive $2n$-th root of unity. Thus, it is natural that the noise bound E depends on n and the threshold t.

In many threshold cryptographic applications, however, the number of parties N is much smaller than the ring dimension n. Our initial observation is therefore to derive an upper bound on E that depends on N rather than on n. To this end, we adopt a smaller subtractive set $\{\omega^{a_1} \ldots, \omega^{a_N}\}$, where ω is a primitive $\frac{2n}{M}$-th root of unity.

The following subsection provides an improved analysis of this additional structure using a geometric perspective on the Lagrange coefficients. This geometric property originates from the fact that all elements of the subtractive set lie on the unit circle. As a consequence, the major difference between our approach and prior works lies not in the choice of the subtractive set itself, but in how the Lagrange coefficients are analyzed.

The work of [15] follows a broadly similar methodology to [5, 23, 37] and ours. However, its instantiation of the evaluation points differs substantially, leading to a distinct denominator-clearing factor Δ.

3.2 Geometric Analysis of Our Refined Shamir SSS

The share generation and reconstruction algorithms of our refined Shamir SSS are purely algebraic. When these are embedded in cryptographic protocols (e.g., threshold decryption), however, the shares may carry small perturbations. To reason about correctness under such perturbations, we require a *minimal analysis* that upper-bounds how much the reconstruction weights can amplify small errors in $\mathbb{C}^n$. In this section, we analyze the smallness of the Lagrange coefficients based on their geometric properties.

More precisely, we will estimate an upper bound on

$$\max_T \sum_{j \in T} \|\Delta \cdot \lambda_j^{(T)}(0)\|$$

in order to tightly set parameters for cryptographic primitives involving a denominator-clearing factor Δ. To this end, we use the relation $\rho(t) \le \max_T \sum_{j \in T} \|\Delta \cdot \lambda_j^{(T)}(0)\| \le \sqrt{t}\rho(t)$, where $\rho(t)$ is a recovery-expansion factor in Definition 2.1.

Our geometric bound relies on the fact that all evaluation points lie on the unit circle ($|\sigma_\ell(\alpha_i)| = 1$). The quantity $\|\Delta \cdot (1, 0, \ldots, 0) \cdot V_T^{-1}\|_\infty$ is determined by the geometric properties of the angles among these points. In particular, the relevant denominators can be expressed as $\prod_{i \ne j} |\sigma_\ell(\alpha_j) - \sigma_\ell(\alpha_i)| = \prod_{i \ne j} |2 \sin(\pi |j - i|/M)|$, which captures the angular separation induced by the M-th roots of unity.

Theorem 3.2. *Let $N \ge 2$ denote the number of parties, and define*

$$M := 2^{\lceil \log_2 N \rceil} \quad \text{and} \quad \omega := X^{2n/M} \in R$$

so that ω has exact order M. Let I_t be an index set of size t, where $2 \le t \le N$. For each $i \in I_t$, fix a distinct exponent $b_i \in \mathbb{Z}_M$ and define the interpolation nodes $\alpha_i := \omega^{b_i} \in R$. Let V_T denote the row-style Vandermonde matrix associated with the set $T = \{\alpha_{i_1}, \ldots, \alpha_{i_t}\}$ for indices $i_j \in I_t$. Then, for $\Delta = 2^{\lceil \log_2 \tilde{t} \rceil}$, $\|\Delta \cdot (1, 0, \ldots, 0) \cdot V_T^{-1}\|_\infty$ is bounded by

$$\Delta \prod_{r=1}^{\tilde{t}} \frac{1}{\sin^2(\pi r/M)} \le \Delta \cdot \left(\frac{M}{2}\right)^{t-1} \cdot \frac{1}{(\tilde{t}!)^2},$$

where $\tilde{t} = \lfloor \frac{t-1}{2} \rfloor$.

Proof. By Lemma 2.2, it holds that $\Delta \lambda_j^{(T)} \in R$. To establish the bound, we divide the analysis by two cases, since the geometric structure of the denominator-minimizing set changes fundamentally depending on t. We prove the main case $t \ge 3$ here, and defer the proof for $t = 2$ to Appendix B due to the space limitation.

Suppose $t \ge 3$. Let $\sigma_\ell : K \to \mathbb{C}$ be the canonical embedding that maps X to $X^{2\ell+1}$, and let V be the Vandermonde matrix associated with the set $\{\alpha_{i_1}, \ldots, \alpha_{i_t}\} \subset K$. Let $\sigma_\ell(V^{-1})$ be the matrix defined

by applying σ_ℓ on V^{-1} entry-wise. By [33, Thm. 3.1], it holds that

$$\|\sigma_\ell(V^{-1})\|_\infty \le \max_{j\in[t]} \prod_{i\in[t],i\neq j} \frac{1+|\sigma_\ell(\alpha_i)|}{|\sigma_\ell(\alpha_i-\alpha_j)|}.$$

Without loss of generality, fix $j \in I_t$. Write $I_t = \{k_0, k_1, \dots, k_{t-1}\}$ with $k_0 = j$. For each $i \in I_t \setminus \{j\}$ define the cyclic distance

$$d(i) := \min\big(|b_i - b_j|, M - |b_i - b_j|\big) \in \{1, 2, \dots, \lfloor M/2 \rfloor\}.$$

Geometrically, $d(i)$ is the shorter arc length on the regular M-gon from $\alpha_j = \omega^{b_j}$ to $\alpha_i = \omega^{b_i}$.

A crucial observation is that for each positive integer r, there are at most two indices $i \in I_t \setminus \{j\}$ such that $d(i) = r$: one may lie r steps clockwise from j, and another r steps counterclockwise, but no more. Hence, if we list the multiset

$$\mathcal{D} := \{d(i) : i \in T \setminus \{j\}\},$$

then for every $r \ge 1$,

$$\#\{d \in \mathcal{D} : d = r\} \le 2.$$

Thus, we obtain

$$|\alpha_j - \alpha_i| = |\omega^{b_j} - \omega^{b_i}| = |\omega^{b_j - b_i} - 1| = 2\big|\sin(\pi d(i)/M)\big|.$$

Similarly, to analyze $\sigma_\ell(\alpha_j - \alpha_i)$, we define the cyclic distance

$$d_\ell(i) := \min\big(c_\ell(i) \bmod M, M - c_\ell(i) \bmod M\big).$$

where $c_\ell(i) = |(2\ell+1)(b_i - b_j)|$. Then, for all ℓ, it holds that

$$|\sigma_\ell(\alpha_j - \alpha_i)| = 2\big|\sin(\pi d_\ell(i)/M)\big|.$$

On the other hand, since all α_i lie on the unit circle, we have $1 + |\sigma_\ell(\alpha)| \le 2$.

Now define a multiset $\mathcal{D}_\ell = \{d_\ell(i) : i \in I_t \setminus \{j\}\}$ and order it nondecreasingly. Because each positive integer can appear at most twice, we can write

$$\mathcal{D}_\ell \subset \{1, 1, 2, 2, 3, 3, \dots\}$$

taking as many terms from the left as needed to obtain $t-1$ elements. More precisely, if $t - 1 = 2\tilde{t}$ is even,

$$\mathcal{D}_\ell \text{ is dominated term-wise by } \{1, 1, 2, 2, \dots, \tilde{t}, \tilde{t}\},$$

and if $t - 1 = 2\tilde{t} + 1$ is odd, then

$$\mathcal{D}_\ell \text{ is dominated term-wise by } \{1, 1, 2, 2, \dots, \tilde{t}, \tilde{t}, \tilde{t} + 1\}.$$

Since $x \mapsto 1/\sin(\pi x/M)$ is non-increasing for $x \in \{1, 2, \dots, \lfloor M/2 \rfloor\}$, replacing each $d_\ell(i)$ by a smaller integer can only make the product larger. Hence it suffices to bound the worst-case (i.e. smallest-distance) pattern, namely

$$\prod_{r=1}^{\tilde{t}} \frac{1}{\sin^2(\pi r/M)},$$

and possibly one extra factor $\frac{1}{\sin(\pi(\tilde{t}+1)/M)}$ if $t-1$ is odd. Next, we use the standard inequality $\sin x \ge \frac{2}{\pi}x$ if $0 \le x \le \frac{\pi}{2}$. In our grid setting, we always have $r \le \tilde{t} \le (t-1)/2 \le M/2$, so $\pi r/M \le \pi/2$. Hence, the following inequality applies:

$$\sin(\pi r/M) \ge \frac{2}{\pi} \cdot \frac{\pi r}{M} = \frac{2r}{M}.$$

Thus, $\frac{1}{\sin^2(\pi r/M)} \le \left(\frac{M}{2r}\right)^2$. Therefore, $\|\Delta \cdot (1, 0, \dots, 0) \cdot V_T^{-1}\|_\infty$ is bounded by

$$\Delta \cdot \max_\ell \|\sigma_\ell(V_T^{-1})\| \le \begin{cases} \Delta \prod_{r=1}^{\tilde{t}} \left(\frac{M}{2r}\right)^2 & \text{if } t-1 = 2\tilde{t} \text{ is even} \\ \Delta \left(\frac{M}{2(\tilde{t}+1)}\right) \prod_{r=1}^{\tilde{t}} \left(\frac{M}{2r}\right)^2 & \text{if } t-1 = 2\tilde{t}+1 \text{ is odd} \end{cases}$$

which suffices to prove

$$\|\Delta \cdot (1, 0, \dots, 0) \cdot V_T^{-1}\|_\infty \le \Delta \prod_{r=1}^{\tilde{t}} \frac{1}{\sin^2(\pi r/M)} \le \Delta \cdot \left(\frac{M}{2}\right)^{t-1} \cdot \frac{1}{(\tilde{t}!)^2}$$

where $\tilde{t} = \lfloor \frac{t-1}{2} \rfloor$.

□

Corollary 3.3. *For any subset $T = \{\alpha_1, \dots, \alpha_t\}$ of size t, defined as in Theorem 3.2, it holds that*

$$\max_T \sum_{j\in T} \|\Delta \cdot \lambda_j^{(T)}(0)\| \le t \cdot \Delta(t) \cdot \left(\frac{M}{2}\right)^{t-1} \cdot \frac{1}{(\lfloor \frac{t-1}{2} \rfloor!)^2}.$$

Due to the space limitation, we defer the proof of Corollary 3.3 to Appendix B.

3.3 Improved Geometric Bound via Dual Analysis

The bound in Section 3.2 is effective when $t \ll N$. As t approaches N, this bound can become overly conservative. In this section, we propose a dual analysis whose estimates explicitly depend on $k = N - t$, leading to bounds controlled by the effective threshold $\hat{t} := \min(t, N - t)$. To distinguish terminology, we refer to the analysis and bound in Section 3.2 as the *primal* analysis and bound, and to the analysis in this section as the *dual* analysis and bound.

Dual Identity. The dual analysis starts from an identity relating Lagrange coefficients over a subset T to those over the full set S. Let $P_S(Y) := \prod_{\alpha\in S}(Y - \alpha)$. We first prove the following lemma.

Lemma 3.4. *For any finite set S and $j \in S$,*

$$\lambda_j^{(S)}(Y) = \frac{P_S(Y)}{(Y - \alpha_j)P_S'(\alpha_j)}.$$

Proof. By definition,

$$\lambda_j^{(S)}(Y) = \prod_{\alpha_i \in S\setminus\{\alpha_j\}} \frac{Y - \alpha_i}{\alpha_j - \alpha_i}.$$

The numerator equals $P_S(Y)/(Y - \alpha_j)$, and the denominator equals $P_S'(\alpha_j) = \prod_{\alpha_i\in S\setminus\{\alpha_j\}}(\alpha_j - \alpha_i)$. □

Using the representation, we derive the dual identity for the standard Lagrange basis.

Lemma 3.5 (Dual identity). *Fix a reconstruction point x_0 with $P_S(x_0) \neq 0$. For any $T \subset S$, let $U := S \setminus T$. Then for any $j \in T$,*

$$\lambda_j^{(T)}(x_0) = \lambda_j^{(S)}(x_0) \cdot \prod_{\alpha_k \in U} \frac{\alpha_j - \alpha_k}{x_0 - \alpha_k}.$$

Proof. By definition,

$$\lambda_j^{(S)}(x_0) = \prod_{\alpha_i \in S\setminus\{\alpha_j\}} \frac{x_0 - \alpha_i}{\alpha_j - \alpha_i}.$$

Split the index set as $S \setminus \{\alpha_j\} = (T \setminus \{\alpha_j\}) \dot\cup U$ to obtain

$$\lambda_j^{(S)}(x_0) = \left(\prod_{\alpha_i \in T\setminus\{\alpha_j\}} \frac{x_0-\alpha_i}{\alpha_j-\alpha_i}\right)\cdot\left(\prod_{\alpha_k\in U}\frac{x_0-\alpha_k}{\alpha_j-\alpha_k}\right) = \lambda_j^{(T)}(x_0)\cdot\prod_{\alpha_k\in U}\frac{x_0-\alpha_k}{\alpha_j-\alpha_k}.$$

Rearranging the above identity yields the claim. □

Specializing to $x_0 = 0$ (note $P_S(0) \neq 0$ since $0 \notin S$), we obtain

$$\lambda_j^{(T)}(0) = \lambda_j^{(S)}(0)\cdot\prod_{\alpha_k\in U}\frac{\alpha_j-\alpha_k}{-\alpha_k}. \tag{1}$$

Fix any complex embedding σ_ℓ and write $z_i := \sigma_\ell(\alpha_i)$. By construction, the evaluation points are roots of unity; hence $|z_i| = 1$ for all i. For each $\alpha_k \in U$, write $z_j/z_k = e^{i\theta_{jk}}$ with $\theta_{jk} \in (-\pi, \pi]$. Then each factor in (1) satisfies

$$\left|\frac{z_j-z_k}{-z_k}\right| = \left|1-\frac{z_j}{z_k}\right| = \left|1-e^{i\theta_{jk}}\right| = 2\left|\sin\left(\frac{\theta_{jk}}{2}\right)\right| \le 2.$$

Hence, for every $j \in T$,

$$\prod_{\alpha_k\in U}\left|\frac{\sigma_\ell(\alpha_j)-\sigma_\ell(\alpha_k)}{-\sigma_\ell(\alpha_k)}\right| \le 2^k, \qquad k := |U| = N-t. \tag{2}$$

Combining (1) and (2) yields

$$|\sigma_\ell(\lambda_j^{(T)}(0))| \le 2^k\cdot|\sigma_\ell(\lambda_j^{(S)}(0))|.$$

Define the constant

$$L_S(0) := \max_{j\in S}\left\|\lambda_j^{(S)}(0)\right\|_\infty = \max_\ell\max_{j\in S}\left|\sigma_\ell(\lambda_j^{(S)}(0))\right|.$$

Then for every $T \subset S$ with $|T| = t$,

$$\max_\ell\max_{j\in T}\left|\sigma_\ell(\lambda_j^{(T)}(0))\right| \le 2^{N-t}L_S(0).$$

A Dual Bound and the $\min(t, N-t)$ Effect. Based on the above, we can directly obtain

$$\max_{T:|T|=t}\sum_{j\in T}\left\|\Delta(t)\lambda_j^{(T)}(0)\right\| \le t\cdot\Delta(t)\cdot 2^{N-t}L_S(0).$$

Combining this with the primal bound from Section 3.2 yields the following unified statement.

Corollary 3.6. *Let $T \subset S$ with $|T| = t$, and set $k := N-t$ and $\tilde t := \lfloor (t-1)/2 \rfloor$. Then*

$$\max_{T:|T|=t}\sum_{j\in T}\left\|\Delta(t)\lambda_j^{(T)}(0)\right\| \le t\cdot\Delta(t)\cdot\min\left\{\left(\frac{M}{2}\right)^{t-1}\frac{1}{(\tilde t!)^2}, 2^kL_S(0)\right\}.$$

In particular, the overall bound transitions from a t-driven regime (primal) to a k-driven regime (dual), and is thus controlled by $\hat t = \min(t, N-t)$.

Discussion and Simple Control of $L_S(0)$. Fix any complex embedding σ_ℓ and write $z_i := \sigma_\ell(\alpha_i)$. Using the representation above and the fact that $P_S(0) = \prod_{\alpha\in S}(-\alpha)$, we have $|\sigma_\ell(P_S(0))| = \prod_{\alpha\in S}|z_i| = 1$, and therefore

$$|\sigma_\ell(\lambda_j^{(S)}(0))| = \frac{1}{|\sigma_\ell(P_S'(\alpha_j))|} = \frac{1}{\prod_{\alpha_i\in S\setminus\{\alpha_j\}}|z_j-z_i|}.$$

Hence, $L_S(0) = \max_\ell\max_{j\in S}|\sigma_\ell(\lambda_j^{(S)}(0))|$ is governed by the geometry of S on the unit circle: it increases when points in S become clustered.

For a simple worst-case upper bound depending only on (M, N), compare S to the full M-grid $G := \{\omega^0, \omega^1, \ldots, \omega^{M-1}\}$. A direct computation gives $\lambda_j^{(G)}(0) = 1/M$ for all $j \in G$. Applying Lemma 3.5 with $(S, T) = (G, S)$ and $x_0 = 0$, and using the factor bound $\left|\frac{z_j-z_k}{-z_k}\right| \le 2$, yields

$$L_S(0) \le \frac{2^{M-N}}{M}.$$

This worst-case estimate can be loose; for structured choices of S with good angular separation, $L_S(0)$ can be much smaller, strengthening the dual term in Corollary 3.6. For instance, suppose $M = N$. Then Corollary 3.6 becomes especially sharp by taking S to be the full M-grid $G = \{\omega^0, \omega^1, \ldots, \omega^{M-1}\}$, for which $\lambda_j^{(G)}(0) = 1/M = 1/N$ for all j, and thus $L_S(0) = 1/N$. Consequently, the dual contribution $2^{N-t}L_S(0)$ simplifies to $2^{N-t}/N$.

Comparison of the Derived Bounds. To determine which branch of the unified estimate is active, we compare the two terms inside the minimum. Specifically, we define the primal contribution $P(t)$ and the dual contribution $D(t)$ as follows:

$$P(t) := \left(\frac{M}{2}\right)^{t-1}\frac{1}{(\tilde t!)^2},\ D(t) := 2^{N-t}L_S(0),$$

where $\tilde t := \left\lfloor\frac{t-1}{2}\right\rfloor$. Using the worst-case bound $L_S(0) \le 2^{M-N}/M$, we obtain $D(t) \le \frac{2^{M-t}}{M}$. Hence, the dual branch is selected whenever $D(t) \le P(t)$.

Approximating $\tilde t \approx t/2$ and using Stirling formula

$$\log_2(\tilde t!) = \tilde t\log_2\tilde t - \tilde t\log_2 e + O(\log_2 t),$$

we obtain the leading terms

$$\log_2 P(t) = t\log_2\left(\frac{eM}{t}\right) + O(\log_2 t),\ \log_2 D(t) = (M-t) - \log_2 M.$$

Ignoring lower-order terms, the crossover point is approximated by

$$M - t \approx t\log_2\left(\frac{eM}{t}\right). \tag{3}$$

Write $M = \alpha N$ with $1 \le \alpha < 2$ and $t = cN$. Dividing (3) by N yields

$$\alpha - c \approx c\log_2\left(\frac{e\alpha}{c}\right). \tag{4}$$

Let $c(\alpha)$ denote the solution to (4). Then, for $t \gtrsim c(\alpha)N$, the dual term is typically smaller than the primal term and therefore determines the minimum.

Solving (4) numerically yields $c(1) \approx 0.214$, $c(1.25) \approx 0.268$, $c(1.5) \approx 0.322$, $c(1.75) \approx 0.375$, $c(2) \approx 0.429$. In particular, for $N \le M < 2N$, the crossover fraction lies in the range

$$0.214 \lesssim c(\alpha) \lesssim 0.429,$$

and improves (i.e., shifts downward) for structured choices of S that yields smaller $L_S(0)$ than the worst-case bound.

4 Application to Threshold Fully Homomorphic Encryption Schemes

As a primary application of the refined Shamir SSS, we consider ThFHE schemes [11, 15]. The refined Shamir SSS significantly enhances the efficiency of ThFHE constructions. Throughout this section, we directly apply Corollary 3.6 to ThFHE schemes.

4.1 Application to Boneh et al.'s ThFHE

The construction proposed by Boneh et al. [11], referred to as BGG$^+$18 in this paper, consists of two primitives:

- the classic Shamir SSS, and
- a *BFV-style*[2] FHE scheme [14, 28] satisfying

$$\langle \mathsf{ct}, \mathsf{sk} \rangle \bmod Q = \left\lfloor \frac{Q}{2} m \right\rfloor + \Delta^2 e \quad (\text{in } R_Q), \tag{5}$$

  where ct is a ciphertext under the public key pk, sk is the corresponding secret key, Q is the ciphertext modulus, Δ is the denominator-clearing factor associated with the underlying Shamir SSS.[3]

By replacing the classic Shamir SSS with our refined approach defined in the previous section, we obtain a more efficient ThFHE construction. This modification yields substantial efficiency gains. In essence, unlike the previous design that requires a prohibitively large ciphertext modulus $Q \geq \Omega((N!)^4)$, our construction only needs $Q \geq 2^{\Omega(t \log_2(N/t^2))}$ or $Q \geq 2^{\Omega(N-t)}$ depending on t and N.

Let $\mathsf{FHE} = (\mathsf{FHE.Setup}, \mathsf{FHE.Enc}, \mathsf{FHE.Eval}, \mathsf{FHE.Dec})$ be a BFV-style leveled FHE scheme with a multiplicative constant $\Delta = 2^{\lceil \log_2 t \rceil}$ whose decryption is linear in the secret key and whose centralized decryption error is bounded by $B = B(\lambda, d, Q)$ after a depth-d evaluation at modulus Q. Let $\mathsf{SS} = (\mathsf{SS.Setup}, \mathsf{SS.ShareGen}, \mathsf{SS.Reconstruct})$ be the refined Shamir SSS proposed in Section 3. Let $B_{\mathsf{sm}} > 0$ denote the bound on the public smudging noise used in partial decryption.

Based on these primitives, we now present the refined ThFHE scheme. Our construction incorporates a slight modification of the original scheme of [11] to account for the recent attack identified in [21]. A detailed discussion of the security implications appears in Appendix C; here, we simply remark that replacing the underlying SSS with our refined variant does not alter the security guarantees of the overall ThFHE scheme. Let $\mathbb{A}_t$ denote a t-out-of-N threshold access structure.

Construction 4.1. A ThFHE scheme $\mathsf{ThFHE} = (\mathsf{ThFHE.Setup}, \mathsf{ThFHE.Encrypt}, \mathsf{ThFHE.Eval}, \mathsf{ThFHE.PartDec}, \mathsf{ThFHE.FinDec})$ is designed as follows.

- $\mathsf{ThFHE.Setup}(1^\lambda, 1^d, \mathbb{A}_t)$: Given the security parameter λ, a depth bound d, and a t-out-of-N threshold access structure $\mathbb{A}_t$, it proceeds as follows:
  (1) Run $\mathsf{FHE.Setup}(1^\lambda, 1^d) \to (\mathsf{pk}_{\mathsf{fhe}}, \mathsf{sk}_{\mathsf{fhe}})$.
  (2) Run $\mathsf{SS.Setup}(n, Q, N, t) \to S = \{\alpha_1, \alpha_2, \ldots, \alpha_N\}$ where n is the ring dimension and Q is the ciphertext modulus contained in $\mathsf{pk}_{\mathsf{fhe}}$.
  (3) Run $\mathsf{SS.Share}(\mathsf{sk}_{\mathsf{fhe}}, S, t) \to (\mathsf{sk}_1, \ldots, \mathsf{sk}_N)$.
  (4) Output $\mathsf{pk} = (\mathsf{pk}_{\mathsf{fhe}}, S, \Delta = 2^{\lceil \log_2 t \rceil})$ and $\mathsf{sk}_i \in R_Q$ for all $i \in [N]$.
- $\mathsf{ThFHE.Encrypt}(\mathsf{pk}, m)$: Given the public key pk and a message $m \in R_2$, it runs $\mathsf{FHE.Enc}(\mathsf{pk}_{\mathsf{fhe}}, m) \to \mathsf{ct}$ and outputs ct.
- $\mathsf{ThFHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k)$: Given the public key pk, a circuit C, and a set of ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_k$, it runs $\mathsf{FHE.Eval}(\mathsf{pk}_{\mathsf{fhe}}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k) \to \mathsf{ct}$ and outputs the evaluated ciphertext ct.
- $\mathsf{ThFHE.PartDec}(\mathsf{pk}, \mathsf{ct}, \mathsf{sk}_i)$: Given the public key pk, a ciphertext $\mathsf{ct} = (c_0, c_1)$, and a secret share sk_i for party P_i, it samples e_i from a predefined distribution χ_D, computes the partial decryption

$$\mathsf{p}_i = c_1 \cdot \mathsf{sk}_i + \Delta e_i \quad \text{in} \quad R_Q,$$

  and outputs p_i.
- $\mathsf{ThFHE.FinDec}(\mathsf{pk}, \{p_i\}_{i \in T})$: Given the public key pk and partial decryption results $\{p_i\}_{i \in T}$, if $|T| \geq t$, then it computes $\mathsf{p} = \sum_{i \in T} \lambda_i^{(T)}(0) \mathsf{p}_i$ and outputs m by computing $m = \left\lfloor \frac{2}{Q} \mathsf{p} \right\rceil \bmod 2$.

Lemma 4.2 (Correctness of Construction 4.1). *Let* ct *be a ciphertext of a special FHE satisfying*

$$\langle \mathsf{ct}, \mathsf{sk} \rangle = \left\lfloor \frac{Q}{2} m \right\rfloor + \Delta^2 e$$

in R_Q and let $T \subseteq [N]$ with $|T| \geq t$. Each party computes its partial decryption as $\mathsf{p}_i := \langle \mathsf{ct}, \mathsf{sk}_i \rangle + \Delta e_i \in R_Q$. Then

$$\sum_{i \in T} \lambda_i^{(T)}(0) \mathsf{p}_i = \left\lfloor \frac{Q}{2} m \right\rfloor + \Delta^2 e + \Delta \sum_{i \in T} \lambda_i^{(T)}(0) e_i \tag{6}$$

in R_Q. Therefore, the final decryption correctly outputs m if

$$\left\| \Delta^2 e + \Delta \sum_{i \in T} \lambda_i^{(T)}(0) e_i \right\| \leq Q/4. \tag{7}$$

Let $\Lambda := \max_T \sum_{i \in T} \|\Delta \lambda_i^{(T)}(0)\|$. Then, a sufficient explicit condition for correctness is given by

$$\Delta^2 B + \Lambda \cdot B_{\mathsf{sm}} \leq Q/4 \tag{8}$$

where B denotes the bound on the ciphertext noise and B_{sm} denotes the bound on the public smudging noise introduced during partial decryption.

Lemma 4.2 directly implies the following asymptotic result. Due to space limitations, we defer its proof to Appendix B.

Theorem 4.3. *Using Stirling approximation and the unified bound, we obtain*

$$\log_2 Q = O\left(\min\left\{ t \log_2\left(\frac{N}{t^2}\right), M - t \right\} \right),$$

where $M := 2^{\lceil \log_2 N \rceil}$, and we used the worst-case bound $L_S(0) \leq 2^{M-N}/M$, hence $2^{N-t} L_S(0) \leq 2^{M-t}/M$.

[2] For simplicity of presentation, we focus on a specific type of FHE scheme; however, our approach can be readily adapted to other FHE variants, such as BGV [16] and CKKS [20].

[3] In general, a (correct) BFV-style FHE scheme satisfies $\langle \mathsf{ct}, \mathsf{sk} \rangle \bmod Q = \lfloor \frac{Q}{2} m \rceil + e$. On the other hand, in the original paper [11], an FHE scheme satisfying (5) is referred to as a special FHE and the authors describe how to obtain such schemes from general FHE constructions.

4.2 Application to Brakerski et al.'s ThFHE

As another application, we consider the recent ThFHE scheme proposed by Brakerski et al. [15], referred to as BFM$^+$25 in this paper. Their work presents the first *asynchronous* ThFHE construction that achieves universal composability (UC) while simultaneously addressing major scalability challenges. One of their key technical contributions is the design of a new variant of the Shamir SSS over a polynomial ring R, which serves as a core component enabling low ciphertext overhead. Furthermore, the BFM$^+$25 framework attains malicious security by incorporating additional cryptographic primitives such as zero-knowledge proofs and publicly verifiable secret sharing, in contrast to the construction described in Section 4.1. However, in this section, we focus solely on the correctness condition when our refined approach is applied to the BFM$^+$25 framework. In particular, we show that our refinement improves the correctness and efficiency of the BFM$^+$25 construction while preserving its robust asynchronous structure and tighter reconstruction bounds. Since our modification only affects the choice of the underlying Shamir SSS, the malicious security and UC guarantees established in [15] are directly inherited. For consistency with [15], we consider a $(t+1)$-out-of-N threshold setting throughout this section.

Overview of the BFM$^+$25 Framework. The construction of Brakerski et al. [15] introduces a ThFHE scheme for ring-based FHE (such as BGV [16], BFV [14, 28], and CKKS [20]) that operates in a fully *asynchronous* communication model. Their framework follows the standard MPC-from-FHE paradigm and consists of three main phases:

- distributed key generation (DKG) to jointly generate a single public key pk and secret key shares $\{\mathsf{sk}_i\}$;
- homomorphic evaluation to perform circuit evaluation under the shared public key; and
- threshold decryption to jointly decrypt the evaluated ciphertext.

The main technical innovation of BFM$^+$25 lies in addressing the modulus growth problem by transitioning from the LWE to the Ring-LWE (RLWE) setting. To this end, they select a structured set of evaluation points $\mathcal{I} = \{\pm X^j\}$ within the polynomial ring.

Their correctness analysis [15, Theorem 2] shows that the final ciphertext modulus Q must be large enough to accommodate two dominant noise terms:

$$\log_2 Q \approx \log_2(\underbrace{B \cdot \|\Delta_{\mathsf{BFM+}}\|}_{\text{FHE noise term}} + \underbrace{r_D \cdot \|\Lambda_{\mathsf{BFM+}}\|}_{\text{smudging noise term}}).$$

In their analysis, they estimate $\|\Delta_{\mathsf{BFM+}}\| \approx 1.2^{\frac{2}{3}N}$ and $\|\Lambda_{\mathsf{BFM+}}\| \approx 2^{\frac{3}{4}N}$, both of which cause the bit length of the ciphertext modulus to grow linearly with N, i.e., $\log_2 Q = \Theta(N)$.

When replacing their SSS with ours, only the correctness condition is affected, while the overall security remains unchanged. Accordingly, we restrict our discussion in this section to the correctness constraint of the original scheme and its adaption using our refined secret sharing framework.

Lemma 4.4 (Parameter Constraints in [15]). *Let Q be the ciphertext modulus in the auxiliary ThFHE scheme of [15], which is used for asynchronous decryption. To ensure correctness and security, Q must be large enough to accommodate the total accumulated noise:*

$$\frac{Q}{p} > nN\left\lceil \frac{N^2}{n} \right\rceil (B \cdot 1.2^{\frac{2}{3}N} + r_D 2^{\frac{3}{4}N}),$$

where p is the plaintext modulus, B bounds the noise in the base FHE scheme, and r_D bounds the security-dependent smudging noise satisfying $r_D > n2^t 2^\kappa r_E$ [15]. Here, r_E denotes a parameter related to the noise distribution and κ denotes the statistical security parameter.

These quantities are derived from the bounds

$$\|\Delta_{\mathsf{BFM+}} e\| \le Bn\frac{N^2}{3n}1.2^{\frac{2}{3}N}, \quad \|\Delta_{\mathsf{BFM+}}\lambda^{(T)}_{i,\mathsf{BFM+}}(0)\| \le \frac{N^2}{3n}2^{\frac{3}{4}N}.$$

As a result, substituting our improved analysis into the framework of [15] yields the following constraint.

Proposition 4.5. *When the BFM$^+$25 framework [15] is instantiated with our refined secret sharing scheme from Section 3, the ciphertext modulus Q must be large enough to ensure correctness and security:*

$$\frac{Q}{p} > 2^{\lceil \log_2(t+1) \rceil}\left(B + r_D \min\left\{\left(\frac{M}{2}\right)^t \frac{1}{(\lfloor \frac{t}{2} \rfloor !)^2}, \frac{2^{M-(t+1)}}{M}\right\}\right)$$

where p is the plaintext modulus, B bounds the ciphertext noise, and r_D bounds the smudging noise in partial decryption.

4.3 Comparison

In this section, we compare our refined Shamir SSS with those employed in existing ThFHE constructions, considering both asymptotic and concrete parameter settings. We restrict our scope to *one-round, asynchronous* decryption protocols, since multi-round or DKG-based threshold FHE systems (e.g., [18, 36, 40, 49]) can trade additional interaction for smaller ciphertext moduli and are therefore not directly comparable. Under this one-round restriction, we focus on the ThFHE schemes of [11, 15, 19], which are the most natural targets for integrating a more efficient SSS. Furthermore, since our analysis focuses on the scaling behavior with respect to N, we exclude [13, 24], as these constructions require $\binom{N}{t}$ to remain small, making them unsuitable for large-N comparison.[4] We note that our comparison against [11] uses our own same-environment implementation built on OpenFHE [7], the comparison against [18] uses the authors' public Lattigo-based implementation [2] under the same machine, and the comparison against [19] is restricted to parameter and ciphertext-size analysis only (not runtime), as no public implementation is available. In all cases, setup costs (key generation, evaluation key distribution) are excluded from the reported timings.

Asymptotic Comparison. Table 1 categorizes prior secret-sharing-based thresholdizers according to the *source* of their modulus growth, rather than their specific protocol designs:

- Schemes that clear *all* possible reconstruction denominators in advance (e.g., BGG$^+$18 [11] with classical Shamir secret sharing), which inevitably incur $O(N \log_2 N)$ growth.

[4] The authors of [24] also proposed a ThFHE variant that supports large $\binom{N}{t}$, but it no longer achieves one-round asynchronous threshold decryption, since it relies on an additional secure multiparty computation protocol.

- Schemes that maintain a smaller modulus by introducing multiple auxiliary shares or keys (e.g., the $\{0,1\}$-LSSS variant in BGG$^+$18 [11], and the iterative approach of [19]).
- Schemes that operate directly over the FHE ring, where the modulus scales linearly with N (e.g. [15]).

According to the table, the refined Shamir SSS attains the asymptotic bound $O\big(\min\{t\log_2(N/t^2), M-t\}\big)$ for $M = 2^{\lceil \log_2 N\rceil}$, which follows directly from our Lagrange amplification analysis. In particular, when $t = O(1)$ the bound simplifies to $O(\log_2 N)$, while $t = \Theta(\log_2 N)$ yields $O((\log_2 N)^2)$. Moreover, the size of each key share is determined by the product of the underlying ring dimension n, the ciphertext modulus bit-length $\log_2 Q$, and the number of keys held per party. Since the total number of parties is N and each party possesses only a single key share in our construction, the per-party share size becomes $O(n\log_2 Q) = O(nt\log_2(N/t)^2)$. This represents the smallest asymptotic key-share size among all compared schemes in the table.

Table 1: Asymptotic comparison of ciphertext modulus size (reported as $\log_2 Q$) and key/share count in the system for t-out-of-N ThFHE

Secret Sharing Scheme		$\log_2 Q$	# of keys per party
[11]	SSS over $\mathbb{Z}_Q$	$O(N\log_2 N)$	N
	$\{0,1\}$-LSSS	$O(\log_2 N)$	$O(N^{5.3})$
[19]	SSS$(3,2)$	$O(\log_2 N)$	$O(N^{4.3})$
	SSS$(2s-1,s)$	$O(s\log_2 s\cdot\log_2 N)$	$O(N^{3+\frac{2.3}{\log_2 s}})$
[15]	SSS over R	$O(N)$	N
Ours+[11] Ours+[15]	SSS over R_Q	$O\big(\min\{t\log_2(N/t^2),\ M-t\}\big)$	N

*SSS(N,t): A t-out-of-N Shamir secret sharing over $\mathbb{Z}_Q$, and $M = 2^{\lceil \log_2 N\rceil}$

Concrete Comparison. Beyond the asymptotic comparison, we extend the analysis to concrete parameter settings. Specifically, we compare the ciphertext sizes required by four different secret sharing configurations, using the same values of N (number of parties) and a common threshold t. We examine various threshold regimes—constant, logarithmic, and linear in N—and adopt the baseline parameters from [15] for consistency:

- Security: computational security parameter $\lambda \geq 128$ and statistical security parameter $\kappa = 40$ [15].
- FHE base: ring dimension $n = 2^{10}$ and ciphertext modulus q with $\log_2 q = 10$.
- Common security noise: all schemes must satisfy the security requirement from [15, Thm. 3], which specifies a common smudging noise parameter r_D with bit-length

$$\log_2 r_D = \begin{cases} \kappa = 40 & \text{in [11]},\\ \log_2(n) + t + \kappa = t + 50 & \text{in [15]}. \end{cases}$$

Parameter Selection for ThFHE. We first estimate the error size, defined as the bit-length of the combined noise magnitude, given by $\log_2$(FHE Noise + Smudging Noise). Specifically, we evaluate this quantity as $\log_2(2^A + 2^B)$, where 2^A and 2^B represent the FHE and smudging noise terms, respectively. We estimate the error size of each construction as follows:

(1) BGG$^+$18 [11]: We adopt the purely algebraic overhead term $4\log_2(N!)$, as justified by the robustness analysis against the recent attack in [21].[5]
(2) BFM$^+$25 [15]: The formula is derived from Theorem 2 in [15], corresponding to the bound in Lemma 4.4.
(3) Ours+[11]: This configuration applies our improved analysis to the BGG$^+$18 framework, following the correctness condition in Lemma 4.2.
(4) Ours+[15]: This configuration integrates our approach into the BFM$^+$25 framework, as captured by Proposition 4.5.

For correctness, we then choose the minimum value of $\log_2 Q$ that satisfies the corresponding correctness constraint. We determine a new ring dimension $\hat{n}$ to achieve at least $\lambda \geq 128$ bits of security, following the lattice-estimation framework of [1] under the `list_decoding-classical` security model, which is the default setting. In addition, the secret key s is chosen as a sparse ternary polynomial with $\|s\|_1 = 128$, meaning that its Hamming weight is 128. For each configuration (N,t), we estimate the ciphertext size following the same methodology as Brakerski et al. [15].[6]

Table 2 summarizes the concrete ciphertext sizes estimated from the parameters derived above, covering both low-threshold regimes ($t = 5$ or $t \approx \log_2 N$) and high-threshold regimes ($t = \lfloor N/3\rfloor$, $t = \lfloor N/2\rfloor$, or $t = \lfloor 2N/3\rfloor$). When $N \in \{32, 64\}$, our BGG$^+$18-based instantiation achieves dramatic reductions: for $N = 32$, we obtain about a 57×–66× decrease in ciphertext size, and for $N = 64$, the reduction ranges from about 107× to 290×, depending on t. This gap already widens at these values of N, reflecting that the ciphertext size in [11] grows much faster with N than in our construction.

Against [15], our refined Shamir SSS also yields consistent savings across all tested regimes. Concretely, the reduction factors range from about 1.1× up to roughly 18.5×. For example, when $(N,t) = (512,5)$, the ciphertext size drops from 1933.31 KB to 104.45 KB (about 18.5×), while for $(N,t) = (512,341)$ it decreases from 6619.14 KB to 2322.43 KB (about 2.8×). Furthermore, we empirically compare the Shamir SSS adaptations of [15] and our variant, and observe that $\|\Delta\lambda_i^{(T)}\|_\infty$ is consistently smaller for our construction across all tested regimes; see Section 5 for details.

Overall, our refined Shamir SSS yields the smallest ciphertext sizes among the compared frameworks for essentially all tested parameter sets. The smaller $\log_2 Q$ achieved by our construction directly translates into a smaller ring dimension $\hat{n}$ required to achieve $\lambda = 128$ bits of security under the lattice estimator [1].

5 Experimental Results

In this section, we empirically evaluate the efficiency of our refined Shamir SSS. To this end, we replace the classical Shamir SSS in the ThFHE scheme of [11] with our refined variant[7], and compare the performance of the resulting construction with the original baseline. We additionally benchmark our approach against the recent ThFHE scheme of [18], whose joint decryption requires two rounds of communication. For this comparison, we use the authors' public

[5] For comparison, Table 2 of [15] estimates this overhead as $2\log_2(N!)$.
[6] Namely, the ciphertext size is approximated as $|\mathrm{ct}| = A = \frac{B\cdot C}{8000}$ where $B = \hat{n}$ is the ring dimension and $C = \log_2 Q$ is the bit-length of the ciphertext modulus.
[7] Available at https://github.com/seunghu-kim/2adic-ss.git.

Table 2: Estimated ciphertext size $|\mathsf{ct}|$. A (B, C) indicates that the ciphertext size is A (KB), and $B = \hat{n}$ and $C = \log_2 Q$. We take a formula $A = \frac{B \cdot C}{8000}$ as in [15].

N	t	BGG$^+$18 [11]	BFM$^+$25 [15]	Ours +BGG$^+$18	Ours+BFM$^+$25
32	5	1927.78 $(2^{15}, 470.65)$	102.40 $(2^{13}, 100.00)$	31.40 $(2^{12}, 61.32)$	41.98 $(2^{12}, 82.00)$
32	10	1927.78 $(2^{15}, 470.65)$	107.52 $(2^{13}, 105.00)$	33.96 $(2^{12}, 66.32)$	88.06 $(2^{13}, 86.00)$
32	16	1927.78 $(2^{15}, 470.65)$	113.66 $(2^{13}, 111.00)$	31.23 $(2^{12}, 61.00)$	89.09 $(2^{13}, 87.00)$
32	21	1927.78 $(2^{15}, 470.65)$	118.78 $(2^{13}, 116.00)$	29.38 $(2^{12}, 57.39)$	89.09 $(2^{13}, 87.00)$
64	5	9699.16 $(2^{16}, 1183.98)$	130.05 $(2^{13}, 127.00)$	33.44 $(2^{12}, 65.32)$	89.09 $(2^{13}, 87.00)$
64	6	9699.16 $(2^{16}, 1183.98)$	131.07 $(2^{13}, 128.00)$	36.14 $(2^{12}, 70.58)$	91.99 $(2^{13}, 89.83)$
64	21	9699.16 $(2^{16}, 1183.98)$	146.43 $(2^{13}, 143.00)$	90.51 $(2^{13}, 88.39)$	120.83 $(2^{13}, 118.00)$
64	32	9699.16 $(2^{16}, 1183.98)$	157.70 $(2^{13}, 154.00)$	39.94 $(2^{12}, 78.00)$	121.86 $(2^{13}, 119.00)$
64	42	9699.16 $(2^{16}, 1183.98)$	167.94 $(2^{13}, 164.00)$	35.53 $(2^{12}, 69.39)$	121.86 $(2^{13}, 119.00)$
128	5	–	364.54 $(2^{14}, 178.00)$	35.49 $(2^{12}, 69.32)$	94.21 $(2^{13}, 92.00)$
128	7	–	368.64 $(2^{14}, 180.00)$	40.26 $(2^{12}, 78.64)$	105.30 $(2^{13}, 102.83)$
128	42	–	440.32 $(2^{14}, 215.00)$	135.57 $(2^{13}, 132.39)$	372.74 $(2^{14}, 182.00)$
128	64	–	485.38 $(2^{14}, 237.00)$	113.66 $(2^{13}, 111.00)$	374.78 $(2^{14}, 183.00)$
128	85	–	528.38 $(2^{14}, 258.00)$	93.60 $(2^{13}, 91.41)$	374.78 $(2^{14}, 183.00)$
256	5	–	567.30 $(2^{14}, 277.00)$	37.54 $(2^{12}, 73.32)$	99.33 $(2^{13}, 97.00)$
256	8	–	573.44 $(2^{14}, 280.00)$	94.03 $(2^{13}, 91.83)$	117.59 $(2^{13}, 114.83)$
256	85	–	1462.27 $(2^{15}, 357.00)$	447.30 $(2^{14}, 218.41)$	634.88 $(2^{14}, 310.00)$
256	128	–	1638.40 $(2^{15}, 400.00)$	360.45 $(2^{14}, 176.00)$	636.93 $(2^{14}, 311.00)$
256	170	–	1810.43 $(2^{15}, 442.00)$	138.66 $(2^{13}, 135.41)$	636.93 $(2^{14}, 311.00)$
512	5	–	1933.31 $(2^{15}, 472.00)$	39.59 $(2^{12}, 77.32)$	104.45 $(2^{13}, 102.00)$
512	9	–	1949.70 $(2^{15}, 476.00)$	106.50 $(2^{13}, 104.00)$	134.99 $(2^{13}, 131.83)$
512	170	–	2609.15 $(2^{15}, 637.00)$	1599.12 $(2^{15}, 390.41)$	2318.34 $(2^{15}, 566.00)$
512	256	–	5922.82 $(2^{16}, 723.00)$	624.64 $(2^{14}, 305.00)$	2322.43 $(2^{15}, 567.00)$
512	341	–	6619.14 $(2^{16}, 808.00)$	453.45 $(2^{14}, 221.41)$	2322.43 $(2^{15}, 567.00)$

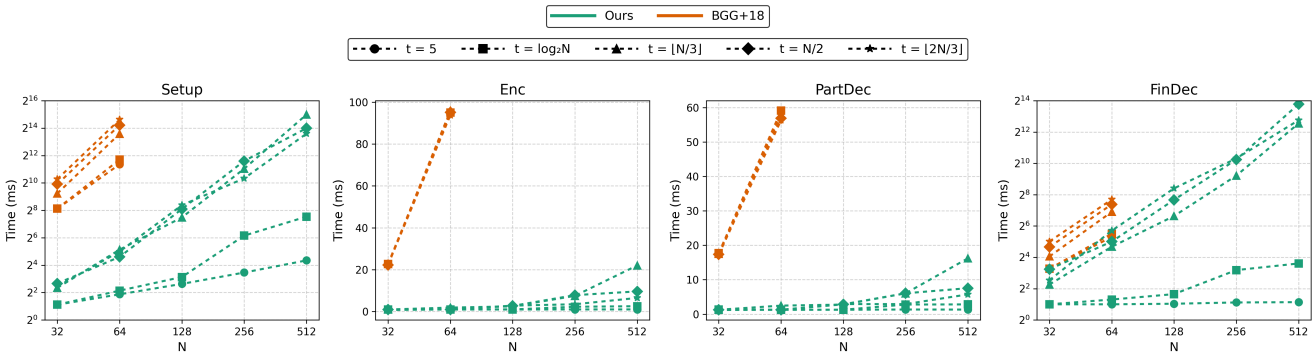


Figure 2: Running times of the ThFHE algorithms, averaged over 100 trials. The Setup algorithm includes both key generation and sharing.

implementation[8], which is built on the Lattigo library [2], and run it under the same experimental conditions as our implementation.

Experimental Settings. For the underlying FHE component of the BGG$^+$18-based ThFHE scheme, we used the BFV implementation from OpenFHE [7], modifying its setup algorithm so that it functions as a special FHE scheme with an appropriate choice of Δ. All cryptographic parameters are selected to achieve at least 128-bit security. Experiments were conducted on a machine equipped with an Apple M3 Max processor and 48 GB of unified memory.

[8]Available at https://github.com/Yijia-Oneplus-Chang/Usenix2025.git.

ThFHE Comparison Results. Our refined Shamir SSS substantially reduces the required ciphertext modulus. This, in turn, enables more compact parameters and improves the performance of the corresponding ThFHE constructions. Using the parameter sets in Table 2 that satisfy both correctness and security requirements, we benchmark the running time of the ThFHE algorithms.

Figure 2 compares the running time of Setup, Enc, PartDec, and FinDec between our construction and BGG$^+$18. Across the entire range of tested parameters, our refined construction consistently outperforms the original scheme. For example, when $N = 64$, depending on t, the observed speedups range from 351×–789× for

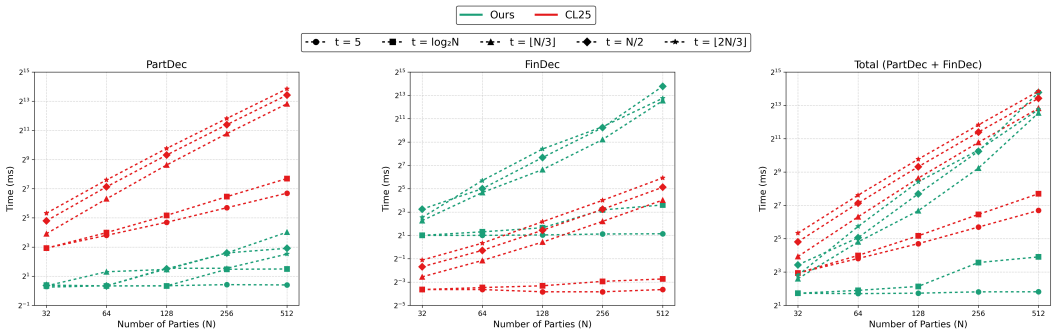
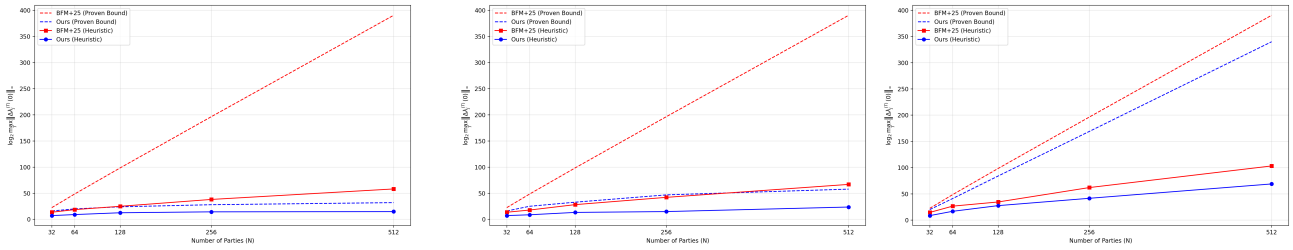
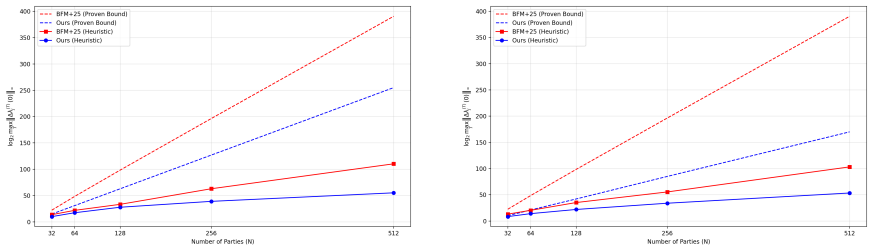


Figure 3: Running times of distributed decryption for ours (one-round) and CL25 [18] (two-round). The time for PartDec **is measured per party.**



(a) $t = 5$ **(b)** $t = \log_2 N$ **(c)** $t = \lfloor N/3 \rfloor$



(d) $t = N/2$ **(e)** $t = \lfloor 2N/3 \rfloor$

Figure 4: Comparison of $\log_2 \left(\max_T \|\Delta\lambda_i^{(T)}(0)\|_\infty \right)$ **between our refined Shamir SSS and BFM$^+$25**

Setup, 52×–103× for Enc, 23×–47× for PartDec, and 4×–20× for FinDec. These improvements are observed uniformly across both low- and high-threshold regimes. As a representative low-threshold example, for $(N, t) = (64, 6)$, the running times of Setup, Enc, and PartDec are 4.60, 0.94, and 1.28 ms, yielding speedups of approximately 682.8×, 103.5×, and 46.5× over BGG$^+$18, respectively. Comparable gains are also present in high-threshold settings; for instance, at $(N, t) = (32, 21)$, the corresponding speedups are about 229.3× for Setup, 32.4× for Enc, and 14.5× for PartDec.

More importantly, while the classic Shamir SSS used in BGG$^+$18 incurs substantial parameter growth and becomes increasingly inefficient for larger party counts (e.g., $N \geq 128$), our scheme continues to scale favorably across the full spectrum of tested parameters. For example, with $(N, t) = (256, 8)$, the algorithms Setup, Enc, PartDec, and FinDec complete in approximately 17.64, 0.97, 1.27 and 12.74 ms, respectively. These results indicate that the refined construction maintain efficient end-to-end performance while supporting parameter regimes that are difficult to accommodate using the classical approach.

Next, we compare our instantiation with the approximate ThFHE scheme of Chang and Li [18], which employs a *two-round* asynchronous decryption procedure; hereafter, we refer to their scheme as CL25. For a consistent comparison with our one-round construction, we interpret CL25's two-round workflow by treating PartDec as all per-party computations across both rounds and FinDec as the aggregator's total computation. In contrast, our scheme uses the standard single-round definitions of PartDec and FinDec.

Figure 3 reports the running times of distributed decryption under this aligned interpretation. Despite CL25's more compact parameters, our ThFHE consistently outperforms CL25 in PartDec, since CL25 requires the t participating parties to secret share ephemeral keys. The resulting speedups range from about 5.8× ($N = 32$, $t = 5$) to 2570.2× ($N = 512$, $t = 341$), substantially reducing the per-party

computational burden. By contrast, CL25 achieves a shorter FinDec time, which in turn reduces the computational burden on the single aggregator responsible for completing reconstruction.

Although our approach uses larger parameters to support *one-round* asynchronous decryption, the overall decryption cost (PartDec per party + FinDec) is lower than CL25 in all but one setting. The only exception is $(N, t) = (512, 256)$, where our construction requires heavier parameters (e.g., ring dimension $n = 2^{15}$). For example, at $(N, t) = (256, 8)$ and $(N, t) = (256, 170)$, CL25 requires 87.82 ms and 3630.64 ms in total, whereas our scheme is faster by approximately 7.40× and 2.85×, respectively.

Communication Cost. Since our refined SSS reduces the ciphertext modulus Q and consequently the ring dimension $\hat{n}$, the resulting ciphertext sizes (Table 2) are substantially smaller, which directly translates to reduced communication cost during threshold decryption. For instance, at $(N, t) = (512, 5)$, the per-party partial decryption share size decreases from 1933.31 KB (BFM$^+$25) to 104.45 KB (Ours+BFM$^+$25), a reduction of approximately 18.5×. In a network setting, this directly implies an 18.5× reduction in the bandwidth required for each party to transmit its partial decryption share.

Experimental Analysis for Heuristic Bound. We empirically evaluate the magnitude of $\Delta\lambda_j^{(T)}(0)$ to examine trends in our heuristic and proven bounds and compare them with both the heuristic and proven bounds of BFM$^+$25 [15]. For each method and each (N, t) in Table 2, we sample a random size-t subset $T \subset S = \{\alpha_1, \ldots, \alpha_N\}$, compute $\|\Delta\lambda_j^{(T)}(0)\|_\infty$, and repeat this process over 10 trials. We report the bit size of the maximum over the sampled subsets T, i.e., $\log_2\left(\max_T \|\Delta\lambda_j^{(T)}(0)\|_\infty\right)$, which serves as heuristic bound in Figure 4.

Our proven bound is consistently tighter than that of BFM$^+$25, avoiding overestimated parameter choices for ThFHE. In particular, for $t = \log_2 N$, our bound is 1.40×–6.75× smaller, and for high thresholds ($t = \lfloor 2N/3 \rfloor$), the dual analysis yields improvements of 2.24×–2.34×.

As shown in Figure 4, the empirical values under our refined SSS are also uniformly smaller than those of BFM$^+$25 across all tested parameters. Moreover, the growth of $\log_2(\max_T \|\Delta\lambda_j^{(T)}(0)\|_\infty)$ is noticeably slower as N increases, including in high-threshold regimes, matching our theoretical predictions. Although heuristic, these results further support the practical advantages of our refined SSS.

6 Acknowledgments

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00399491, 75%). Jiseung Kim was also supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. RS-2026-25477662, 25%).

References

[1] [n. d.]. Lattice-Estimator. https://github.com/malb/lattice-estimator. Accessed: 2025-10-06.

[2] 2020. Lattigo v4. https://github.com/tuneinsight/lattigo.git, EPFL-LDS, Tune Insight SA.

[3] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck Wee. 2012. Functional Encryption for Threshold Functions (or Fuzzy IBE) from Lattices. In *Public Key Cryptography – PKC 2012*, Marc Fischlin, Johannes Buchmann, and Mark Manulis (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 280–297.

[4] Shweta Agrawal, Damien Stehlé, and Anshu Yadav. 2022. Round-Optimal Lattice-Based Threshold Signatures, Revisited. In *49th International Colloquium on Automata, Languages, and Programming (ICALP 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

[5] Martin R Albrecht and Russell WF Lai. 2021. Subtractive sets over cyclotomic rings: Limits of schnorr-like arguments over lattices. In *Annual International Cryptology Conference*. Springer, 519–548.

[6] Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. 2012. Multiparty computation with low communication, computation and interaction via threshold FHE. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 483–501.

[7] Ahmad Al Badawi, Jack Bates, Flávio Bergamaschi, David Bruce Cousins, Saroja Erabelli, Nicholas Genise, Shai Halevi, Hamish Hunt, Andrey Kim, Yongwoo Lee, Zeyu Liu, Daniele Micciancio, Ian Quah, Yuriy Polyakov, R. V. Saraswathy, Kurt Rohloff, Jonathan Saylor, Dmitriy Suponitsky, Matthew Triplett, Vinod Vaikuntanathan, and Vincent Zucca. 2022. OpenFHE: Open-Source Fully Homomorphic Encryption Library. In *WHAC 2022*, Michael Brenner, Anamaria Costache, and Kurt Rohloff (Eds.). ACM, 53–63.

[8] Rikke Bendlin and Ivan Damgård. 2010. Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems. In *Theory of Cryptography Conference*. Springer, 201–218.

[9] Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. 2014. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 551–572.

[10] Alexandra Boldyreva. 2003. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In *International Workshop on Public Key Cryptography*. Springer, 31–46.

[11] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter MR Rasmussen, and Amit Sahai. 2018. Threshold cryptosystems from threshold fully homomorphic encryption. In *Annual International Cryptology Conference*. Springer, 565–596.

[12] Cecilia Boschini, Darya Kaviani, Russell WF Lai, Giulio Malavolta, Akira Takahashi, and Mehdi Tibouchi. 2025. Ringtail: practical two-round threshold signatures from learning with errors. In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE, 149–164.

[13] Katharina Boudgoust and Peter Scholl. 2023. Simple Threshold (Fully Homomorphic) Encryption from LWE with Polynomial Modulus. In *Advances in Cryptology – ASIACRYPT 2023*, Jian Guo and Ron Steinfeld (Eds.). Springer Nature Singapore, Singapore, 371–404.

[14] Zvika Brakerski. 2012. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In *Advances in Cryptology – CRYPTO 2012*. Springer Berlin Heidelberg, Berlin, Heidelberg, 868–886.

[15] Zvika Brakerski, Offir Friedman, Avichai Marmor, Dolev Mutzari, Yuval Spiizer, and Ni Trieu. 2025. Threshold FHE with Efficient Asynchronous Decryption. *Cryptology ePrint Archive* (2025).

[16] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. 2014. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)* 6, 3 (2014), 1–36.

[17] Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. 2024. Partially non-interactive two-round lattice-based threshold signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 268–302.

[18] Yijia Chang and Songze Li. 2025. Arbitrary-threshold fully homomorphic encryption with lower complexity. *USENIX Security 2025* (2025).

[19] Jung Hee Cheon, Wonhee Cho, and Jiseung Kim. 2025. Improved universal thresholdizer from iterative shamir secret sharing. *Journal of Cryptology* 38, 1 (2025), 15.

[20] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. 2017. Homomorphic encryption for arithmetic of approximate numbers. In *International conference on the theory and application of cryptology and information security*. Springer, 409–437.

[21] Wonhee Cho, Jiseung Kim, and Changmin Lee. 2024. (In) Security of Threshold Fully Homomorphic Encryption based on Shamir Secret Sharing. *Cryptology ePrint Archive* (2024).

[22] Siddhartha Chowdhury, Sayani Sinha, Animesh Singh, Shubham Mishra, Chandan Chaudhary, Sikhar Patranabis, Pratyay Mukherjee, Ayantika Chatterjee, and Debdeep Mukhopadhyay. 2022. Efficient FHE with Threshold Decryption and Application to Real-Time Systems. *Cryptology ePrint Archive* (2022).

[23] Valerio Cini, Russell WF Lai, and Ivy KY Woo. 2025. Pilvi: Lattice Threshold PKE with Small Decryption Shares and Improved Security. *To appear at ASIACRYPT'25* (2025).

[24] Morten Dahl, Daniel Demmler, Sarah El Kazdadi, Arthur Meyre, Jean-Baptiste Orfila, Dragos Rotaru, Nigel P Smart, Samuel Tap, and Michael Walter. 2023.

Noah's ark: Efficient threshold-fhe using noise flooding. In *Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*. 35–46.
[25] Alfredo De Santis, Yvo Desmedt, Yair Frankel, and Moti Yung. 1994. How to share a function securely. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*. ACM, 522–533.
[26] Rafaël Del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani Saarinen. 2024. Threshold raccoon: practical threshold signatures from standard lattice assumptions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 219–248.
[27] Yvo Desmedt and Yair Frankel. 1989. Threshold Cryptosystesns. *Advance in Cryptology* (1989), 305–315.
[28] Junfeng Fan and Frederik Vercauteren. 2012. Somewhat Practical Fully Homomorphic Encryption. Cryptology ePrint Archive, Paper 2012/144. https://eprint.iacr.org/2012/144
[29] Hossein Fereidooni, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Helen Möllering, Thien Duc Nguyen, Phillip Rieger, Ahmad-Reza Sadeghi, Thomas Schneider, Hossein Yalame, et al. 2021. SAFELearn: Secure aggregation for private federated learning. In *2021 IEEE security and privacy workshops (SPW)*. IEEE, 56–62.
[30] Yair Frankel. 1989. A practical protocol for large group oriented networks. In *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 56–61.
[31] David Froelicher, Hyunghoon Cho, Manaswitha Edupalli, Joao Sa Sousa, Jean-Philippe Bossuat, Apostolos Pyrgelis, Juan Ramón Troncoso-Pastoriza, Bonnie Berger, and Jean-Pierre Hubaux. 2023. Scalable and Privacy-Preserving Federated Principal Component Analysis. In *S&P 2023*. IEEE, 1908–1925.
[32] David Froelicher, Juan R Troncoso-Pastoriza, Apostolos Pyrgelis, Sinem Sav, Joao Sa Sousa, Jean-Philippe Bossuat, and Jean-Pierre Hubaux. 2021. Scalable Privacy-Preserving Distributed Learning. *Proceedings on Privacy Enhancing Technologies* 2 (2021), 323–347.
[33] Walter Gautschi. 1963. On inverses of Vandermonde and confluent Vandermonde matrices. II. *Numer. Math.* 5, 1 (1963), 425–430.
[34] Kamil Doruk Gur, Jonathan Katz, and Tjerand Silde. 2024. Two-round threshold lattice-based signatures from threshold homomorphic encryption. In *International Conference on Post-Quantum Cryptography*. Springer, 266–300.
[35] Xiaohan Hao, Chao Lin, Wenhan Dong, Xinyi Huang, and Hui Xiong. 2023. Robust and secure federated learning against hybrid attacks: A generic architecture. *IEEE Transactions on Information Forensics and Security* 19 (2023), 1576–1588.
[36] Zhenkai Hu, Haofei Liang, Xiao Wang, Xiang Xie, Kang Yang, Yu Yu, and Wenhao Zhang. 2025. Ajax: Fast Threshold Fully Homomorphic Encryption without Noise Flooding. *Cryptology ePrint Archive* (2025).
[37] Michael Klooß, Russell WF Lai, Ngoc Khanh Nguyen, and Michał Osadnik. 2024. RoK, paper, SISsors toolkit for lattice-based succinct arguments. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 203–235.
[38] Oleksandra Lapiha and Thomas Prest. 2025. A Lattice-Based IND-CCA Threshold KEM from the BCHK+ Transform. *To appear at Asiacrypt'25* (2025).
[39] Daniele Micciancio and Adam Suhl. 2025. Simulation-Secure Threshold PKE from LWE with Polynomial Modulus. *IACR Communications in Cryptology* 1, 4 (2025).
[40] Christian Mouchet, Elliott Bertrand, and Jean-Pierre Hubaux. 2023. An efficient threshold access-structure for rlwe-based multiparty homomorphic encryption. *Journal of Cryptology* 36, 2 (2023), 10.
[41] Hiroki Okada and Tsuyoshi Takagi. 2025. Low Communication Threshold FHE from Standard (Module-) LWE. *To appear at Asiacrypt'25* (2025).
[42] Alain Passelègue and Damien Stehlé. 2024. Low communication threshold fully homomorphic encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 297–329.
[43] Sinem Sav, Apostolos Pyrgelis, Juan R Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuat, Joao Sa Sousa, and Jean-Pierre Hubaux. 2020. POSEIDON: Privacy-preserving federated neural network learning. *NDSS Symposium* (2020).
[44] Adi Shamir. 1979. How to share a secret. *Commun. ACM* 22, 11 (1979), 612–613.
[45] Victor Shoup. 2000. Practical threshold signatures. In *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 207–220.
[46] Haris Smajlovic, David Froelicher, Ariya Shajii, Bonnie Berger, Hyunghoon Cho, and Ibrahim Numanagic. 2025. Shechi: A Secure Distributed Computation Compiler Based on Multiparty Homomorphic Encryption. In *USENIX Security 2025*, Lujo Bauer and Giancarlo Pellegrino (Eds.). USENIX Association, 7703–7722.
[47] Haibo Tian, Yanchuan Wen, Fangguo Zhang, Yunfeng Shao, and Bingshuai Li. 2022. A distributed threshold additive homomorphic encryption for federated learning with dropout resiliency based on lattice. In *International Symposium on Cyberspace Safety and Security*. Springer, 277–292.
[48] Narasimha Raghavan Veeraragavan, Svetlana Boudko, and Jan Franz Nygård. 2024. A Multiparty Homomorphic Encryption Approach to Confidential Federated Kaplan Meier Survival Analysis. *CoRR* abs/2412.20495 (2024).
[49] Guy Zyskind, Doron Zarchy, Max Leibovich, and Chris Peikert. 2025. High-Throughput Universally Composable Threshold FHE Decryption. *ACM CCS 2025* (2025).

A Definitions of FHE and ThFHE

In this section, we provide the formal definitions of FHE and ThFHE schemes. We begin by recalling the formal definition of a fully homomorphic encryption (FHE) scheme. An FHE scheme consists of the following four probabilistic polynomial-time (PPT) algorithms $\mathsf{FHE} = (\mathsf{FHE.Setup}, \mathsf{FHE.Enc}, \mathsf{FHE.Eval}, \mathsf{FHE.Dec})$:

- $\mathsf{FHE.Setup}(1^\lambda, 1^d)$: Given the security parameter λ and a depth bound d, it outputs a public key pk and a secret key sk.
- $\mathsf{FHE.Enc}(\mathsf{pk}, m)$: Given the public key pk and a message m, it outputs a ciphertext ct.
- $\mathsf{FHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k)$: Given the public key pk, a circuit C of depth at most d, and ciphertexts $\mathsf{ct}_1, \ldots, \mathsf{ct}_k$, it outputs an evaluated ciphertext $\mathsf{ct}_{\mathsf{out}}$.
- $\mathsf{FHE.Dec}(\mathsf{pk}, \mathsf{sk}, \mathsf{ct})$: Given the public key pk, the secret key sk, and a ciphertext ct, it outputs the decrypted message m'.

An FHE scheme must satisfy the standard properties of compactness, correctness, and security, which are formally defined as follows.

Definition A.1 (Compactness of FHE). *An FHE scheme* FHE *is said to be compact if there exists a polynomial* $\mathsf{poly}(\cdot)$ *such that, for any security parameter* λ*, any depth bound* d*, any circuit* $C : \mathcal{M}^k \to \mathcal{M}$*, and any message* m_i *for* $i \in [k]$*, we have* $|\mathsf{ct}| \le \mathsf{poly}(\lambda, d)$ *where* $\mathsf{FHE.Setup}(1^\lambda, 1^d) \to (\mathsf{pk}, \mathsf{sk})$*,* $\mathsf{FHE.Enc}(\mathsf{pk}, m_i) \to \mathsf{ct}_i$ *for* $i \in [k]$*, and* $\mathsf{FHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k) \to \mathsf{ct}$.

Definition A.2 (Correctness of FHE). *An FHE scheme* FHE *is said to be correct if, for any security parameter* λ*, any depth bound* d*, any circuit* $C : \mathcal{M}^k \to \mathcal{M}$*, and any message* m_i *for* $i \in [k]$*, it holds that*

$$\Pr[\mathsf{FHE.Dec}(\mathsf{pk}, \mathsf{sk}, \mathsf{ct}) = C(m_1, \ldots, m_k)] = 1 - \mathsf{negl}(\lambda)$$

where $\mathsf{FHE.Setup}(1^\lambda, 1^d) \to (\mathsf{pk}, \mathsf{sk})$*,* $\mathsf{FHE.Enc}(\mathsf{pk}, m_i) \to \mathsf{ct}_i$ *for* $i \in [k]$*, and* $\mathsf{FHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k) \to \mathsf{ct}$.

Definition A.3 (IND-CPA Security of FHE). *An FHE scheme* FHE *is said to be IND-CPA secure if, for any security parameter* λ *and any depth bound* d*, there exists no PPT adversary* $\mathcal{A}$ *for which the following experiment outputs* 1 *with non-negligible probability.*

(1) The challenger $\mathcal{C}$ *runs* $\mathsf{FHE.Setup}(1^\lambda, 1^d) \to (\mathsf{pk}, \mathsf{sk})$*, passes* pk *to* $\mathcal{A}$*, and then obtains two messages* m_0, m_1 *chosen by* $\mathcal{A}$*.* $\mathcal{C}$ *samples a random bit* $b \in \{0, 1\}$ *and runs* $\mathsf{FHE.Enc}(\mathsf{pk}, m_b) \to \mathsf{ct}$*. The ciphertext* ct *is given to* $\mathcal{A}$ *as the challenge ciphertext.*
(2) $\mathcal{A}$ *outputs* b'*. The experiment outputs* 1 *if* $b = b'$*, and* 0 *otherwise.*

Next, the definitions of compactness, correctness, and security for ThFHE schemes, omitted from the main body for clarity, are provided here for completeness. They follow the standard formulation adopted in prior ThFHE work [11].

Definition A.4 (Compactness of ThFHE). *A ThFHE scheme* ThFHE *is said to be compact if there exists polynomials* $\mathsf{poly}_1(\cdot)$ *and* $\mathsf{poly}_2(\cdot)$ *such that, for any security parameter* λ*, any depth bound* d*, any circuit* $C : \mathcal{M}^k \to \mathcal{M}$*, and any message* m_i *for* $i \in [k]$*, we have*

$$|\mathsf{ct}| \le \mathsf{poly}_1(\lambda, d) \quad \text{and} \quad |\mathsf{p}_j| \le \mathsf{poly}_2(\lambda, d, N)$$

for any $j \in [N]$, *where* $\mathsf{ThFHE.Setup}(1^\lambda, 1^d, \mathbb{A}) \to (\mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$, $\mathsf{ThFHE.Enc}(\mathsf{pk}, m_i) \to \mathsf{ct}_i$ *for* $i \in [k]$, $\mathsf{ThFHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k) \to \mathsf{ct}$, *and* $\mathsf{ThFHE.PartDec}(\mathsf{pk}, \mathsf{ct}, \mathsf{sk}_j) \to \mathsf{p}_j$.

Definition A.5 (Correctness of ThFHE). *A ThFHE scheme* ThFHE *is said to be correct if, for any security parameter* λ, *any depth bound* d, *any access structure* $\mathbb{A}$, *any circuit* $C : \mathcal{M}^k \to \mathcal{M}$, *and any message* m_i *for* $i \in [k]$, *it holds that the probability that*

$$\mathsf{ThFHE.FinDec}(\mathsf{pk}, \{\mathsf{ThFHE.PartDec}(\mathsf{pk}, \mathsf{ct}, \mathsf{sk}_i)\}_{i\in S}) \to C(m_1, \ldots, m_k)$$

is $1-\mathsf{negl}(\lambda)$, *where* $S \in \mathbb{A}$, $\mathsf{ThFHE.Setup}(1^\lambda, 1^d, \mathbb{A}) \to (\mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$, $\mathsf{ThFHE.Enc}(\mathsf{pk}, m_i) \to \mathsf{ct}_i$ *for* $i \in [k]$, *and* $\mathsf{ThFHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k) \to \mathsf{ct}$.

Now, we present the formal definition of security in the *simulation-based* paradigm.

Definition A.6 (Simulation Security of ThFHE). *A ThFHE scheme* ThFHE *achieves simulation-based security with security parameter* λ, *depth bound* d, *and access structure* $\mathbb{A}$ *if, for any PPT adversary* $\mathcal{A}$, *there exists a stateful PPT simulator* $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ *such that the real and ideal experiments* $\mathsf{Exp}^{\mathcal{A},\mathsf{Real}}(1^\lambda, 1^d)$ *and* $\mathsf{Exp}^{\mathcal{A},\mathsf{Ideal}}(1^\lambda, 1^d)$ *are computationally indistinguishable.*

Real Experiment $\mathsf{Exp}^{\mathcal{A},\mathsf{Real}}(1^\lambda, 1^d)$*:*

1. *Given the security parameter* λ *and the depth bound* d, $\mathcal{A}$ *outputs an access structure* $\mathbb{A} \in \mathbb{S}$.
2. *The challenger* $\mathcal{C}$ *runs* $\mathsf{ThFHE.Setup}(1^\lambda, 1^d, \mathbb{A}) \to (\mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$ *and sends* pk *to* $\mathcal{A}$.
3. $\mathcal{A}$ *outputs a maximal invalid party set* $S^* \subseteq \{P_1, \ldots, P_N\}$ *and messages* $m_1, \ldots, m_k \in \mathcal{M}$ *from the message space* $\mathcal{M}$ *of the ThFHE scheme.*
4. $\mathcal{C}$ *passes* $\{\mathsf{sk}_i\}_{i\in S^*}$ *and* $\{\mathsf{ThFHE.Encrypt}(\mathsf{pk}, m_i)\}_{i\in[k]}$ *to* $\mathcal{A}$.
5. $\mathcal{A}$ *issues a polynomial number of adaptive queries* $(S \subseteq \{P_1, \ldots, P_N\}, C)$, *where* $C : \mathcal{M}^k \to \mathcal{M}^\ell$ *is a circuit of depth at most* d. *For each query,* $\mathcal{C}$ *computes*
$$\mathsf{ThFHE.Eval}(\mathsf{pk}, C, \mathsf{ct}_1, \ldots, \mathsf{ct}_k) \to \hat{\mathsf{ct}}$$
and sends partial decryptions $\{\mathsf{ThFHE.PartDec}(\mathsf{pk}, \hat{\mathsf{ct}}, \mathsf{sk}_i)\}_{i\in S}$ *to* $\mathcal{A}$.
6. *Finally,* $\mathcal{A}$ *outputs a distinguishing bit* b.

Ideal Experiment $\mathsf{Exp}^{\mathcal{A},\mathsf{Ideal}}(1^\lambda, 1^d)$*:*

1. *Given the security parameter* λ *and the depth bound* d, $\mathcal{A}$ *outputs an access structure* $\mathbb{A} \in \mathbb{S}$.
2. $\mathcal{C}$ *runs* $\mathcal{S}_1(1^\lambda, 1^d, \mathbb{A}) \to (\mathsf{pk}, \mathsf{sk}_1, \ldots, \mathsf{sk}_N)$ *and sends* pk *to* $\mathcal{A}$.
3. $\mathcal{A}$ *outputs a maximal invalid party set* $S^* \subseteq \{P_1, \ldots, P_N\}$ *and messages* $m_1, \ldots, m_k \in \mathcal{M}$.
4. $\mathcal{C}$ *passes* $\{\mathsf{sk}_i\}_{i\in S^*}$ *and* $\{\mathsf{ThFHE.Encrypt}(\mathsf{pk}, m_i)\}_{i\in[k]}$ *to* $\mathcal{A}$.
5. *For each query* (S, C) *made by* $\mathcal{A}$, $\mathcal{C}$ *invokes the simulator*
$$\mathcal{S}_2\big(C, \{\mathsf{ct}_1, \ldots, \mathsf{ct}_k\}, C(m_1, \ldots, m_k), S, \mathsf{st}\big) \to \{\mathsf{p}_i\}_{i\in S}$$
and returns $\{\mathsf{p}_i\}_{i\in S}$ *to* $\mathcal{A}$.
6. *Finally,* $\mathcal{A}$ *outputs a distinguishing bit* b.

B Missing Proofs

In this section, we present the proofs that were omitted from the main body of the paper.

B.1 Proof of the Case $t = 2$ in Theorem 3.2

Suppose $t = 2$. We then have $\Delta = 2^{\lceil \log_2 2 \rceil} = 2$ and a t-subset is $T = \{\alpha_i, \alpha_j\}$. The Lagrange coefficient for j at 0 is

$$\lambda_j^{(T)}(0) = \frac{0 - \alpha_i}{\alpha_j - \alpha_i}.$$

We analyze its slot-wise ℓ_∞-norm after scaling by Δ and applying the canonical embedding σ_ℓ which maps $\omega \to \omega^{2\ell+1}$. Then, we have

$$\begin{aligned}\max_{\ell,T}\left|\sigma_\ell\left(\Delta \cdot \lambda_j^{(T)}(0)\right)\right| &= \max_{\ell,T}\left|2 \cdot \frac{-\sigma_\ell(\alpha_i)}{\sigma_\ell(\alpha_j) - \sigma_\ell(\alpha_i)}\right| \\ &\le \max_{\ell,T}\left|2 \cdot \frac{1}{|\sigma_\ell(\alpha_j) - \sigma_\ell(\alpha_i)|}\right| \\ &= \max_{d_\ell}\left|2 \cdot \frac{1}{2|\sin(\pi d_\ell / M)|}\right|\end{aligned}$$

where $d_\ell = \min(c_\ell \bmod M, M - c_\ell \bmod M)$ with $c_\ell = |(2\ell+1)(b_i - b_j)|$. The last equality holds since

$$\begin{aligned}|\sigma_\ell(\alpha_j - \alpha_i)| &= |\omega^{(2\ell+1)b_j} - \omega^{(2\ell+1)b_i}| \\ &= |\omega^{(2\ell+1)(b_j - b_i)} - 1| = 2\left|\sin(\pi d_\ell / M)\right|.\end{aligned}$$

The maximum occurs when the denominator is minimized. Under the worst-case, the minimum distance is $d_\ell = 1$. Thus, the maximum value is bounded by

$$\frac{1}{\sin(\pi/M)} \le \frac{1}{2/M} = \frac{M}{2} < \Delta\left(\frac{M}{2}\right) \cdot \frac{1}{(0!)^2}$$

using $\sin(x) \ge 2x/\pi$ for $x = \pi/M \le \pi/2$.

B.2 Proof of Corollary 3.3

From the definition of V_T^{-1}, for any T, $\Delta \sum_{j\in T} \lambda_j^{(T)}$ corresponds to $\|\Delta \cdot (1, 0, \ldots, 0) \cdot V_T^{-1}\|$. Moreover, by the norm relation from [23, Lemma 2], we know

$$\begin{aligned}\|V_T^{-1}\|^2 = \max_{\mathbf{x}} \frac{\|V_T^{-1}\mathbf{x}\|^2}{\|\mathbf{x}\|^2} &= \max_{\mathbf{x}} \frac{\sum_\ell \|\sigma_\ell(V_T^{-1})\sigma_\ell(\mathbf{x})\|^2}{\sum_\ell \|\sigma_\ell(\mathbf{x})\|^2} \\ &\le \max_{\mathbf{x}} \frac{\sum_\ell \|\sigma_\ell(V_T^{-1})\|^2 \|\sigma_\ell(\mathbf{x})\|^2}{\sum_\ell \|\sigma_\ell(\mathbf{x})\|^2} \\ &\le \max_\ell \|\sigma_\ell(V_T^{-1})\|^2 \le t \cdot \max_\ell \|\sigma_\ell(V_T^{-1})\|_\infty^2,\end{aligned}$$

which implies $\rho(t) \le \sqrt{t} \cdot \Delta(t) \cdot \left(\frac{M}{2}\right)^{t-1} \cdot \frac{1}{(\lfloor \frac{t-1}{2} \rfloor !)^2}$. Since $\rho(t) \le \max_T \sum_{j\in T} \|\Delta \cdot \lambda_j^{(T)}\| \le \sqrt{t}\rho(t)$, we complete the proof.

B.3 Proof of Lemma 4.2

By the correctness of the refined Shamir SSS, $\sum_{i\in T} \lambda_i^{(T)} \mathsf{sk}_i = \mathsf{sk}$. Hence,

$$\sum_{i\in T} \lambda_i^{(T)} \langle \mathsf{ct}, \mathsf{sk}_i \rangle = \langle \mathsf{ct}, \mathsf{sk} \rangle = \left\lfloor \frac{Q}{2} m \right\rceil + \Delta^2 e.$$

Adding the smudging terms yields (6). If the infinity norm of the total error remains below the rounding threshold, i.e., the condition in (7), then the final decryption algorithm correctly outputs m.

To derive (8), we apply a coordinate-wise bound under the canonical embedding:

$$\max_T \sum_{i\in T} \left\| \Delta\lambda_i^{(T)} e_i \right\| \le \max_T \sum_{i\in T} \|\Delta\lambda_i^{(T)}\| \cdot \|e_i\|_\infty \le \Lambda \cdot B_{\mathsf{sm}}.$$

Multiplying by Δ and combining with $\|e\|_\infty \le B$ yields the correctness condition in (8).

C Security of Construction 4.1

The security of Construction 4.1 is directly derived from previous works [11, 21], since the only differences between our work and theirs lie in the definitions of Δ and the Lagrange coefficients. In previous constructions, Δ was defined as $(N!)^2$, whereas in our work it is defined as $2^{\lceil \log_2 t \rceil}$. Furthermore, the authors of [21] showed that, for an error term of the form $\Delta^\alpha e + \Delta^\beta \lambda_i e_i$, if $\alpha \ge \beta + 1$, then the ThFHE scheme remains secure.[9] By setting $(\alpha, \beta) = (2, 1)$, their argument continues to hold for our construction; thus, we do not reanalyze the security of the ThFHE scheme in detail. Our focus in this section is instead on demonstrating the efficiency improvements achieved by our refined approach over R_Q.

Remark C.1 (Attack Idea of [21]). For completeness, we briefly recall the core attack idea from [21]. Under a setting with $t-1$ corrupted parties and one honest party h, the adversary aims to recover the value

$$Z = \Delta^2 e + \Delta\lambda_h e_h \in R,$$

where e is the centralized decryption error, e_h is the honest party's smudging error, and λ_h is the Lagrange coefficient at 0 for h. Writing λ_h in lowest terms as a rational function over R,

$$\lambda_h = \frac{B(X)}{A(X)} \quad \text{with} \quad \gcd(A, B) = 1 \text{ in } R,$$

one can express $A(X) \cdot Z = \Delta^2 A(X) e + \Delta B(X) e_h$. If $B(X)$ is not a unit in R, then reducing $A(X) \cdot Z$ modulo $B(X)$ can reveal partial information about e under certain conditions, which constitutes the core idea of the attack described in [21].[10] In our construction, however, each $B(X) = \omega^{b_i}$ is a unit in R, which ensures that reduction modulo $B(X)$ yields no information about e.

D Supplementary Tables for Experimental Results

In this section, we provide experimental results that go beyond the trend illustrations presented in Section 5. Table 3 presents a runtime comparison of distributed decryption between our ThFHE and CL25's ThFHE, whose overall trends are depicted in Figure 3. Distributed decryption consists of PartDec and FinDec, and we report their sum as the total time in the table. As noted earlier, distributed decryption in CL25 [18] follows a two-round protocol, which we denote as R1 and R2. In both rounds, we treat the per-party computation as PartDec and aggregator-side computation as FinDec.

Table 3: Runtime comparison of distributed decryption between ours and CL25 (ms)

(N, t)	PartDec			FinDec			**Total**	
	Ours	CL25		Ours	CL25		Ours	CL25
		R1	R2		R1	R2		
(32, 5)	1.31	7.53	0.06	2.00	0.01	0.07	3.31	7.67
(32, 10)	1.26	14.96	0.11	4.81	0.02	0.15	6.07	15.24
(32, 16)	1.29	27.63	0.16	9.49	0.04	0.27	10.78	28.10
(32, 21)	1.19	39.71	0.21	5.80	0.07	0.39	6.99	40.38
(64, 5)	1.26	13.90	0.06	2.00	0.01	0.07	3.26	14.04
(64, 6)	1.26	15.80	0.07	2.47	0.01	0.08	3.73	15.96
(64, 21)	2.47	78.80	0.22	25.52	0.08	0.37	27.99	79.47
(64, 32)	1.26	139.56	0.33	32.09	0.17	0.65	33.35	140.71
(64, 42)	1.27	193.94	0.42	52.05	0.30	0.96	53.32	195.62
(128, 5)	1.27	25.89	0.06	2.05	0.01	0.06	3.32	26.02
(128, 7)	1.26	35.94	0.08	3.14	0.01	0.09	4.40	36.12
(128, 42)	2.76	395.09	0.42	99.46	0.31	1.03	102.22	396.85
(128, 64)	2.84	634.97	0.62	203.74	0.70	2.01	206.58	638.30
(128, 85)	2.92	869.61	0.82	338.37	1.20	3.30	341.29	874.93
(256, 5)	1.34	51.75	0.06	2.17	0.01	0.06	3.51	51.88
(256, 8)	2.78	87.60	0.09	9.09	0.02	0.11	11.87	87.82
(256, 85)	6.04	1752.13	0.84	595.30	1.23	3.37	601.34	1757.57
(256, 128)	6.05	2686.15	1.23	1209.00	2.66	6.78	1215.05	2696.82
(256, 170)	2.91	3612.97	1.64	1271.32	4.61	11.42	1274.23	3630.64
(512, 5)	1.32	103.41	0.06	2.20	0.01	0.07	3.52	103.55
(512, 9)	2.82	207.45	0.10	12.19	0.02	0.13	15.01	207.70
(512, 170)	16.20	7244.62	1.66	5989.26	4.75	11.54	6005.46	7262.57
(512, 256)	7.53	10973.01	2.48	14084.17	10.50	24.51	14091.70	11010.50
(512, 341)	5.73	14723.78	3.28	6908.96	18.48	42.47	6914.69	14788.01

Table 4 provides a comprehensive comparison between ThFHE instantiations for our scheme and BGG$^+$18. It reports the parameter choices used in the experiments (aligned with Table 2) and the running times of the ThFHE algorithms in milliseconds, complementing the trends previously shown in Figure 2.

[9] In [21], the authors required that $\alpha \ge \beta + 2$. However, for our purpose it suffices to assume $\alpha \ge \beta + 1$ since $\Delta^\alpha e + \Delta^\beta \lambda_i e_i = \Delta^\beta \lambda_i (e \cdot e' + e_i)$ for some $e' \in R$ and a distribution of e_i is statistically close to that of $e \cdot e'$ when $\|e_i\|$ is superpolynomially larger than $\|e \cdot e'\|$.

[10] In fact, the attack presented in [21] was conducted under a different setting. Specifically, their attack targeted an LWE-based ThFHE scheme, where all values are represented as integer vectors.

Table 4: ThFHE experimental results

(N, t)	n		$\log_2 Q$		Setup		Enc		PartDec†		FinDec	
	BGG⁺18	**Ours**	BGG⁺18	**Ours**	BGG⁺18	**Ours**	BGG⁺18	**Ours**	BGG⁺18	**Ours**	BGG⁺18	**Ours**
$(32, 5)$	2^{15}	2^{12}	484	62	278.31	2.17	22.64	0.93	17.69	1.31	9.63	2.00
$(32, 10)$	2^{15}	2^{12}	484	68	601.90	5.07	22.64	0.92	17.53	1.26	16.64	4.81
$(32, 16)$	2^{15}	2^{12}	484	62	961.66	6.34	22.23	0.95	17.33	1.29	25.33	9.49
$(32, 21)$	2^{15}	2^{12}	484	58	1245.06	5.43	22.36	0.69	17.30	1.19	32.35	5.80
$(64, 5)$	2^{16}	2^{12}	1200	66	2633.47	3.66	94.85	0.92	58.70	1.26	39.37	2.00
$(64, 6)$	2^{16}	2^{12}	1200	72	3340.64	4.41	95.01	0.93	59.11	1.26	45.31	2.47
$(64, 21)$	2^{16}	2^{13}	1200	90	12320.48	35.06	95.97	1.83	58.00	2.47	119.41	25.52
$(64, 32)$	2^{16}	2^{12}	1200	80	19078.04	24.34	95.14	0.94	56.89	1.26	166.42	32.09
$(64, 42)$	2^{16}	2^{12}	1200	70	25165.37	31.88	93.79	0.98	56.31	1.27	206.57	52.05
$(128, 5)$	–	2^{12}	–	70	–	6.20	–	0.94	–	1.27	–	2.05
$(128, 7)$	–	2^{12}	–	80	–	8.78	–	0.95	–	1.26	–	3.14
$(128, 42)$	–	2^{13}	–	135	–	179.05	–	2.43	–	2.76	–	99.46
$(128, 64)$	–	2^{13}	–	111	–	273.55	–	2.65	–	2.84	–	203.74
$(128, 85)$	–	2^{13}	–	93	–	332.74	–	2.77	–	2.92	–	338.37
$(256, 5)$	–	2^{12}	–	74	–	11.01	–	0.96	–	1.34	–	2.17
$(256, 8)$	–	2^{13}	–	92	–	71.26	–	2.25	–	2.78	–	9.09
$(256, 85)$	–	2^{14}	–	220	–	2101.42	–	7.46	–	6.04	–	595.30
$(256, 128)$	–	2^{14}	–	180	–	3110.74	–	7.79	–	6.05	–	1209.00
$(256, 170)$	–	2^{13}	–	138	–	1290.33	–	3.44	–	2.91	–	1271.32
$(512, 5)$	–	2^{12}	–	80	–	20.34	–	0.97	–	1.32	–	2.20
$(512, 9)$	–	2^{13}	–	104	–	185.86	–	2.50	–	2.82	–	12.19
$(512, 170)$	–	2^{15}	–	396	–	32456.19	–	21.99	–	16.20	–	5989.26
$(512, 256)$	–	2^{14}	–	308	–	16297.05	–	9.58	–	7.53	–	14084.17
$(512, 341)$	–	2^{14}	–	232	–	12374.86	–	6.45	–	5.73	–	6908.96

† measured per party.