Asynchronous Shamir-Based Threshold FHE: Smaller Moduli and Strong Simulation Security

Won Kim[1], Changmin Lee[1], JeongHwan Lee[1],
Alain Passelègue[2], and Damien Stehlé*[3]

[1] Korea University, Seoul, Republic of Korea
[2] CryptoLab Inc., Lyon, France,
[3] PQShield, Oxford, United Kingdom

Abstract. We study t-out-of-n threshold fully homomorphic encryption (ThFHE) based on Shamir secret sharing (SSS) in the asynchronous setting. With SSS, a partial decryption share is a single ring element; this allows to avoid the large number of ring elements stored per party required by prior strongly secure constructions based on $\{0, 1\}$ reconstruction coefficients. However, this reduction introduces a fundamental trade-off: Lagrange reconstruction during distributed decryption severely amplifies noise, forcing a substantially larger ciphertext modulus.
In this work, we give SSS-based asynchronous ThFHE constructions over standard RLWE-based FHE schemes (BFV, BGV, and CKKS) for both standard and strong simulation security. Through tight analysis of the modulus constraints, our constructions simultaneously reduce the required modulus, compared with prior asynchronous Shamir-based constructions, and the per-party storage, compared with the prior strongly secure construction. For example, for $n = 512$ under standard simulation security, our analysis reduces the modulus overhead of distributed decryption by 33% at $t = n/2$ and by up to 90% for t close to n, relative to the prior works. Under strong simulation security, the per-party storage for $n = 16$ and $t = 8$ at 128-bit security drops from 79 GB in prior work to 897 KB.

1 Introduction

Fully homomorphic encryption (FHE) has matured significantly over the past decade, with efficient and highly parallelizable schemes such as BGV [BGV12], BFV [Bra12,FV12], and CKKS [CKKS17]. It now enables scalable private computation over real/complex or discrete data. Yet, in many real-world scenarios, the decryption secret key should not reside on a single device. Threshold fully homomorphic encryption (ThFHE) addresses this by distributing the decryption capability across multiple parties [AJLA+12,BGG+18]. This mitigates single-point compromise and reduces the risk of a single point of failure. In the t-out-of-n setting, any subset of t eligible parties can jointly decrypt, while any subset of at most $t - 1$ of them learns nothing about the encrypted data. In

* This work was conducted while the author was affiliated with CryptoLab Inc.

addition to enabling secure key management, ThFHE also enables secure multi-party computation. Each party can encrypt their private data using ThFHE so that it is possible to compute over their joint encrypted data, while threshold decryption limits access to data by requiring t parties to agree before being able to decrypt a ciphertext.

ThFHE extends the standard FHE syntax by splitting the decryption algorithm into a 2-round threshold decryption protocol. Specifically, a ThFHE scheme is a tuple $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{PartDec}, \mathsf{FinDec})$, which satisfies the following: KeyGen outputs a public key pk and n secret key shares $(\mathsf{sk}_i)_{i\in[n]}$. Each party P_i for $i \in [n]$ is given a share sk_i, which allows them to participate in the 2-round threshold decryption of a ciphertext ct as follows:

1. Party P_i produces a *decryption share* p_i by running $\mathsf{p}_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$;
2. Given t decryption shares from t distinct parties, one can recover the underlying plaintext by running $\mathsf{FinDec}(\mathsf{ct}, (\mathsf{p}_i)_{i\in\mathcal{S}})$, where $\mathcal{S} \subseteq [n]$ denotes the set of t participants.

In this work, we focus on the asynchronous setting, in which a party running $\mathsf{PartDec}$ does not know who is participating in threshold decryption when producing its decryption share. In particular, this requires that any set of t decryption shares from t distinct participants can be combined to decrypt. This is in contrast with the synchronous setting, which assumes that the set of t participants is known by parties when they run $\mathsf{PartDec}$, so that these t shares are meant to be combined together. This setting simplifies the design considerably, and several constructions exploit it [MTBH21,MBH23,CPS26], but it requires the deployment infrastructure to fix the decryptor set in advance.

In order to build a ThFHE scheme, the common approach is to exploit the fact that the FHE decryption equation is linear in the secret key, up to a final rounding step, in combination with a linear secret sharing scheme (LSSS). Recall that an LSSS allows one to share a secret, in this case the FHE secret key sk, among n parties by distributing each share sk_i to each party P_i so that any t distinct shares $(\mathsf{sk}_{i_j})_{j\in[t]}$ can be recombined to obtain sk via a linear equation $\mathsf{sk} = \sum_{j\in[t]} L_{i_j}\mathsf{sk}_{i_j}$, where $\{L_{i_j}\}_{j\in[t]}$ are publicly computable from the set of participants $\mathcal{S} = \{i_1, \ldots, i_t\}$, which is known only at FinDec in the asynchronous setting. Using an LSSS, $\mathsf{PartDec}$ is implemented by having each party P_i run the FHE decryption using sk_i to produce a decryption share; FinDec then linearly combines t distinct decryption shares, and decodes the result to extract a plaintext. For security, each party further needs to add noise during $\mathsf{PartDec}$. This noise masks the exact linear relationship between the decryption share and sk_i, preventing trivial key-recovery attacks via linear equation solving.

This approach has been considered with various LSSS-based ThFHE constructions [BGG$^+$18,BS23]. Having an LSSS whose reconstruction coefficients are binary makes it simpler to achieve correctness and security. However, known constructions with binary reconstruction have very large per-party storage: each party stores $O(n^{4.2})$ elements of the same type as the secret key. This makes them impractical even for a moderate number of parties. On the other hand, an alternative line of research relies on Shamir secret sharing(SSS). In this ap-

proach, only a single element of the same type as the secret key per party is required to realize a ThFHE scheme. [4]

The price of this compactness is paid in correctness. Unlike binary reconstruction coefficients, the reconstruction coefficients of SSS—known as Lagrange coefficients—can be large, and the noise that each party adds during PartDec is scaled by them when the decryption shares are combined. This necessitates a significantly larger ciphertext modulus to accommodate the noise amplification introduced by the Lagrange coefficients.

Security is formulated in two simulation-based notions, both stated against an adversary that statically corrupts up to $t-1$ parties. In both notions, security requires the existence of an efficient simulator that, without access to any honest secret-key shares, outputs decryption shares computationally indistinguishable from the real honest decryption shares. The honest shares therefore carry no information about the honest keys beyond what the adversary already holds.

The two notions differ in which decryption-share queries the adversary is allowed to make, and the plaintext therefore reaches the simulator at different points. In the standard notion of [BGG$^+$18], the adversary queries the honest shares on a ciphertext whose decryption has been authorized, so that all t shares are to be released and the plaintext revealed. The plaintext is thus fixed before the first honest share, and the simulator is given it up front. In the *strong simulation security* of Ebrahimi and Yadav [EY24], the adversary may query decryption shares on ciphertexts of its own choice, one share at a time, without any of them reaching the threshold. The simulator then receives the plaintext of a ciphertext only when the t-th share on it is queried, and must answer queries for up to $t-1$ shares (including those of the corrupted parties) without access to the plaintext. Of the two, only the standard notion has so far been achieved by Shamir-based constructions [BFM$^+$25,CLW25]. In contrast, the only construction achieving the strong notion [EY24] relies on $\{0,1\}$-LSSS built over the specialized FHE scheme of [BGG$^+$18] and the (almost) key-homomorphic pseudorandom function of [BLMR15]. Consequently, this design cannot be generically extended to other FHE schemes such as CKKS.

This raises the question of what a Shamir-based scheme costs under each notion: how small the ciphertext modulus can be made for the standard notion, and whether such a scheme exists for the strong one, at what per-party storage and ciphertext modulus. We answer both.

1.1 Contributions

Our contributions are as follows.

Generic Shamir-based Asynchronous ThFHE. We propose a Shamir-based asynchronous ThFHE construction that leaves the underlying FHE algorithms

[4] ThFHE based on LSSS with binary reconstruction and SSS also induce different ciphertext-modulus constraints. Hence, our reference point (counting the secret key as "one element") for comparison is biased. Nevertheless, it is a reasonable baseline for comparing per-party storage.

unchanged, enabling generic instantiation over standard RLWE-based FHE schemes such as BFV, BGV, and CKKS. By separating the two roles of the public scaling factor of threshold decryption—clearing the Lagrange denominators during reconstruction, and shaping the flooding noise for simulation—we establish rigorous sufficient conditions for correctness and for simulation security against $t-1$ static corruptions, without relying on the special FHE of [BGG$^+$18].

Explicit bounds for the Lagrange-reconstruction overhead. We derive explicit worst-case bounds on the Lagrange-coefficient norms governing these conditions, for the integer (Section 3.5), centered-integer (Section 3.6), and monomial (Section 3.7) interpolation sets. The integer set serves as a warm-up: directly tracking the Lagrange coefficients yields explicit factorial-type bounds and a clean baseline for the modulus overhead in this regime. Our main technical contribution is the analysis of the monomial set in a power-of-two cyclotomic ring, yielding trigonometric-product bounds on the dominant modulus-overhead term; our experiments indicate that these bounds are close to tight (Section 6.1). We further show how spaced evaluation points and virtual parties sharpen the bound, and characterize when adding virtual parties is optimal (Section 5). Table 1 reports modulus overhead caused by the Lagrange reconstruction noise: for $n = 512$, our bounds reduce this overhead by about 33% at $t = n/2$ and by up to 90% at $t = 500$, relative to [BFM$^+$25].

Bound	Reference in this paper	$t = 12$	$t = 128$	$t = 256$	$t = 384$	$t = 500$
[BGG$^+$18]	Corollary 3.5	7918	8696	9016	8951	8403
[BFM$^+$25]	Lemma A.1	412	528	656	784	900
[CLW25]	Lemma A.2	189	1938	3862	5784	7524
Ours	Corollary 3.9	81	361	438	363	86

Table 1: Modulus overhead needed to accommodate the Lagrange reconstruction noise, for $n = 512$ and various threshold values t.

Strong simulation security with compact shares. The only prior construction achieving strong simulation security is that of [EY24], which relies on three ingredients: the special-FHE of [BGG$^+$18], an abstract almost-KHPRF without a concrete instantiation, and the $\{0,1\}$-LSSS of [BGG$^+$18] with its large shares. Our second construction removes all three: each party's share consists of two ring elements, and the partial-decryption mask is a direct RLWE mechanism whose non-canceling error is explicitly tracked, which is what enables the concrete modulus bounds below. Assuming IND-CPA security of the underlying scheme and the RLWE assumption, we prove strong simulation security in the random-oracle model against static corruption of fewer than t parties, again for BFV, BGV, and CKKS. At $n = 16$, $t = 8$, and $N = 2^{14}$, the per-party storage of our second construction is approximately 897 KB, compared with approximately 79 GB for the construction of [EY24] (Section 6.2).

A tight sufficient modulus condition for strong simulation. For the second construction, we derive a sufficient lower bound on the ciphertext modulus that ensures both correctness and strong simulation security. We instantiate this condition for the monomial interpolation set and obtain concrete modulus estimates for the strong-simulation setting. At $N = 2^{14}$ and 128-bit security, the sufficient ciphertext modulus has 219 bits for $(n, t) = (16, 8)$ and 1589 bits for $(n, t) = (1024, 512)$ (Table 3).

1.2 Technical Overview

We construct t-out-of-n threshold decryption for RLWE-based FHE schemes whose ciphertexts satisfy a decryption equation linear in the secret key up to rounding. Concretely, let $R = \mathbb{Z}[x]/(x^N + 1)$ with N a power of two, $R_q = R/qR$, and $q > p \geq 2$; a BFV-like ciphertext $\mathsf{ct} = (a, b) \in R_q^2$ encrypting $\mu \in R_p$ under $\mathsf{sk} \in R_q$ satisfies

$$b + a \cdot \mathsf{sk} = \left\lceil \frac{q}{p} \right\rfloor \cdot \mu + e \pmod{q}, \qquad \|e\|_\infty \leq B_{\mathsf{eval}} \ ,$$

where the displayed error is its centered lift and B_{eval} bounds the error magnitude after evaluation. The overview is phrased for BFV; the adaptations to BGV and CKKS (Sections 3.3 and 4.3) modify only the decoding step of final decryption.

Shamir secret sharing makes this equation distributable: the secret key becomes a linear combination of shares, and each summand can be computed by one party. Fix interpolation points $\mathcal{I} = \{\alpha_0, \alpha_1, \ldots, \alpha_n\} \subset R_q$ with pairwise invertible differences and $\alpha_0 = 0$; sample $f \in R_q[Y]$ of degree $< t$ with $f(0) = \mathsf{sk}$ and set $\mathsf{sk}_i = f(\alpha_i)$. The Lagrange coefficients then yield the reconstruction identity:

$$\lambda_i^{\mathcal{S}\to\beta} := \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{\beta - \alpha_j}{\alpha_i - \alpha_j} \in R_q \quad (\beta \in R_q) \ , \quad \mathsf{sk} = \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}\to 0} \cdot \mathsf{sk}_i \quad (|\mathcal{S}| = t) \ .$$

The reconstruction identity is linear in the shares, and the phase $b + a \cdot \mathsf{sk}$ is linear in sk up to the public term b; substituting the identity therefore distributes over the shares, so each party can compute $a \cdot \mathsf{sk}_i$ locally and final decryption combines these values linearly. The nonlinear rounding is deferred until after this combination.

Threshold decryption then takes the following form, and its cost is that each party's masking noise is amplified by a Lagrange coefficient. Each party returns $\mathsf{p}_i = C_{\mathsf{dec}} \cdot a \cdot \mathsf{sk}_i + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q$, where $C_{\mathsf{dec}}, C_{\mathsf{sim}} \in R$ are public scaling factors clearing the Lagrange denominators—their role is detailed in the next paragraph—and $e_{\mathsf{fl},i}$ is masking noise of infinity norm at most B_{sm}. Final decryption combines the partial decryptions from an authorized set $\mathcal{S}$ of size t as

$$C_{\mathsf{dec}}\, b + \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}\to 0} \cdot \mathsf{p}_i \ = \ \left\lceil \frac{q}{p} \right\rfloor C_{\mathsf{dec}}\, \mu \ + \ C_{\mathsf{dec}}\, e \ + \ C_{\mathsf{sim}} \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}\to 0} \cdot e_{\mathsf{fl},i} \pmod{q} \ .$$

Rounding recovers $C_{\mathsf{dec}}\,\mu \bmod p$—hence μ, as C_{dec} is invertible modulo p—provided the noise remains below $q/(2p)$; each $e_{\mathsf{fl},i}$ enters this noise scaled by its Lagrange coefficient. For binary reconstruction coefficients this scaling factor is trivial, whereas Lagrange coefficients can be large.

The first construction. The first construction imposes no structure on the FHE error, which is what allows generic instantiation over BFV, BGV, and CKKS. Prior Shamir-based constructions clear the denominators differently: for their rounding step to remain correct, the FHE error itself must carry the clearing factor—i.e., the scheme must be *special*, with every ciphertext satisfying $a \cdot \mathsf{sk} + b = \mu + \bar{C} \cdot e$ for a fixed $\bar{C} \in R$ [BGG+18,BFM+25]. This property is enforced at key generation and encryption by sampling errors of the form $\bar{C} \cdot e'$, but it is not preserved by evaluation in general—notably by the $\mathsf{Rescale}$ operation of CKKS, whose rounding errors are not of this form. In our protocol, C_{dec} multiplies the entire phase $b + a \cdot \mathsf{sk}$, as visible in the combination above, and final decryption multiplies by $C_{\mathsf{dec}}^{-1} \bmod p$ after rounding; the encryption and evaluation algorithms are left unchanged.

Correctness is governed by a single coefficient norm, B_2, and its origin is the noise term of the combination above. Rounding succeeds provided

$$\left\| C_{\mathsf{dec}}\, e + C_{\mathsf{sim}} \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}\to 0} \cdot e_{\mathsf{fl},i} \right\|_\infty < \frac{q}{2p} \ ,$$

and the polynomial product bound $\|f \cdot g\|_\infty \le \|f\|_1 \, \|g\|_\infty$ together with the triangle inequality controls the sum by $t \cdot \max_{i \in \mathcal{S}} \|(C_{\mathsf{sim}} \lambda_i^{\mathcal{S}\to 0}) \bmod q\|_1 \cdot B_{\mathsf{sm}}$. Maximizing over authorized sets defines

$$B_2 := \max_{i,\mathcal{S}} \left\| (C_{\mathsf{sim}} \lambda_i^{\mathcal{S}\to 0}) \bmod q \right\|_1 \ ,$$

the amplification of the flooding noise during reconstruction. The precise sufficient conditions, including the invertibility requirements on C_{dec} and C_{sim}, are Conditions **(C1)**–**(C2)** of Theorem 3.1.

Simulation security is governed by a second norm, B_3, and its origin is the following interpolation identity. The simulator is given the plaintext μ and the corrupted shares; for an honest index i and $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, Shamir reconstruction gives

$$\mathsf{sk}_i = \lambda_0^{\mathcal{S}^*\to\alpha_i} \cdot \mathsf{sk} + \sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^*\to\alpha_i} \cdot \mathsf{sk}_k \ ,$$

and substituting $a \cdot \mathsf{sk} = \left\lceil \frac{q}{p} \right\rfloor \mu - b + e$ from the decryption equation yields

$$a \cdot \mathsf{sk}_i = \lambda_0^{\mathcal{S}^*\to\alpha_i} \left(\left\lceil \frac{q}{p} \right\rfloor \mu - b + e \right) + a \sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^*\to\alpha_i} \mathsf{sk}_k \ .$$

Every term on the right is computable from (μ, ct) and the corrupted shares, except the unknown error e, which appears multiplied by the anchor coefficient $\lambda_0^{\mathcal{S}^*\to\alpha_i}$. The simulator therefore outputs the computable part, and uniform flooding hides the remaining shift once B_{sm} is proportional to $B_3 := \max_{i,\mathcal{S}^*} \|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \lambda_0^{\mathcal{S}^*\to\alpha_i}) \bmod q\|_1$ (Conditions **(C3)**–**(C4)** of Theorem 3.2).

Since B_{sm} is proportional to B_3 and B_{sm} re-enters the correctness bound through the term $tB_{\mathsf{sm}}B_2$, the dominant contribution to the modulus is $t \cdot B_{\mathsf{eval}} \cdot 2^{\lambda} N \cdot B_2 B_3$. The modulus overhead of an interpolation set is therefore determined by the product $B_2 B_3$.

Bounding the Lagrange overhead. For the monomial interpolation set, the product $B_2 B_3$ admits an explicit trigonometric bound, which is the source of our modulus savings. Let $\mathcal{I}_{\mathrm{mon}} := \{0, 1, x, \ldots, x^{n-1}\}$, $n \leq 2N$, the family also used in [BFM+25,CLW25]; in contrast with the factorial-type bounds obtained for integer interpolation points (Sections 3.5 and 3.6), differences of these points reduce, up to units of R, to factors $x^k - 1$ (Lemma 2.2). Consequently, $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$ suffices to clear all denominators. Under the complex embeddings of R, these factors satisfy:

$$|\zeta^k - 1| = 2 \left| \sin\left(\frac{\pi r k}{2N}\right) \right| \quad , \qquad \zeta = \sigma(x) = e^{\pi \mathrm{i} r / N} \quad .$$

A coefficient $\lambda_i^{\mathcal{S} \to 0} = \pm \prod_{j \in \mathcal{S} \setminus \{i\}} (x^{i-j} - 1)^{-1}$ embeds, up to a power of two, to a product of $t-1$ inverse sines with angles $\pi r(i-j)/(2N)$; since r is coprime to $2N$, multiplication by r permutes the nonzero residues, so the worst case is over the distances $i - j$ themselves. Each distance can occur at most twice among the $t - 1$ points, so the product is maximized by the nearest-distance configuration $\{1, 1, 2, 2, \ldots\}$, and symmetrically the numerator factors of $\lambda_0^{\mathcal{S}^* \to \alpha_i}$ are maximized by distances closest to N. Bounding any coefficient $\lambda_\ell^{\mathcal{S}^* \to \alpha_i}$ thus reduces to this worst-case placement of angles: denominator factors yield inverse-sine products, and numerator factors yield cosine products. For B_2 only denominators appear, giving an inverse-sine product; for B_3 the anchor coefficient has a unit denominator, so only a cosine product survives. The two products combine into the bound of Corollary 3.9:

$$B_2 B_3 \leq 2^{\lceil \log t \rceil} N \cdot \frac{1}{\sin^2\left(\pi \frac{\lfloor t/2 \rfloor}{2N}\right)} \prod_{k=1}^{\lfloor t/2 \rfloor - 1} \cot^2\left(\frac{\pi k}{2N}\right) \quad .$$

Our experiments indicate that this bound is close to tight (Section 6.1); at $n = 512$, it reduces the modulus overhead by about 33% at $t = n/2$ and by up to 90% at $t = 500$, relative to [BFM+25] (Table 1).

The bounds further improve by placing the interpolation points in the smallest cyclotomic subring containing them, and can be tuned by adding public *virtual* interpolation points, which enlarge the interpolation size without changing the real-party threshold or the communication of threshold decryption (Section 5).

The second construction. Standard simulation security suffices when the simulator already knows the plaintext before producing honest partial decryptions; strong simulation security requires it to answer queries *before* the plaintext

is available, and to make those answers consistent with the plaintext revealed once the threshold is reached. Flooding alone does not provide the ciphertext-dependent entropy needed for these early answers. The first construction indeed fails this notion: combining a single party's partial decryptions of related ciphertexts recovers the plaintext (see Section 4).

The second construction supplies the missing ciphertext-dependent entropy by masking each partial decryption with a term that cancels exactly during authorized reconstruction. Key generation additionally distributes a Shamir sharing $(s_1, \ldots, s_n)$ of zero—each party's share is the pair (sk_i, s_i), two ring elements—and partial decryption becomes

$$\mathsf{p}_i = C_{\mathsf{dec}}\big(a \cdot \mathsf{sk}_i + H(\mathsf{ct}) \cdot s_i + e_{\mathsf{RLWE},i}\big) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \pmod q \ ,$$

where $H : \{0,1\}^* \to R_q$ is a random oracle and $e_{\mathsf{RLWE},i} = H_\chi((\mathsf{sk}_i, s_i), \mathsf{ct})$ is an RLWE error. During authorized reconstruction the masks cancel exactly, since $\sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S} \to 0} s_i = 0$; the RLWE errors do not cancel and enter the correctness bound explicitly (the B_χ term of Theorem 4.1). Before the threshold, at most $t - 1 - |\mathcal{S}_{\mathsf{cor}}|$ honest parties are queried on a fixed ciphertext; their zero shares are jointly uniform given the corrupted shares by Shamir privacy, so each pair $(H(\mathsf{ct}),\ H(\mathsf{ct}) \cdot s_i + e_{\mathsf{RLWE},i})$ is a RLWE sample and the corresponding replies are pseudorandom under the RLWE assumption. This replaces the almost-KHPRF layer of [EY24] by a direct RLWE mechanism, and reduces the per-party storage from $O(n^{4.2})$ elements to two.[5]

The additional cost of strong simulation is an enlarged family of coefficients to control: the simulator must absorb the interpolation error at every index $\ell \in \mathcal{S}^*$, not only the anchor $\ell = 0$. When a query first reaches the threshold, the simulator learns the plaintext and must output a p_i consistent with the $t - 1$ previously issued answers, whose deterministic components are $(\mathsf{p}_\ell^{\mathrm{det}})_{\ell \in T}$ for the fixed index set T: final decryption applied to the combined set must recover μ. The only candidate is the interpolation over $\mathcal{S}^* = \{0\} \cup T$,

$$\mathsf{p}_i = C_{\mathsf{dec}} \lambda_0^{\mathcal{S}^* \to \alpha_i} \left(\left\lceil \frac{q}{p} \right\rfloor \mu - b \right) + \sum_{\ell \in T} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{p}_\ell^{\mathrm{det}} + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \pmod q \ ,$$

and comparing it with a real partial decryption leaves a residual error in which the ciphertext error is multiplied by $\lambda_0^{\mathcal{S}^* \to \alpha_i}$ and each earlier RLWE error by $\lambda_\ell^{\mathcal{S}^* \to \alpha_i}$ for $\ell \in T$. Flooding must dominate all of these simultaneously, which, for the second construction, redefines the simulation-side norm as

$$B_3 := \max_{i, \ell, \mathcal{S}^*} \|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \lambda_\ell^{\mathcal{S}^* \to \alpha_i}) \bmod q\|_1,$$

extending $\ell = 0$ of the first construction to every index $\ell \in \mathcal{S}^*$. By the angle-placement argument above, the coefficients with $\ell \neq 0$ reintroduce denominators, so the cosine product of the standard-simulation bound is replaced by a

[5] The $O(n^{4.2})$ element count in [EY24] stems from Valiant's monotone-majority $\{0,1\}$-LSSS [BGG+18, Section 5.4], which yields $O(\ell/n)$ elements per party for $\ell = O(n^{5.2})$.

second inverse-sine product (Table 2). Unlike the corresponding factor of the first construction, this product is increasing in the interpolation size; consequently, adding virtual points increases the resulting modulus bound, and the bound is minimized with no virtual points ($c = 0$) and interpolation in the subring of degree $n'/2$ with $n' = 2^{\lceil \log \max\{n, 2t\} \rceil}$ (Theorem 5.5). At $N = 2^{14}$ and 128-bit security, the sufficient modulus is 219 bits for $n = 16$, $t = 8$, and 1589 bits for $n = 1024$, $t = 512$ (Table 3); each party stores the two elements $\mathsf{sk}_i, s_i \in R_q$, about 897 KB, in place of the $O(n^{4.2})$ share elements of [EY24] (Section 6.2).

	First construction	**Second construction**
Correctness side	$B_2 = \max_{i,\mathcal{S}} \|(C_{\mathsf{sim}} \lambda_i^{\mathcal{S}\to 0}) \bmod q\|_1$	
Simulation side	$B_3 = \max_{i,\mathcal{S}^*} \|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \lambda_0^{\mathcal{S}^*\to\alpha_i}) \bmod q\|_1$	$B_3 = \max_{i,\ell,\mathcal{S}^*} \|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \lambda_\ell^{\mathcal{S}^*\to\alpha_i}) \bmod q\|_1$
Dominant factor	$\prod_{k=1}^{\lfloor t'/2 \rfloor} \cot^2\left(\frac{\pi k}{n'}\right)$	$\prod_{k=1}^{\lfloor t'/2 \rfloor} \sin^{-2}\left(\frac{\pi k}{n'}\right) \cdot \prod_{k=1}^{\lfloor (t'-1)/2 \rfloor} \sin^{-2}\left(\frac{\pi k}{n'}\right)$

Table 2: Interpolation-dependent part of the modulus bound for our two constructions, at threshold $t' = t + c$, where c is the number of virtual parties, and n', a power of two such that the interpolation points are n'-th roots of unity and hence lie in the cyclotomic subring of degree $n'/2$ (Section 5). The correctness-side quantity B_2 is common to both. On the simulation side, the bound on the Lagrange coefficient $\lambda_\ell^{\mathcal{S}^*\to\alpha_i}$ depends on the construction: the first construction bounds only the anchor coefficient ($\ell = 0$), whereas the second construction (strong simulation) requires a bound for all $\ell \in \mathcal{S}^*$. Accordingly, B_3 is defined separately for each construction (Sections 3.4 and 4.4).

Organization. Section 2 recalls the algebraic setting, Shamir secret sharing, and the two simulation notions. Section 3 presents the first construction, proves its correctness and simulation security, and bounds its ciphertext modulus for concrete interpolation sets. Section 4 presents the second construction, proves its correctness and strong simulation security, and bounds its ciphertext modulus. Section 5 analyzes spaced evaluation and virtual points. Section 6 evaluates the bounds and compares the resulting parameter choices with prior work.

2 Preliminaries

Notation. We let $\lambda \in \mathbb{N}$ denote the security parameter. A function $\mathsf{negl} : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is called *negligible* if $\mathsf{negl}(\lambda) = o(\lambda^{-c})$ for all $c \in \mathbb{N}$. For a positive integer n, we write $[n] := \{1, \ldots, n\}$. Bold lowercase letters such as $\mathbf{v}$ denote column vectors, and bold uppercase letters such as $\mathbf{M}$ denote matrices. The L_1 and L_∞ norms of a vector $\mathbf{v}$ are respectively denoted by $\|\mathbf{v}\|_1$ and $\|\mathbf{v}\|_\infty$. The base-2 and natural logarithms are respectively denoted log and ln. When reducing an

integer modulo q, we consider representatives in $(-q/2, q/2]$; this is extended coefficient-wise to integer polynomials. For any nonzero integer a, we let $\mathsf{PoT}(a)$ denote the unique positive power-of-2 integer such that $a = \mathsf{PoT}(a) \cdot u$ for an odd integer u. We define the statistical distance between two distributions X_1 and X_2 over a countable support $\mathcal{X}$ as $\Delta(X_1, X_2) := \frac{1}{2} \sum_{x \in \mathcal{X}} |\Pr[X_1 = x] - \Pr[X_2 = x]|$. For a finite set $\mathcal{S}$, we write $|\mathcal{S}|$ for its cardinality.

We now recall the Clausen function of order 2.

Definition 2.1. *The Clausen function of order 2 is* $\mathrm{Cl}_2(\theta) = \sum_{k \geq 1} \sin(k\theta)/k^2$, *for* $\theta \in \mathbb{R}$. *For* $\theta \in [0, 2\pi]$, *it admits the following integral representation:*

$$\mathrm{Cl}_2(\theta) \;=\; -\int_0^\theta \ln\left(2 \sin\left(\tfrac{x}{2}\right)\right) \,\mathrm{d}x \;\; .$$

We write $G := \mathrm{Cl}_2(\pi/2)$ *for Catalan's constant.*

2.1 Algebraic Setting

Let N be a power of 2. We define the cyclotomic ring $R := \mathbb{Z}[x]/(x^N + 1)$, i.e., the quotient of the polynomial ring $\mathbb{Z}[x]$ by the ideal generated by $x^N + 1$: elements of R are equivalence classes of integer polynomials modulo the relation $x^N \equiv -1$. The associated cyclotomic field is $K := \mathbb{Q}[x]/(x^N + 1)$, and R is the ring of integers of K. For any integer $q \geq 2$, we define $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$, and $R_q := R/qR = \mathbb{Z}_q[x]/(x^N + 1)$. By a slight abuse of notation, we identify each element $a \in R$ with its unique representative of degree strictly less than N, i.e., $a(x) = \sum_{0 \leq j < N} a_j x^j$ with $a_j \in \mathbb{Z}$ for all j.

We recall that $\langle 2 \rangle = \langle 1 - x \rangle^N$ (see, e.g. [MS77, Theorem 26]). We will also use the following *cyclotomic reduction* result.

Lemma 2.2. *For* $m \in (0, 2N)$, *it holds that* $\langle 1 - x^m \rangle = \langle 1 - x \rangle^{\mathsf{PoT}(m)}$.

Proof. We first prove by induction that for an arbitrary $r \geq 0$ with $2^r \leq N$, we have $\langle 1 - x^{2^r} \rangle = \langle 1 - x \rangle^{2^r}$. The base case $r = 0$ is a tautology. For $r > 0$, we observe that:

$$\langle 1 - x^{2^r} \rangle = \langle 1 - x^{2^{r-1}} \rangle \cdot \langle 1 + x^{2^{r-1}} \rangle = \langle 1 - x^{2^{r-1}} \rangle \cdot \sigma(\langle 1 - x^{2^{r-1}} \rangle) \;\; ,$$

where σ is the automorphism that sends x to $x^{1+N/2^{r-1}}$. Using the induction assumption, we obtain the following:

$$\langle 1 - x^{2^r} \rangle = \langle 1 - x \rangle^{2^{r-1}} \cdot (\sigma(\langle 1 - x \rangle))^{2^{r-1}} = \langle 1 - x \rangle^{2^r} \cdot \left\langle \frac{1 - x^{1+N/2^{r-1}}}{1 - x} \right\rangle^{2^{r-1}} \;\; .$$

The fact that $(1 - x^{1+N/2^{r-1}})/(1 - x)$ is a (cyclotomic) unit allows us to complete the proof of the claim.

We are now ready to prove the lemma statement. Let $m \in (0, 2N)$. The following holds:

$$\langle 1 - x^m \rangle = \left\langle 1 - (x^{m/\mathsf{PoT}(m)})^{\mathsf{PoT}(m)} \right\rangle = \left\langle 1 - x^{m/\mathsf{PoT}(m)} \right\rangle^{\mathsf{PoT}(m)} \ .$$

The last equality follows from applying the automorphism $x \mapsto x^{m/\mathsf{PoT}(m)}$ to the previously proved relation $\langle 1 - x^{\mathsf{PoT}(m)} \rangle = \langle 1 - x \rangle^{\mathsf{PoT}(m)}$ (note that $\mathsf{PoT}(m)$ is a power of two). Finally, using the fact that the ratio $(1 - x^{m/\mathsf{PoT}(m)})/(1 - x)$ is a cyclotomic unit, since $m/\mathsf{PoT}(m)$ is odd, we obtain

$$\langle 1 - x^m \rangle = \left\langle 1 - x^{m/\mathsf{PoT}(m)} \right\rangle^{\mathsf{PoT}(m)} = \langle 1 - x \rangle^{\mathsf{PoT}(m)} \ .$$

This completes the proof. □

For $a(x) = \sum_{0 \le j < N} a_j x^j \in R$, we define $\|a\|_\infty := \max_{0 \le j < N} |a_j|$ and $\|a\|_1 := \sum_{0 \le j < N} |a_j|$. We define the evaluation embedding over the $(2N)$-th primitive roots of unity as:

$$\boldsymbol{\sigma}(a) := \left(a(\omega^{2k-1})\right)_{k \in [N]} \in \mathbb{C}^N \ ,$$

where $\omega := e^{\pi \mathsf{i}/N}$. The following lemma establishes norm relationships.

Lemma 2.3. *Let $a(x) = \sum_{0 \le j < N} a_j x^j \in R$. Then we have:*

$$\|a\|_\infty \le \|a\|_1 \quad \textit{and} \quad \|\boldsymbol{\sigma}(a)\|_\infty \le \|a\|_1 \le \sqrt{N} \|\boldsymbol{\sigma}(a)\|_\infty \ .$$

Proof. The first inequality follows directly from the definitions:

$$\|a\|_\infty = \max_{0 \le j < N} |a_j| \le \sum_{0 \le j < N} |a_j| = \|a\|_1.$$

For the lower bound on $\|a\|_1$, let $z = \omega^{2k-1}$. Since $|z| = 1$, we have

$$|a(z)| = \left| \sum_{0 \le j < N} a_j z^j \right| \le \sum_{0 \le j < N} |a_j| = \|a\|_1.$$

Taking the maximum over $k \in [N]$ gives $\|\boldsymbol{\sigma}(a)\|_\infty \le \|a\|_1$.

For the upper bound, let $V \in \mathbb{C}^{N \times N}$ be the evaluation matrix

$$V_{k,j} = (\omega^{2k-1})^j \qquad (k \in [N],\ 0 \le j < N).$$

Then $\boldsymbol{\sigma}(a) = V(a_0, \ldots, a_{N-1})^T$. The matrix $N^{-1/2}V$ is unitary, and therefore

$$\|(a_0, \ldots, a_{N-1})\|_2 = \frac{1}{\sqrt{N}} \|\boldsymbol{\sigma}(a)\|_2 \le \|\boldsymbol{\sigma}(a)\|_\infty.$$

By the Cauchy–Schwarz inequality, $\|a\|_1 \le \sqrt{N}\, \|(a_0, \ldots, a_{N-1})\|_2$. Combining the two inequalities proves $\|a\|_1 \le \sqrt{N}\, \|\boldsymbol{\sigma}(a)\|_\infty$.

For an integer $B \geq 1$, let $R^B := \{e \in R : \|e\|_\infty \leq B\}$. The following result is at the center of ThFHE simulation security.

Lemma 2.4 (Flooding lemma). *Let $B_1, B_2 \in \mathbb{N}$. Let $e \in R$ satisfy $\|e\|_\infty \leq B_1$, and let E_1, E_2 be independent random variables uniformly distributed over the hypercube $R^{B_2} := \{x \in R : \|x\|_\infty \leq B_2\}$. Then*

$$\Delta\left(E_1 + e, E_2\right) \leq N \cdot \frac{B_1}{B_2} \ .$$

We will use the result with $B_2 = 2^\lambda \cdot N \cdot B_1$. Note that, in practice, it may be preferable to use Gaussian distributions as they allow one to achieve λ-bit security by flooding by $\approx \lambda/2$ bits instead of λ bits [LMSS22]. In this work, we flood using the uniform hypercube distribution for the sake of simplicity.

Distributions and hash functions. For a finite set S, we write $U(S)$ for the uniform distribution over S. The notation $U(R^B)$ denotes the uniform distribution over R^B.

Throughout the paper, we use hash functions with codomains in R or R_q. A hash function $H : \{0,1\}^* \to R_q$ is modeled as a random oracle. Given a distribution χ over R whose support has infinity norm bounded by $B_\chi \geq 1$, we write $H_\chi : \{0,1\}^* \to R$ for a hash function that, on each fresh input, returns an independent sample from χ; it is also modeled as a random oracle.

RLWE assumption. Let $q \geq 2$ be an integer and let χ be a distribution over R. The $RLWE_{q,\chi}$ hardness assumption states that, for any polynomially bounded m, the following two distributions are computationally indistinguishable:

$$\left\{(a_j,\, a_j \cdot s + e_j)\right\}_{j\in[m]} \quad \text{and} \quad \left\{(a_j,\, b_j)\right\}_{j\in[m]},$$

where s, the a_j's, and the b_j's are independently uniform in R_q, and the e_j's are independently sampled from χ.

2.2 Secret Sharing

Throughout, we consider a (t, n)-threshold setting in which any subset containing at least t of the n parties is authorized, while no subset of smaller size is authorized. For convenience, we number the parties and identify party P_i with i.

Definition 2.5 ((t, n)-threshold structure). *Let $n \in \mathbb{N}$ be the number of parties. Let $t \in [n]$ be the threshold. The* (t, n)-threshold access structure *is the family $\mathbb{A}_{n,t} := \{\mathcal{S} \subseteq [n] : |\mathcal{S}| \geq t\}$. Sets in $\mathbb{A}_{n,t}$ are* authorized*, and all other subsets of $[n]$ are* unauthorized*.*

We often abuse notation by implicitly assuming that sets $\mathcal{S} \in \mathbb{A}_{n,t}$ have precisely size t.

Definition 2.6 (Maximal unauthorized set). *Let $\mathbb{A}_{n,t}$ be a (t,n)-threshold access structure. A set $\mathcal{S}' \subseteq [n]$ is called a* maximal unauthorized set *if $\mathcal{S}'$ is unauthorized and the set $\mathcal{S}' \cup \{i\}$ is authorized for every $i \in [n] \setminus \mathcal{S}'$, or, equivalently, if $|\mathcal{S}'| = t-1$. We let $\mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ denote the set of maximal unauthorized sets.*

Shamir Secret Sharing. We consider t-out-of-n Shamir secret sharing over the ring R_q for some $q \geq 2$. It is parameterized by interpolation points $\mathcal{I} = \{\alpha_0, \ldots, \alpha_n\} \subset R_q$ with $\alpha_i - \alpha_j$ invertible in R_q for all $0 \leq i \neq j \leq n$. Sharing a secret sk is done by sampling a uniform polynomial $f \in R_q[Y]$ of degree smaller than t conditioned on $f(\alpha_0) = \mathsf{sk}$; the share of the i-th party is $\mathsf{sk}_i = f(\alpha_i)$. In this work, we always set $\alpha_0 = 0$. We let $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n) \leftarrow \mathsf{Share}(\mathsf{sk}; n, t, \mathcal{I})$ denote the process of t-out-of-n Shamir-secret-sharing a secret sk over R_q with interpolation points $\mathcal{I}$.

Shamir secret sharing reconstructs the secret by a linear combination based on Lagrange interpolation, whose coefficients are the so-called Lagrange coefficients.

Definition 2.7 (Lagrange coefficients). *Let $t \leq n$, $q \geq 2$ and $\mathcal{I} = \{\alpha_0, \ldots, \alpha_n\} \subseteq R_q$ such that $\alpha_i - \alpha_j$ is invertible in R_q for all $0 \leq i \neq j \leq n$. Let $\mathcal{S} \subseteq \{0, 1, \ldots, n\}$ with $|\mathcal{S}| = t$ and $\beta \in R_q$. For each $i \in \mathcal{S}$, define*

$$\lambda_i^{\mathcal{S}\to\beta}(q, \mathcal{I}) \coloneqq \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{\beta - \alpha_j}{\alpha_i - \alpha_j} \in R_q \ .$$

We call $\lambda_i^{\mathcal{S}\to\beta}(q, \mathcal{I})$ the i-th Lagrange coefficient from $\mathcal{S}$ towards β *associated with $\mathcal{I}$ modulo q, and omit $\mathcal{I}$ and q when they are clear from the context. We refer to the set of all such coefficients as the* Lagrange coefficients associated with $\mathcal{I}$.

It follows from [Feh98, Section 3.1] that for every polynomial $f \in R_q[Y]$ of degree $< t$ we have $f(\beta) = \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}\to\beta} \cdot f(\alpha_i)$. In particular, if we sample $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n) \leftarrow \mathsf{Share}(\mathsf{sk}; n, t, \mathcal{I})$, then for any $\mathcal{S} \in \mathbb{A}_{n,t}$ it holds that $\mathsf{sk} = \sum_{i \in \mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} \cdot \mathsf{sk}_i$.

Shamir secret sharing achieves *perfect privacy*, in the sense that for any subset $\mathcal{S}_{\mathsf{cor}} \subseteq [n]$ with $|\mathcal{S}_{\mathsf{cor}}| < t$, for any $\mathsf{sk}, \mathsf{sk}' \in R_q$, the two distributions $\{(\mathsf{sk}_i)_{i \in \mathcal{S}_{\mathsf{cor}}} | (\mathsf{sk}_i)_{i \in [n]} \leftarrow \mathsf{Share}(\mathsf{sk}; n, t, \mathcal{I})\}$ and $\{(\mathsf{sk}'_i)_{i \in \mathcal{S}_{\mathsf{cor}}} | (\mathsf{sk}'_i)_{i \in [n]} \leftarrow \mathsf{Share}(\mathsf{sk}'; n, t, \mathcal{I})\}$ are identical (and uniform).

2.3 Threshold Fully Homomorphic Encryption

We recall the definition of a ThFHE scheme and define two different security notions: simulation security and strong simulation security.

Definition 2.8 (Threshold Fully Homomorphic Encryption). *A Threshold Fully Homomorphic Encryption scheme (ThFHE) is a tuple of PPT algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{PartDec}, \mathsf{FinDec})$ *with the following specifications.*

- $\mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$*: on input a security parameter* λ*, a positive number of parties* n*, and a threshold* $t \in [n]$*, it outputs* n *secret-key shares* $(\mathsf{sk}_i)_{i\in[n]}$ *and a public key* pk*.*
- $\mathsf{Enc}(\mathsf{pk}, \mu)$*: on input a public key* pk *and a plaintext* μ*, it outputs a ciphertext* ct*.*
- $\mathsf{Eval}(\mathsf{pk}, f, (\mathsf{ct}_j)_{j\in[\ell]})$*: on input a public key* pk*, a circuit* f *with arity* $\ell \geq 1$ *and ciphertexts* $(\mathsf{ct}_j)_{j\in[\ell]}$*, it outputs a ciphertext* $\hat{\mathsf{ct}}$*.*
- $\mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$*: on input a secret-key share* sk_i *and a ciphertext* ct*, it outputs a partial decryption share* p_i*.*
- $\mathsf{FinDec}(\mathsf{ct}, (\mathsf{p}_i)_{i\in\mathcal{S}})$*: on input a ciphertext* ct *and* t *partial decryption shares* $(\mathsf{p}_i)_{i\in\mathcal{S}}$ *for a set of* t *distinct decryptors* $\mathcal{S} \in \mathbb{A}_{n,t}$*, it outputs a plaintext* μ'*.*

Correctness.[6] *We require that for any circuit* f *with arity* $\ell \geq 1$*, for any plaintexts* $(\mu_j)_{j\in[\ell]}$*, for any* n*, and any subset* $\mathcal{S} \subseteq [n]$ *of* t *parties, we have:*

$$\Pr\left[\mathsf{FinDec}(\hat{\mathsf{ct}}, (\mathsf{p}_i)_{i\in\mathcal{S}}) = \hat{\mu} \;\middle|\; \begin{array}{c} ((\mathsf{sk}_i)_{i\in[n]}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n, 1^t) \\ \mathsf{ct}_j \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu_j), \forall j \leq \ell \\ \hat{\mathsf{ct}} \leftarrow \mathsf{Eval}(\mathsf{pk}, f, (\mathsf{ct}_j)_{j\in[\ell]}) \\ \mathsf{p}_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \hat{\mathsf{ct}}), \forall i \in \mathcal{S} \end{array}\right] \geq 1 - 2^{-\Omega(\lambda)} \enspace ,$$

where $\hat{\mu} = f(\mu_1, \ldots, \mu_\ell)$ *and where the probability is taken over the randomness of the algorithms.*

Compactness. *There exists a polynomial* P *such that for any* λ*,* n*,* t*, and execution of* $\mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$*, all ciphertexts produced by any combination of* Enc *and* Eval *with arbitrary circuits* f *have bit-size at most* $P(\lambda, n)$*.*

We consider a simulation-based security definition.

Definition 2.9 (Simulation Security). *A ThFHE scheme* $\Pi_{\mathsf{ThFHE}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{PartDec}, \mathsf{FinDec})$ *is said to be* simulation-secure *if it satisfies the following two properties:*

- *the public key encryption scheme induced by* $(\mathsf{KeyGen}, \mathsf{Enc})$ *is* IND-CPA*-secure;*
- *there exists a PPT simulator* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *such that the experiments depicted in Figure 1 are computationally indistinguishable; specifically, we require that for any PPT adversary* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$*, we have:*

$$\left|\Pr\left[\mathcal{A}(\mathsf{Exp}^{\mathsf{Sim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{Exp}^{\mathsf{Sim}}_{\mathsf{Ideal}}(1^\lambda, 1^n, 1^t)) = 1\right]\right| \leq 2^{-\Omega(\lambda)} \enspace .$$

We now define strong simulation security, adapting the framework from [EY24] primarily by decoupling evaluation queries from partial decryption queries.

Definition 2.10 (Strong Simulation Security). *A ThFHE scheme is said to be* strongly simulation-secure *if it satisfies the following two properties:*

[6] We focus on exact correctness and discuss an extension to CKKS in Subsection 3.3.

$\mathsf{Exp}^{\mathsf{Sim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)$:

$((\mathsf{sk}_i)_{i\in[n]}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$
$\mathsf{ctr} \leftarrow 0,\ \mathsf{L} \leftarrow \varnothing$
$(\mathcal{S}_{\mathsf{cor}}, \mathsf{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(\mathsf{pk})$ with $|\mathcal{S}_{\mathsf{cor}}| = t-1$
$\mathsf{out} \leftarrow \mathcal{A}_1^{\mathsf{OEnc},\mathsf{OEval},\mathsf{ODec}}((\mathsf{sk}_i)_{i\in\mathcal{S}_{\mathsf{cor}}}, \mathsf{pk}, \mathsf{st}_{\mathcal{A}})$
return $(\mathsf{out} = \mathsf{real})$

$\mathsf{OEnc}(\mu)$:

$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu)$
$\mathsf{ctr} \leftarrow \mathsf{ctr} + 1$
$\mathsf{L}[\mathsf{ctr}] \leftarrow (\mu, \mathsf{ct})$
return ct

$\mathsf{OEval}(f, (j_1, \ldots, j_\ell))$:

if $\exists k \in [\ell] : j_k > \mathsf{ctr}$ **then**
  return $\perp$
for $k \in [\ell]$ **do**
  $(\mu_k, \mathsf{ct}_k) \leftarrow \mathsf{L}[j_k]$
$\mathsf{ct} \leftarrow \mathsf{Eval}(\mathsf{pk}, f, (\mathsf{ct}_1, \ldots, \mathsf{ct}_\ell))$
$\mathsf{ctr} \leftarrow \mathsf{ctr} + 1$
$\mu \leftarrow f(\mu_1, \ldots, \mu_\ell)$
$\mathsf{L}[\mathsf{ctr}] \leftarrow (\mu, \mathsf{ct})$
return ct

$\mathsf{Exp}^{\mathsf{Sim}}_{\mathsf{Ideal}}(1^\lambda, 1^n, 1^t)$:

$((\mathsf{sk}_i)_{i\in[n]}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$
$\mathsf{ctr} \leftarrow 0,\ \mathsf{L} \leftarrow \varnothing$
$(\mathcal{S}_{\mathsf{cor}}, \mathsf{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(\mathsf{pk})$ with $|\mathcal{S}_{\mathsf{cor}}| = t-1$
$(\mathsf{st}, (\mathsf{sk}'_i)_{i\in\mathcal{S}_{\mathsf{cor}}}) \leftarrow \mathsf{Sim}_0(\mathsf{pk}, \mathcal{S}_{\mathsf{cor}})$
$\mathsf{out} \leftarrow \mathcal{A}_1^{\mathsf{OEnc},\mathsf{OEval},\mathsf{OSim}}((\mathsf{sk}'_i)_{i\in\mathcal{S}_{\mathsf{cor}}}, \mathsf{pk}, \mathsf{st}_{\mathcal{A}})$
return $(\mathsf{out} = \mathsf{ideal})$

$\mathsf{ODec}(j, i)$:

if $j > \mathsf{ctr} \vee i \in \mathcal{S}_{\mathsf{cor}}$ **then**
  return $\perp$
$(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
$\mathsf{p}_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$
return p_i

$\mathsf{OSim}(j, i)$:

if $j > \mathsf{ctr} \vee i \in \mathcal{S}_{\mathsf{cor}}$ **then**
  return $\perp$
$(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
$(\mathsf{st}, \mathsf{p}_i) \leftarrow \mathsf{Sim}_1(\mathsf{st}, \mathsf{ct}, i, \mu)$
return p_i

Fig. 1: Simulation security experiments for ThFHE.

- *the public key encryption scheme induced by* $(\mathsf{KeyGen}, \mathsf{Enc})$ *is* IND-CPA*-secure;*
- *there exists a PPT simulator* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1, \mathsf{Sim}_2)$ *such that the experiments described in Figure 2 are computationally indistinguishable. That is, for any PPT adversary* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$*, we require:*

$$\left|\Pr\left[\mathcal{A}(\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)) = 1\right] - \Pr\left[\mathcal{A}(\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Ideal}}(1^\lambda, 1^n, 1^t)) = 1\right]\right| \leq 2^{-\Omega(\lambda)}.$$

Note that strong simulation security (Definition 2.10) implies simulation security (Definition 2.9), since the adversary in the latter is a restricted case of the strong adversary.

$\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)$:

$((\mathsf{sk}_i)_{i\in[n]}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$
$\mathsf{ctr} \leftarrow 0,\ \mathsf{L} \leftarrow \varnothing,\ \mathsf{P} \leftarrow \varnothing$
$(\mathcal{S}_{\mathsf{cor}}, \mathsf{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(\mathsf{pk})$ with $|\mathcal{S}_{\mathsf{cor}}| < t$
$\mathsf{out} \leftarrow \mathcal{A}_1^{\mathsf{OEnc},\mathsf{OEval},\mathsf{ODec}}((\mathsf{sk}_i)_{i\in\mathcal{S}_{\mathsf{cor}}}, \mathsf{pk}, \mathsf{st}_{\mathcal{A}})$
return $(\mathsf{out} = \mathsf{real})$

$\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Ideal}}(1^\lambda, 1^n, 1^t)$:

$((\mathsf{sk}_i)_{i\in[n]}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$
$\mathsf{ctr} \leftarrow 0,\ \mathsf{L} \leftarrow \varnothing,\ \mathsf{P} \leftarrow \varnothing$
$(\mathcal{S}_{\mathsf{cor}}, \mathsf{st}_{\mathcal{A}}) \leftarrow \mathcal{A}_0(\mathsf{pk})$ with $|\mathcal{S}_{\mathsf{cor}}| < t$
$(\mathsf{st}, (\mathsf{sk}'_i)_{i\in\mathcal{S}_{\mathsf{cor}}}) \leftarrow \mathsf{Sim}_0(\mathsf{pk}, \mathcal{S}_{\mathsf{cor}})$
$\mathsf{out} \leftarrow \mathcal{A}_1^{\mathsf{OEnc},\mathsf{OEval},\mathsf{OSim}}((\mathsf{sk}'_i)_{i\in\mathcal{S}_{\mathsf{cor}}}, \mathsf{pk}, \mathsf{st}_{\mathcal{A}})$
return $(\mathsf{out} = \mathsf{ideal})$

$\mathsf{OEnc}(\mu)$:

$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu)$
$\mathsf{ctr} \leftarrow \mathsf{ctr} + 1$
if $\mathsf{P}[\mathsf{ct}]$ *does not exist* **then**
  $\mathsf{P}[\mathsf{ct}] \leftarrow \mathcal{S}_{\mathsf{cor}}$
$\mathsf{L}[\mathsf{ctr}] \leftarrow (\mu, \mathsf{ct})$
return ct

$\mathsf{ODec}(j, i)$:

if $j \notin [\mathsf{ctr}] \vee i \notin [n]$ **then**
  return $\perp$
$(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
$\mathsf{p}_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$
return p_i

$\mathsf{OEval}(f, (j_1, \ldots, j_\ell))$:

if $\exists k \in [\ell] : j_k \notin [\mathsf{ctr}]$ **then**
  return $\perp$
for $k \in [\ell]$ **do**
  $(\mu_k, \mathsf{ct}_k) \leftarrow \mathsf{L}[j_k]$
$\mathsf{ct} \leftarrow \mathsf{Eval}(\mathsf{pk}, f, (\mathsf{ct}_1, \ldots, \mathsf{ct}_\ell))$
$\mathsf{ctr} \leftarrow \mathsf{ctr} + 1$
$\mu \leftarrow f(\mu_1, \ldots, \mu_\ell)$
if $\mathsf{P}[\mathsf{ct}]$ *does not exist* **then**
  $\mathsf{P}[\mathsf{ct}] \leftarrow \mathcal{S}_{\mathsf{cor}}$
$\mathsf{L}[\mathsf{ctr}] \leftarrow (\mu, \mathsf{ct})$
return ct

$\mathsf{OSim}(j, i)$:

if $j \notin [\mathsf{ctr}] \vee i \notin [n]$ **then**
  return $\perp$
$(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
$\mathsf{P}[\mathsf{ct}] \leftarrow \mathsf{P}[\mathsf{ct}] \cup \{i\}$
if $|\mathsf{P}[\mathsf{ct}]| \geq t$ **then**
  if T_{ct} *is undefined* **then**
    $T_{\mathsf{ct}} \leftarrow \mathsf{P}[\mathsf{ct}] \setminus \{i\}$;
    $\mathsf{st} \leftarrow \mathsf{st} \cup \{(\mathsf{ct}, T_{\mathsf{ct}})\}$
  $(\mathsf{st}, \mathsf{p}_i) \leftarrow \mathsf{Sim}_2(\mathsf{st}, \mathsf{ct}, i, \mu)$
else
  $(\mathsf{st}, \mathsf{p}_i) \leftarrow \mathsf{Sim}_1(\mathsf{st}, \mathsf{ct}, i)$
return p_i

Fig. 2: Strong simulation security experiments for ThFHE.

3 The First Construction

We now describe the first construction of ThFHE based on Shamir secret sharing and analyze it. The first construction is largely analogous to those described in [BGG+18,CKL24,BFM+25], but is more general. We do not require the underlying scheme to be special[7] and obtain similar guarantees for correctness

[7] Specialness requires that a ciphertext is of the form $(a, b) \in R_q^2$ and satisfies $a \cdot \mathsf{sk} + b = \mu + C_{\mathsf{dec}} \cdot e$ for some scalar $C_{\mathsf{dec}} \in R$. It is enforced in prior works by

and simulation security by design of our threshold decryption protocol. This allows us to obtain ThFHE constructions from plain BFV, BGV, or CKKS, while prior works only considered special variants of GSW [BGG+18,CKL24] or BGV [BFM+25].

3.1 Construction

For simplicity, we focus on a BFV description and discuss later how to adapt the first construction to other schemes. We recall that BFV is an IND-CPA-secure FHE scheme $(\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Eval}', \mathsf{Dec}')$ for which a ciphertext ct is of the form $(a, b) \in R_q^2$ and satisfies:

$$b + a \cdot \mathsf{sk} = \left\lceil \frac{q}{p} \right\rfloor \cdot \mu + e \bmod q \ ,$$

for some error $e \in R_q$ satisfying $\|e\|_\infty \leq B_{\mathsf{eval}}$, where sk denotes the FHE secret key, $p \geq 2$ denotes the plaintext modulus (so that the plaintext space is R_p), and $B_{\mathsf{eval}} \geq 1$ is a bound on the error magnitude.

Let $\mathcal{I} = \{\alpha_0, \ldots, \alpha_n\} \subset R_q$ be a set of interpolation points for Shamir secret sharing, and let $C_{\mathsf{dec}}, C_{\mathsf{sim}} \in R$ denote two parameters. Let us also introduce an additional noise bound $B_{\mathsf{sm}} \geq 1$. We construct a ThFHE scheme $\Pi_{\mathsf{ThFHE}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{PartDec}, \mathsf{FinDec})$ as follows. It uses the same encryption and evaluation algorithms $(\mathsf{Enc}', \mathsf{Eval}')$ as the underlying (BFV) FHE scheme.

3.2 Analysis

We now state correctness and simulation security theorems for Π_{ThFHE}. Note that compactness is inherited from that of the underlying FHE scheme, as we alter neither the encryption nor the evaluation algorithms.

Theorem 3.1. *Assume that the following two conditions hold.*

(C1) Decryption Invertibility. *Parameter $C_{\mathsf{dec}} \in R$ is invertible modulo p.*
(C2) Decryption Correctness. *For any authorized set $\mathcal{S} \in \mathbb{A}_{n,t}$, we have:*

$$\|C_{\mathsf{dec}} \bmod q\|_1 \left(B_{\mathsf{eval}} + \frac{p}{4}\right) + tB_{\mathsf{sm}} \max_{i \in \mathcal{S}} \left\|(C_{\mathsf{sim}} \lambda_i^{\mathcal{S} \to \alpha_0}) \bmod q\right\|_1 < \frac{q}{2p} \ .$$

Then Π_{ThFHE} is well-defined and correct.

---

sampling fresh errors for public keys and encryption of the form $C_{\mathsf{dec}} \cdot e$, so that the property carries over. Yet, preserving this property during evaluation is not always simple, in particular for CKKS, since evaluation involves $\mathsf{Rescale}$ operations which introduce rounding errors that are not of this form. Our approach to threshold decryption circumvents this difficulty and allows us to rely on the usual encryption and evaluation algorithms without modifying them.

$\mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$:

1 $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}'(1^\lambda)$
2 $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n) \leftarrow \mathsf{Share}(\mathsf{sk}; n, t, \mathcal{I})$
3 **return** $((\mathsf{sk}_i)_{i\in[n]}, \mathsf{pk})$

$\mathsf{FinDec}(\mathsf{ct}, (\mathsf{p}_i)_{i\in\mathcal{S}})$:

1 parse ct as $(a, b) \in R_q^2$
2 $x \leftarrow C_{\mathsf{dec}} \cdot b + \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} \cdot \mathsf{p}_i \bmod q$
3 $y \leftarrow \left\lceil x \cdot \frac{p}{q} \right\rfloor \bmod p$
4 **return** $C_{\mathsf{dec}}^{-1} \cdot y \bmod p$

$\mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct})$:

1 parse ct as $(a, b) \in R_q^2$
2 $e_{\mathsf{fl},i} \leftarrow U(R^{B_{\mathsf{sm}}})$, where $R^{B_{\mathsf{sm}}} := \{e \in R : \|e\|_\infty \le B_{\mathsf{sm}}\}$
3 **return** $\mathsf{p}_i \leftarrow C_{\mathsf{dec}} \cdot a \cdot \mathsf{sk}_i + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q$

Fig. 3: The first construction Π_{ThFHE}. Enc and Eval are respectively Enc' and Eval'.

We note that the term $p/4$ above arises from bounding $|q \bmod p|$ and can be decreased by an appropriate design choice for q. In Condition **(C2)**, the interpolation set enters through the Lagrange coefficient in $\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to\alpha_0}) \bmod q\|_1$, while the choice of the clearing factor C_{dec} determines $\|C_{\mathsf{dec}} \bmod q\|_1$.

Proof. Let $t \le n$ and $\mathcal{S} \in \mathbb{A}_{n,t}$ be an authorized set. Let f be a circuit with arity $\ell \ge 1$, $(\mu_j)_{j\in[\ell]}$ be plaintexts, and let $\hat{\mu} = f(\mu_1, \ldots, \mu_\ell)$. Let $\mathsf{ct}_j \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu_j)$ for $j \in [\ell]$ and $\hat{\mathsf{ct}} = (a, b) \leftarrow \mathsf{Eval}(\mathsf{pk}, f, (\mathsf{ct}_j)_{j\in[\ell]})$. Then define $\mathsf{p}_i \leftarrow \mathsf{PartDec}(\mathsf{sk}_i, \hat{\mathsf{ct}})$, for all $i \in \mathcal{S}$. Recall that we have:

$$b + a \cdot \mathsf{sk} = \left\lceil \frac{q}{p} \right\rfloor \cdot \hat{\mu} + \hat{e} \bmod q \ ,$$

for some $\hat{e} \in R$ with $\|\hat{e}\|_\infty \le B_{\mathsf{eval}}$, and that for all $i \in \mathcal{S}$, we have:

$$\mathsf{p}_i = C_{\mathsf{dec}} \cdot a \cdot \mathsf{sk}_i + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ ,$$

for some $e_{\mathsf{fl},i} \in R$ with $\|e_{\mathsf{fl},i}\|_\infty \le B_{\mathsf{sm}}$.

Algorithm FinDec first computes, modulo q,

$$\begin{aligned} x &= C_{\mathsf{dec}} b + \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} \mathsf{p}_i \\ &\equiv C_{\mathsf{dec}}(b + a\mathsf{sk}) + C_{\mathsf{sim}} \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} e_{\mathsf{fl},i} \\ &\equiv \left\lceil \frac{q}{p} \right\rfloor C_{\mathsf{dec}} \hat{\mu} + C_{\mathsf{dec}} \hat{e} + C_{\mathsf{sim}} \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} e_{\mathsf{fl},i} \pmod q. \end{aligned}$$

Let $r := q - p\left\lceil \frac{q}{p} \right\rfloor$. By the definition of $\left\lceil \frac{q}{p} \right\rfloor$ as the nearest integer to q/p, we have $|r| \le p/2$ and $p\left\lceil \frac{q}{p} \right\rfloor = q - r$. For the analysis, choose the lift of x to R

for which the preceding congruence is an equality. Any other lift differs by a multiple of q, which changes $\lceil xp/q \rfloor$ by a multiple of p and therefore does not change its value modulo p. For this chosen lift,

$$\frac{p}{q}x = C_{\mathsf{dec}}\hat{\mu} + \frac{F}{q}, \qquad F := -rC_{\mathsf{dec}}\hat{\mu} + pC_{\mathsf{dec}}\hat{e} + pC_{\mathsf{sim}} \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} e_{\mathsf{fl},i}.$$

Using the centered representative of $\hat{\mu}$, the polynomial product bound, and the triangle inequality, we obtain

$$\begin{aligned} \|rC_{\mathsf{dec}}\hat{\mu}\|_\infty &\le \frac{p^2}{4}\|C_{\mathsf{dec}} \bmod q\|_1, \\ \|pC_{\mathsf{dec}}\hat{e}\|_\infty &\le pB_{\mathsf{eval}}\|C_{\mathsf{dec}} \bmod q\|_1, \\ \left\| pC_{\mathsf{sim}} \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} e_{\mathsf{fl},i} \right\|_\infty &\le ptB_{\mathsf{sm}} \max_{i\in\mathcal{S}} \left\|(C_{\mathsf{sim}}\lambda_i^{\mathcal{S}\to\alpha_0}) \bmod q\right\|_1. \end{aligned}$$

Consequently,

$$\|F\|_\infty \le p\left[\|C_{\mathsf{dec}} \bmod q\|_1 \left(B_{\mathsf{eval}} + \frac{p}{4}\right) + tB_{\mathsf{sm}} \max_{i\in\mathcal{S}} \left\|(C_{\mathsf{sim}}\lambda_i^{\mathcal{S}\to\alpha_0}) \bmod q\right\|_1\right].$$

Condition **(C2)** gives $\|F\|_\infty < q/2$, so coefficient-wise rounding yields $y = \lceil xp/q \rfloor \bmod p = C_{\mathsf{dec}}\hat{\mu} \bmod p$. Condition **(C1)** then gives $\mathsf{FinDec}(\hat{\mathsf{ct}}, (\mathsf{p}_i)_{i\in\mathcal{S}}) = \hat{\mu}$. □

Theorem 3.2. *Assume that the underlying FHE scheme is* IND-CPA*-secure and that the following two conditions hold.*

(C3) Simulation Invertibility. *Parameter $C_{\mathsf{sim}} \in R$ is invertible modulo q.*
(C4) Simulation Flooding. *For any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ and any $i \in [n] \setminus \mathcal{S}^*$ with $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$:*

$$B_{\mathsf{eval}} \cdot 2^\lambda \cdot N \cdot \left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^*\to\alpha_i} \right) \bmod q \right\|_1 \le B_{\mathsf{sm}} \ .$$

Then Π_{ThFHE} is simulation-secure.

Proof. Let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ denote a PPT adversary. On input pk, algorithm $\mathcal{A}_0$ returns a set of users $\mathcal{S}_{\mathsf{cor}}$ to corrupt, with $|\mathcal{S}_{\mathsf{cor}}| = t - 1$, as required in Definition 2.9.

Hybrid H_0. This is the real experiment $\mathsf{Exp}^{\mathsf{Sim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)$.

Hybrid H_1. In this experiment, we change how the partial decryption queries are answered. Consider a partial decryption query (j, i), where the index j determines a previously generated ciphertext $\mathsf{ct}_j = (a_j, b_j)$ and the index i specifies a non-corrupted party P_i.

In the real experiment H_0, the challenger returns $\mathsf{p}_i^{(j)} := \mathsf{PartDec}(\mathsf{sk}_i, \mathsf{ct}_j)$, which is defined as:

$$\mathsf{p}_i^{(j)} = C_{\mathsf{dec}} \cdot a_j \cdot \mathsf{sk}_i + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ ,$$

with $e_{\mathsf{fl},i} \leftarrow U(R^{B_{\mathsf{sm}}})$.

In Hybrid H_1, the challenger replies differently. Since $\mathcal{S}_{\mathsf{cor}}$ is a maximal unauthorized set, we have $\mathcal{S}^* \in \mathbb{A}_{n,t}$. Moreover, for $i \in [n] \setminus \mathcal{S}^*$, Shamir reconstruction gives:

$$\mathsf{sk}_i = \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk} + \sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk}_k \bmod q \ .$$

Furthermore, the ciphertext $\mathsf{ct}_j = (a_j, b_j)$ satisfies:

$$a_j \cdot \mathsf{sk} + b_j = \left\lceil \frac{q}{p} \right\rfloor \cdot \mu_j + e_j \bmod q \ ,$$

for some error $e_j \in R_q$ with $\|e_j\|_\infty \leq B_{\mathsf{eval}}$, where μ_j is the underlying plaintext. Combining the two equations above, we obtain, modulo q:

$$\begin{aligned} a_j \cdot \mathsf{sk}_i &= a_j \cdot \left(\lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk} + \sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk}_k \right) \\ &= \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \left(\left\lceil \frac{q}{p} \right\rfloor \cdot \mu_j + e_j - b_j \right) + a_j \cdot \left(\sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk}_k \right) \ , \end{aligned}$$

and therefore:

$$a_j \cdot \mathsf{sk}_i - \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot e_j = \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \left(\left\lceil \frac{q}{p} \right\rfloor \cdot \mu_j - b_j \right) + a_j \cdot \left(\sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk}_k \right) \bmod q \ .$$

Motivated by the latter equation, in Hybrid H_1, the challenger replies to the decryption query (j, i) as follows:

1. It first recovers $(\mu_j, \mathsf{ct}_j) \leftarrow \mathsf{L}[j]$ and computes $\lambda_k^{\mathcal{S}^* \to \alpha_i}$ for all $k \in \mathcal{S}^*$;
2. It samples $e_{\mathsf{fl},i} \leftarrow U(R^{B_{\mathsf{sm}}})$ and returns $\mathsf{p}_i^{(j)} \leftarrow \mathsf{Sim}_1(\mathsf{st}, \mathsf{ct}_j, i, \mu_j)$, defined as:

$$\begin{aligned} \mathsf{p}_i^{(j)} \leftarrow C_{\mathsf{dec}} \Bigg(& \lambda_0^{\mathcal{S}^* \to \alpha_i} \left(\left\lceil \frac{q}{p} \right\rfloor \mu_j - b_j \right) + a_j \sum_{k \in \mathcal{S}_{\mathsf{cor}}} \lambda_k^{\mathcal{S}^* \to \alpha_i} \mathsf{sk}_k \Bigg) \\ & + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ . \end{aligned}$$

By construction, we have:

$$\mathsf{p}_i^{(j)} = C_{\mathsf{dec}} \cdot a_j \cdot \mathsf{sk}_i - \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot C_{\mathsf{dec}} \cdot e_j + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ .$$

Notice that the challenger no longer relies on knowledge of sk_i to compute $\mathsf{p}_i^{(j)}$, but only on the ciphertext ct_j, the underlying plaintext μ_j, and the corrupted secret keys $(\mathsf{sk}_k)_{k \in \mathcal{S}_{\mathsf{cor}}}$. Lemma 3.3 below follows a standard smudging argument and shows that H_1 is statistically indistinguishable from H_0.

Lemma 3.3. *Assuming Conditions* **(C3)** *and* **(C4)** *hold, Hybrids* H_0 *and* H_1 *are statistically indistinguishable.*

Proof. The difference between the two experiments is that, in H_0, we have:

$$\mathsf{p}_i^{(j)} = C_{\mathsf{dec}} \cdot a_j \cdot \mathsf{sk}_i + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ ,$$

while in H_1, it is set to:

$$\mathsf{p}_i^{(j)} = C_{\mathsf{dec}} \cdot a_j \cdot \mathsf{sk}_i - \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot C_{\mathsf{dec}} \cdot e_j + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ .$$

Since a_j and sk_i are identically distributed in both experiments, it is sufficient to bound:

$$\Delta\left(C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}, -\lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot C_{\mathsf{dec}} \cdot e_j + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}\right) \ ,$$

over the randomness of $e_{\mathsf{fl},i}$, where both sides are computed modulo q. As C_{sim} is invertible modulo q (by Condition **(C3)**), it suffices to bound:

$$\Delta\left(e_{\mathsf{fl},i}, -\lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot e_j + e_{\mathsf{fl},i}\right) \ .$$

By the probability preservation property, it suffices to bound

$$\Delta\left(e_{\mathsf{fl},i}, -\left(\lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \bmod q\right) \cdot e_j + e_{\mathsf{fl},i}\right) \ .$$

Lemma 2.4 ensures that the above quantity is at most $2^{-\lambda}$ as soon as we have:

$$B_{\mathsf{sm}} \geq N \cdot 2^{\lambda} \cdot \left\| \left(\lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \bmod q\right) \cdot e_j \right\|_{\infty} \ ,$$

which is implied by Condition **(C4)**. □

Hybrid H_2. This experiment is as H_1, except that the challenger now generates the corrupted secret keys $(\mathsf{sk}_k)_{k \in \mathcal{S}_{\mathsf{cor}}}$ by sampling $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n) \leftarrow \mathsf{Share}(0; n, t, \mathcal{I})$ and returning $(\mathsf{sk}_k)_{k \in \mathcal{S}_{\mathsf{cor}}}$. We call the latter process Sim_0. By the privacy of Shamir secret sharing, Hybrid H_2 is statistically indistinguishable from Hybrid H_1.

The proof is completed, since H_2 corresponds to $\mathsf{Exp}^{\mathsf{Sim}}_{\mathsf{Ideal}}$ with simulator $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$. □

3.3 Extensions to BGV and CKKS

We now describe how the first construction extends to BGV and CKKS. For BGV, one can convert the BGV ciphertext to be decrypted into a BFV ciphertext at the beginning of $\mathsf{PartDec}$ and then apply the threshold-decryption procedure described above. If the plaintext modulus p and ciphertext modulus q satisfy $q \equiv 1 \pmod{p}$, this conversion is obtained by multiplying the ciphertext by $(q-1)/p$, which is congruent to $-p^{-1}$ modulo q.

For CKKS, we recall that a ciphertext is a pair $(a, b) \in R_q^2$ satisfying $a \cdot \mathsf{sk} + b = \Delta\mu + e$ for some scaling factor $\Delta > 0$ and some error e with $\|e\|_{\infty} \leq B_{\mathsf{eval}}$.

The approach is adapted by changing Step 3 of FinDec to $y \leftarrow \lceil x/\Delta \rfloor$ and changing Step 4 so that it returns y/C_{dec}, where both divisions are defined over K. Consistently, Condition (**C1**) becomes $C_{\mathsf{dec}} \neq 0$, while Condition (**C2**) should be replaced by the requirement that for any authorized set $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, the following two inequalities hold:

$$B_{\mathsf{eval}} \cdot \|C_{\mathsf{dec}} \bmod q\|_1 + t \cdot B_{\mathsf{sm}} \cdot \left\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to\alpha_0}) \bmod q\right\|_1 < \Delta \cdot 2^{-P-1}$$
$$M \cdot \|C_{\mathsf{dec}} \bmod q\|_1 + 2^{-P-1} < \frac{q}{2\Delta} \ ,$$

where M is a bound on $\|\mu\|_\infty$ and P is the target precision. The first inequality implies that the quantity computed at Step 2 of FinDec has its noise terms sufficiently separated from the plaintext $C_{\mathsf{dec}} \cdot \mu$. The second inequality guarantees that this quantity is defined over R rather than R_q. Conditions **(C3)** and **(C4)** of Theorem 3.2 remain unchanged.

3.4 Bounding the Ciphertext Modulus

In this subsection, we derive a lower bound on the ciphertext modulus q for Π_{ThFHE}. This magnitude is governed by Conditions (C2) and (C4) of Theorems 3.1 and 3.2, which ensure correctness and simulation security. Specifically, (C2) depends on the smudging noise bound B_{sm}, while (C4) dictates the minimal choice for B_{sm}. Combining both theorems, we fix B_{sm} throughout our analysis to its minimal valid value:

$$B_{\mathsf{sm}} = B_{\mathsf{eval}} \cdot 2^\lambda \cdot N \cdot \max_{i,\,\mathcal{S}^*} \left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^*\to\alpha_i} \right) \bmod q \right\|_1 \ .$$

From this setting, one may derive the following lower bound on q:

$$\frac{q}{2p} > \left(B_{\mathsf{eval}} + \frac{p}{4}\right) B_1 + t B_{\mathsf{eval}} 2^\lambda N B_2 B_3 \ ,$$

where

$$B_1 := \|C_{\mathsf{dec}} \bmod \ q\|_1 \ ,$$
$$B_2 := \max_{i,\,\mathcal{S}} \ \|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}) \ \bmod \ q\|_1 \ ,$$
$$B_3 := \max_{i,\,\mathcal{S}^*} \ \|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^*\to\alpha_i}) \ \bmod q\|_1 \ .$$

The ranges of i and $\mathcal{S}$ (resp. i and $\mathcal{S}^*$) are as in Theorem 3.1 (resp. Theorem 3.2). Ignoring lower-order terms, the ciphertext modulus q is dominated by the contribution $t \cdot B_{\mathsf{eval}} \cdot 2^\lambda \cdot N \cdot B_2 \cdot B_3$, together with the additive term B_1.

In what follows, we analyze the integer interpolation set $\mathcal{I}_{\text{int}}$ (Section 3.5), the centered integer interpolation set $\mathcal{I}_{\text{c-int}}$ (Section 3.6), and the monomial interpolation set $\mathcal{I}_{\text{mon}}$ (Section 3.7). In these settings, the product $B_2 \cdot B_3$ is the dominant contribution to the required growth of q. Therefore, the rest of this analysis focuses on obtaining tight upper bounds on B_2 and B_3, and hence on $B_2 \cdot B_3$.

3.5 The Integer Interpolation Set

We start our study with the most common choice for Lagrange interpolation points: $\mathcal{I}_{\text{int}} := \{0, 1, \ldots, n\}$. This is, in particular, the set of points considered in [BGG+18,CKL24]. To the best of our knowledge, our analysis improves those available in all prior works. In what follows, we show that for this choice of interpolation points, one can set $C_{\mathsf{dec}} = (n!)^2$ and $C_{\mathsf{sim}} = n!$.

Theorem 3.4. *Let $C_{\mathsf{dec}} = n!^2$ and $C_{\mathsf{sim}} = n!$, and assume that p, q have all their prime factors greater than n. Then:*

- *the Lagrange reconstruction coefficients associated to $\mathcal{I}_{\text{int}}$ are well-defined over R_q;*
- *Conditions* **(C1)** *and* **(C3)** *hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, we have:*

$$\left|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}) \bmod q\right| \;\leq\; \frac{n!^2}{(n-t)! \cdot \lfloor t/2 \rfloor!^2} \;;$$

- *for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ and $i \in [n] \setminus \mathcal{S}^*$ with $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, we have:*

$$\left|\left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^*\to i}\right) \bmod q\right| \;\leq\; \frac{n!^2}{(n-t)! \cdot t!} \;.$$

We note that the condition on p may be restrictive in the BFV and BGV contexts. This condition vanishes in the CKKS context. The proof also hints that these bounds are tight, up to polynomial factors.

Proof. First, observe that $C_{\mathsf{dec}} = n!^2$ (resp. $C_{\mathsf{sim}} = n!$) is invertible modulo p (resp. modulo q) as all prime factors of p (resp. of q) are larger than n. Let $\mathcal{S} \subseteq [n]$ of size t and let $i \in \mathcal{S}$. We have (over R_q):

$$\lambda_i^{\mathcal{S}\to 0} = \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{-j}{i-j} \;.$$

Then the Lagrange reconstruction coefficient $\lambda_i^{\mathcal{S}\to 0}$ is well-defined over R_q as all prime factors of q are larger than any denominator factor. Now, let us consider the denominator of $\lambda_i^{\mathcal{S}\to 0}$. Note that $\prod_{j\in\mathcal{S}\setminus\{i\}}(i-j)$ divides $\prod_{0\leq j\leq n, j\neq i}(i-j)$, which is equal to $\pm i! \cdot (n-i)!$. Since $\binom{n}{i} = \frac{n!}{i!\cdot(n-i)!}$ is an integer, we obtain that $\prod_{j\in\mathcal{S}\setminus\{i\}}(i-j)$ divides $C_{\mathsf{sim}} = n!$. Therefore, the quantity $C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}$ can be viewed as an integer. We now bound it. Observing that an integer in the denominator of $\lambda_i^{\mathcal{S}\to 0}$ can appear twice (up to sign), we have:

$$\left| n! \cdot \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{-j}{i-j} \right| \leq n! \cdot \frac{\displaystyle\prod_{n-t+1\leq j\leq n} j}{\displaystyle\prod_{1\leq j\leq \lfloor t/2\rfloor} j^2} = \frac{n!^2}{(n-t)! \cdot \lfloor t/2 \rfloor!^2} \;,$$

where the divisions in the left-most product are over $\mathbb{Q}$ (with the overall term in $\mathbb{Z}$). Using the fact that the absolute value cannot increase when reducing modulo q, we obtain the third statement of Theorem 3.4.

Let $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$ and $i \in [n] \setminus \mathcal{S}^*$. We have (over R_q):

$$\lambda_0^{\mathcal{S}^* \to i} = \prod_{j \in \mathcal{S}^* \setminus \{0\}} \frac{i-j}{-j} \ .$$

Thanks to the arithmetic assumption on q, this is well-defined over R_q. Furthermore, the denominator divides $C_{\mathsf{dec}}/C_{\mathsf{sim}} = n!$, so that the quantity $(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \to i}$ can be viewed as an integer. We bound it as follows:

$$\left| n! \cdot \prod_{j \in \mathcal{S}^* \setminus \{0\}} \frac{i-j}{-j} \right| \ \leq \ n! \cdot \frac{\prod_{n-t+1 \leq j \leq n-1} j}{\prod_{1 \leq j \leq t-1} j} \ = \ \frac{n! \cdot (n-1)!}{(n-t)! \cdot (t-1)!} \ ,$$

where the divisions in the left-most product are over $\mathbb{Q}$. As the absolute value cannot increase when reducing modulo q, this proves the last statement of Theorem 3.4. □

Combining Theorem 3.4 with Theorems 3.1 and 3.2, we obtain correctness and simulation security. The following corollary gives the bound on $B_2 \cdot B_3$ in that setting.

Corollary 3.5. *Assume that the hypotheses of Theorem 3.4 hold. Then we have:*

$$B_2 \cdot B_3 \leq \frac{n!^4}{(n-t)!^2 \cdot t! \cdot \lfloor t/2 \rfloor !^2} \ .$$

Proof. By Theorem 3.4, we have

$$\left| (C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q \right| \leq \frac{n!^2}{(n-t)! \cdot \lfloor t/2 \rfloor !^2}$$

and

$$\left| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^* \to i} \right) \bmod q \right| \leq \frac{n!^2}{(n-t)! \cdot t!} \ .$$

Multiplying the two bounds yields the result. □

3.6 The Centered Integer Interpolation Set

We now consider the following zero-centered integer interpolation points:

$$\mathcal{I}_{\text{c-int}} = \{-\lfloor n/2 \rfloor, \ldots, 0, \ldots, \lceil n/2 \rceil\} = \left\{ (-1)^{i+1} \cdot \left\lfloor \frac{i+1}{2} \right\rfloor \ \middle| \ 0 \leq i \leq n \right\} \ .$$

We define $\alpha_i = (-1)^{i+1} \cdot \lfloor (i+1)/2 \rfloor$ for $0 \leq i \leq n$. Although the centered set reduces the size of the interpolation points themselves, the simulation coefficient involves differences $\alpha_i - \alpha_j$, which may still be as large as n. We therefore analyze the correctness and simulation coefficients separately.

Theorem 3.6. *Let $C_{\mathsf{dec}} = n! \cdot \lceil n/2 \rceil!^2$ and $C_{\mathsf{sim}} = n!$, and assume that p, q have all their prime factors greater than n. Then:*

- *the Lagrange reconstruction coefficients associated to $\mathcal{I}_{\text{c-int}}$ are well-defined over R_q;*
- *Conditions* **(C1)** *and* **(C3)** *hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, we have:*

$$\left|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}) \bmod q\right| \;\leq\; n! \cdot \binom{\lceil n/2 \rceil}{\lfloor t/2 \rfloor}^2 \;;$$

- *for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ and $i \in [n] \setminus \mathcal{S}^*$ with $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, we have:*

$$\left|\left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^*\to \alpha_i}\right) \bmod q\right| \;\leq\; \lceil n/2 \rceil!^2 \cdot \binom{\lceil n/2 \rceil + \lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}^2 \;.$$

The proof is adapted from the analysis of Section 3.5.

Proof. First, observe that $C_{\mathsf{dec}} = n! \cdot \lceil n/2 \rceil!^2$ (resp. $C_{\mathsf{sim}} = n!$) is invertible modulo p (resp. modulo q) as all prime factors of p (resp. q) are larger than n. Let $\mathcal{S} \subseteq \{-\lfloor n/2 \rfloor, \ldots, \lceil n/2 \rceil\} \setminus \{0\}$ of size t and let $i \in \mathcal{S}$. We have (over R_q):

$$\lambda_i^{\mathcal{S}\to 0} = \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{-\alpha_j}{\alpha_i - \alpha_j} \;.$$

Then the Lagrange reconstruction coefficient $\lambda_i^{\mathcal{S}\to 0}$ is well-defined over R_q as all prime factors of q are larger than any term in the denominator. Now, let us consider the denominator of $\lambda_i^{\mathcal{S}\to 0}$. Note that $\prod_{j\in\mathcal{S}\setminus\{i\}}(\alpha_i - \alpha_j)$ divides

$$\prod_{\substack{-\lfloor n/2 \rfloor \leq j \leq \lceil n/2 \rceil \\ j \neq i}} (\alpha_i - \alpha_j) \;=\; \pm(\lfloor n/2 \rfloor + \alpha_i)! \cdot (\lceil n/2 \rceil - \alpha_i)! \;.$$

Since $\binom{n}{\lfloor n/2 \rfloor + \alpha_i}$ is an integer, we obtain that $\prod_{j\in S\setminus\{i\}}(\alpha_i - \alpha_j)$ divides $C_{\mathsf{sim}} = n!$. Therefore, the quantity $C_{\mathsf{sim}} \cdot \lambda_i^{S\to 0}$ can be viewed as an integer. We now bound it. Observing that an integer in the denominator of $\lambda_i^{\mathcal{S}\to 0}$ can appear twice (up to sign), and that the same holds for the numerator, we have:

$$\begin{aligned}\left| n! \cdot \prod_{j\in S\setminus\{i\}} \frac{-\alpha_j}{\alpha_i - \alpha_j} \right| &\leq n! \cdot \frac{\displaystyle\prod_{\lceil n/2 \rceil - \lfloor t/2 \rfloor + 1 \leq j \leq \lceil n/2 \rceil} j^2}{\displaystyle\prod_{1 \leq j \leq \lfloor t/2 \rfloor} j^2} \\ &= n! \cdot \left(\frac{\lceil n/2 \rceil!}{(\lceil n/2 \rceil - \lfloor t/2 \rfloor)! \cdot \lfloor t/2 \rfloor!}\right)^2 \;,\end{aligned}$$

where the divisions in the left-most product are over $\mathbb{Q}$ (with the overall term in $\mathbb{Z}$). Using the fact that the absolute value cannot increase by reducing modulo q, we obtain the third theorem statement.

Let $\mathcal{S}_{\mathsf{cor}} \subseteq \{-\lfloor n/2 \rfloor, \ldots, \lceil n/2 \rceil\} \setminus \{0\}$ of size $t-1$, $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$ and $i \in \{-\lfloor n/2 \rfloor, \ldots, \lceil n/2 \rceil\} \setminus \mathcal{S}^*$. We have (over R_q):

$$\lambda_0^{\mathcal{S}^* \to \alpha_i} = \prod_{j \in \mathcal{S}^* \setminus \{0\}} \frac{\alpha_i - \alpha_j}{-\alpha_j} \ .$$

Thanks to the arithmetic assumption on q, this is well-defined over R_q. Furthermore, the denominator divides $C_{\mathsf{dec}}/C_{\mathsf{sim}} = \lceil n/2 \rceil!^2$, so that the quantity $(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i}$ can be viewed as an integer, which we bound as follows. For every $j \in \mathcal{S}^* \setminus \{0\}$, we have $|\alpha_i - \alpha_j| \leq |\alpha_i| + |\alpha_j| \leq \lceil n/2 \rceil + |\alpha_j|$, hence

$$\left| \frac{\alpha_i - \alpha_j}{\alpha_j} \right| \ \leq \ 1 + \frac{\lceil n/2 \rceil}{|\alpha_j|} \ .$$

Note that among the nonzero centered interpolation points, each absolute value $r \in \{1, \ldots, \lceil n/2 \rceil\}$ occurs at most twice. Therefore, the product of $t-1$ such factors is bounded from above by taking two copies of $(1 + \lceil n/2 \rceil / r)$ for r from 1 to $\lfloor t/2 \rfloor$:

$$\prod_{j \in \mathcal{S}^* \setminus \{0\}} \left| \frac{\alpha_i - \alpha_j}{\alpha_j} \right| \ \leq \ \prod_{r=1}^{\lfloor t/2 \rfloor} \left(1 + \frac{\lceil n/2 \rceil}{r} \right)^2 \ = \ \binom{\lceil n/2 \rceil + \lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}^2 \ .$$

Consequently, we have

$$\left| \lceil n/2 \rceil!^2 \cdot \prod_{j \in \mathcal{S}^* \setminus \{0\}} \frac{\alpha_i - \alpha_j}{-\alpha_j} \right| \ \leq \ \lceil n/2 \rceil!^2 \cdot \binom{\lceil n/2 \rceil + \lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}^2 \ .$$

As the absolute value cannot increase when reducing modulo q, this proves the last statement of the theorem. □

Corollary 3.7. *Let $C_{\mathsf{dec}} = n! \cdot \lceil n/2 \rceil!^2$ and $C_{\mathsf{sim}} = n!$, and assume that p, q have all their prime factors greater than n. If the first construction described in Section 3.1 using interpolation points $\mathcal{I}_{\text{c-int}}$ is correct and simulation-secure, then for any $\mathcal{S} \in \mathbb{A}_{n,t}$, any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, and any $i \in \mathcal{S}$ such that $i \notin \mathcal{S}_{\mathsf{cor}}$, we have*

$$\begin{aligned} &\left\| (C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q \right\|_1 \cdot \left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \right) \bmod q \right\|_1 \\ &\quad \leq \ \left(n! \cdot \binom{\lceil n/2 \rceil}{\lfloor t/2 \rfloor}^2 \right) \cdot \left(\lceil n/2 \rceil!^2 \cdot \binom{\lceil n/2 \rceil + \lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}^2 \right) \\ &\quad = \ n! \cdot \lceil n/2 \rceil!^2 \cdot \binom{\lceil n/2 \rceil}{\lfloor t/2 \rfloor}^2 \cdot \binom{\lceil n/2 \rceil + \lfloor t/2 \rfloor}{\lfloor t/2 \rfloor}^2 \ . \end{aligned} \tag{1}$$

Proof. The inequality (1) follows by multiplying the two bounds stated in Theorem 3.6 for $\left| (C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q \right|$ and $\left| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \right) \bmod q \right|$. □

As discussed for $\mathcal{I}_{\text{int}}$, the second summand in the first condition gives higher stress on q, when B_{eval} and p are small. One may also check that the condition on q in Corollary 3.7 is asymptotically less demanding than in Corollary 3.5. This may be seen by using the inequalities $(n/2)!^2 \leq n!$ and $\binom{n/2}{t/2}^2 \leq \binom{n}{t}$. Finally, we note that the constraints on q are essentially the same for t and $n-t$.

3.7 The Monomial Interpolation Set

We now study the set of interpolation points $\mathcal{I}_{\text{mon}} := \{0, 1, x, x^2, \ldots, x^{n-1}\}$, assuming $n \leq 2N$. This set is notably studied in [CLW25], in which the authors set $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$. It is also studied in [BFM+25].

Theorem 3.8. *Let $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, and assume that $p, q > 2$ are odd. Then:*

- *the Lagrange reconstruction coefficients associated to $\mathcal{I}_{\text{mon}}$ are well-defined over R_q;*
- *Conditions* **(C1)** *and* **(C3)** *hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, the quantity $\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}) \bmod q\|_1$ is bounded from above by:*

$$2^{-t+\lceil \log t \rceil + 1} \cdot \sqrt{N} \cdot \prod_{k \in [\lfloor t/2 \rfloor]} \frac{1}{\sin^2\left(\pi \frac{k}{2N}\right)} \ ;$$

- *for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ and $i \in [n] \setminus \mathcal{S}^*$ with $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, the quantity $\|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \to x^{i-1}}) \bmod q\|_1$ is bounded from above by:*[8]

$$2^{t-1} \cdot \sqrt{N} \cdot \prod_{k \in [\lfloor t/2 \rfloor - 1]} \cos^2\left(\pi \frac{k}{2N}\right) \ .$$

Proof. Let us first make explicit the Lagrange coefficients involved in the construction. For $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, we have:

$$\lambda_i^{\mathcal{S}\to 0} = \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{-x^j}{x^i - x^j} = \pm \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{1}{x^{i-j} - 1} \ .$$

For $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$ and $i \in [n] \setminus \mathcal{S}^*$, we have:

$$\lambda_0^{\mathcal{S}^* \to x^{i-1}} = \prod_{j \in \mathcal{S}^*\setminus\{0\}} \frac{x^i - x^j}{-x^j} = \prod_{j \in \mathcal{S}^*\setminus\{0\}} \left(1 - x^{i-j}\right) \ .$$

They are well-defined over R_q as the ideal $\langle x^k - 1 \rangle$ can only divide powers of the ideal $\langle 2 \rangle$ (by Lemma 2.2) and q is assumed odd. Further, as p and q are both odd, we have that C_{dec} and C_{sim} are invertible modulo p and q, respectively.

[8] By convention, the product is equal to 1 if the range is over an empty set (which is the case for $t \leq 3$).

Now, consider $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$. Recall that $\lambda_i^{\mathcal{S}\to 0}$ is defined in R_q; however, we would like to pass to R to analyze it. For this purpose, we adapt an argument from [AL21, Theorem 1] and [CLW25, Lemma 1]. By [AL21, Theorem 1], the denominator in the expression of $\lambda_i^{\mathcal{S}\to 0}$ above divides $(1-x)^{N\cdot\lceil \log t\rceil}$ (in the sense that the ratio is an element of R). Now, in the cyclotomic ring $R = \mathbb{Z}[x]/(x^N+1)$, the ideal $\langle (1-x)^N\rangle$ is exactly the ideal $\langle 2\rangle$. It follows that the denominator in the definition of $\lambda_i^{\mathcal{S}\to 0}$ divides $C_{\mathsf{sim}} = 2^{\lceil \log t\rceil}$. Below, we hence consider $C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}$, viewed as an element of R.

Using Lemma 2.3, it suffices to bound the magnitude of all complex embeddings of $C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}$. Let σ be any complex embedding sending x to a $(2N)$-th primitive root of unity. There exists an integer r with $\gcd(r, 2N) = 1$ such that $\sigma(x) = \exp(\pi \mathrm{i} r/N) =: \zeta$. Hence, we have

$$\sigma\big(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}\big) = \pm 2^{\lceil \log t\rceil} \cdot \prod_{j\in\mathcal{S}\setminus\{i\}} \frac{1}{\zeta^{i-j}-1} \ .$$

Using the relation $|\zeta^k - 1| = 2|\sin(\pi r k/(2N))|$ yields

$$\big|\sigma(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0})\big| = 2^{-t+\lceil \log t\rceil+1} \cdot \prod_{j\in\mathcal{S}\setminus\{i\}} \frac{1}{\big|\sin(\frac{\pi r(i-j)}{2N})\big|} \ .$$

As r is coprime with $2N$, multiplication by r induces a bijection from $\mathbb{Z}_{2N}\setminus\{0\}$ to itself. Without loss of generality, we may hence assume that $r = 1$ in the optimization above. Let $d(j) \coloneqq \min\{|i-j|, 2N-|i-j|\}$. The multiset $\{d(j) : j \in \mathcal{S}\setminus\{i\}\}$ that maximizes the product is $\{1,1,2,2,\ldots,(\tau-1),(\tau-1),\tau,\tau\}$ if t is odd and $\{1,1,2,2,\ldots,(\tau-1),(\tau-1),\tau\}$ if t is even, where $\tau = \lfloor t/2\rfloor$. As the multiplicands are no smaller than 1, we obtain, in both cases:

$$\big|\sigma(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0})\big| \le 2^{-t+\lceil \log t\rceil+1} \cdot \prod_{k\in[\tau]} \frac{1}{\sin^2(\pi\frac{k}{2N})} \ .$$

Lemma 2.3 gives the inequality of the third statement of Theorem 3.8.

Finally, consider $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, $\mathcal{S}^* = \{0\}\cup\mathcal{S}_{\mathsf{cor}}$ and $i \in [n]\setminus\mathcal{S}^*$. The denominator in the expression of $\lambda_0^{\mathcal{S}^*\to x^{i-1}}$ above is a unit in R, so that $\lambda_0^{\mathcal{S}^*\to x^{i-1}}$ can be viewed as an element of R. As above, we consider an arbitrary complex embedding σ. It sends x to $\zeta \coloneqq \exp(\pi \mathrm{i} r/N)$ for some r that is coprime with $2N$. Using the relation $|\sigma(1-x^{i-j})| = |1-\zeta^{i-j}| = 2|\sin(\pi r(i-j)/(2N))|$, we have:

$$\big|\sigma(\lambda_0^{\mathcal{S}^*\to x^{i-1}})\big| = \prod_{j\in\mathcal{S}^*\setminus\{0\}} \big|1-\zeta^{i-j}\big| = 2^{t-1} \cdot \prod_{j\in\mathcal{S}^*\setminus\{0\}} \left|\sin\Big(\frac{\pi r(i-j)}{2N}\Big)\right| \ .$$

As above, without loss of generality, we may assume that $r = 1$ in this optimization. The product is bounded from above as follows:

$$\prod_{j\in\mathcal{S}^*\setminus\{0\}} \left|\sin\Big(\frac{\pi r(i-j)}{2N}\Big)\right| \le \prod_{1\le k\le\tau-1} \left|\sin\Big(\frac{\pi(N+k)}{2N}\Big)\right|^2 = \prod_{1\le k\le\tau-1} \cos^2\Big(\frac{\pi k}{2N}\Big) \ ,$$

where $\tau = \lfloor t/2 \rfloor$. Note that the right-hand-side products have fewer terms than the left-hand-side product: one missing term corresponds to "$k = 0$", which brings a factor equal to 1; there is another missing term in the case of odd t that we remove for the sake of simplicity, which is allowed as $|\sin x| \leq 1$ for all x. Using the identity $C_{\mathsf{dec}}/C_{\mathsf{sim}} = 1$ and Lemma 2.3 gives the first inequality of the last statement of Theorem 3.8. □

3.8 Bounding $B_2 \cdot B_3$ for the Monomial Interpolation Set

Theorem 3.8 bounds the reconstruction coefficients by two explicit trigonometric products, one with squared inverse sines and one with squared cosines. Their product bounds $B_2 \cdot B_3$, which dominates the condition on q of Section 3.4. This gives the following bound on $B_2 \cdot B_3$, which we call the *trigonometric bound*.

Corollary 3.9. *Assume that the hypotheses of Theorem 3.8 hold. Then we have:*

$$B_2 \cdot B_3 \leq 2^{\lceil \log t \rceil} \cdot N \cdot \frac{1}{\sin^2\left(\pi \frac{\lfloor t/2 \rfloor}{2N}\right)} \cdot \prod_{k \in [\lfloor t/2 \rfloor - 1]} \cot^2\left(\pi \frac{k}{2N}\right) \ .$$

Note that this bound is convenient for numerical evaluation, but may not easily convey intuition on its behavior. For the purpose of intuition, taking the logarithm, replacing the sum by an integral, and focusing on the cotangent product, it may be replaced by the following *heuristic bound*:

$$B_2 \cdot B_3 \lesssim \exp\left(4N \int_0^{t/(4N)} \ln \cot(\pi u)\, \mathrm{d}u\right) \ .$$

We can also prove a rigorous bound, called the *Clausen bound*, on the trigonometric products in Theorem 3.8 in terms of the Clausen function of order 2, giving the following corollary.

Corollary 3.10. *Assume that the hypotheses of Theorem 3.8 hold. Then we have:*

$$B_2 \cdot B_3 \leq 2^{\lceil \log t \rceil + 2} \cdot N \cdot \exp\left(\frac{2N}{\pi}\left(\mathrm{Cl}_2\left(\pi \frac{\lfloor t/2 \rfloor}{N}\right) + \mathrm{Cl}_2\left(\pi \frac{N - \lfloor t/2 \rfloor + 1}{N}\right)\right)\right) \ .$$

Proof. Let $\tau \leq N$. We start with the inverse-sine product. Taking the logarithm, we obtain:

$$\ln\left(\prod_{k \in [\tau]} \frac{1}{\sin^2(\pi \frac{k}{2N})}\right) = -2 \sum_{k \in [\tau]} \ln \sin\left(\pi \frac{k}{2N}\right) \ .$$

As $\tau \leq N$, the function $x \mapsto -\ln \sin(\pi x/(2N))$ decreases on $(0, \tau]$. Hence, by a standard monotonicity comparison, we have

$$-2 \sum_{k \in [\tau]} \ln \sin\left(\pi \frac{k}{2N}\right) \leq -2 \int_0^{\tau} \ln \sin\left(\pi \frac{x}{2N}\right) \mathrm{d}x \ .$$

With the change of variables $u = \pi x/N$, we obtain:

$$\ln\left(\prod_{k\in[\tau]}\frac{1}{\sin^2(\pi\frac{k}{2N})}\right) \leq -\frac{2N}{\pi}\int_0^{\frac{\pi\tau}{N}} \ln\sin\left(\frac{u}{2}\right)\,\mathrm{d}u = (2\ln 2)\tau + \frac{2N}{\pi}\mathrm{Cl}_2\left(\pi\frac{\tau}{N}\right) \ .$$

We now consider the cosine product. As the function $x \mapsto \ln\cos(\pi x/(2N))$ decreases on $(0,\tau]$, we have:

$$\ln\left(\prod_{k\in[\tau]}\cos^2\left(\pi\frac{k}{2N}\right)\right) = 2\sum_{k\in[\tau]}\ln\cos\left(\pi\frac{k}{2N}\right) \leq 2\int_0^{\tau}\ln\cos\left(\pi\frac{x}{2N}\right)\,\mathrm{d}x \ .$$

Using the identity $\cos(x) = \sin(\pi/2 - x)$, the change of variable $u = \pi(N-x)/N$ and the identity $\mathrm{Cl}_2(\pi) = 0$, we obtain:

$$\begin{aligned}
2\int_0^{\tau}\ln\cos\left(\pi\frac{x}{2N}\right)\,\mathrm{d}x &= 2\int_0^{\tau}\ln\sin\left(\pi\frac{N-x}{2N}\right)\,\mathrm{d}x \\
&= \frac{2N}{\pi}\int_{\pi(1-\frac{\tau}{N})}^{\pi}\ln\sin\left(\frac{u}{2}\right)\,\mathrm{d}u \\
&= -(2\ln 2)\tau + \frac{2N}{\pi}\mathrm{Cl}_2\left(\pi\frac{N-\tau}{N}\right) \ .
\end{aligned}$$

The claimed bound follows by taking $\tau = \lfloor t/2\rfloor$ for the inverse-sine product and $\tau = \lfloor t/2\rfloor - 1$ in the cosine product. □

Finally, we give a more explicit bound in the following corollary. This *quadratic bound* tightly approximates the behavior of the product of the trigonometric bounds from Theorem 3.8 for the parameter range that maximizes it, i.e., for t close to N.

Corollary 3.11. *Assume that the hypotheses of Theorem 3.8 hold. Then we have:*

$$B_2 \cdot B_3 < 2^{\lceil\log t\rceil+1}\cdot N\cdot\exp\left(\frac{4GN}{\pi} - \frac{\pi}{N}\left(1-\frac{\pi}{2N}\right)\left(\left\lfloor\frac{t}{2}\right\rfloor - \frac{N+1}{2}\right)^2\right) \ ,$$

where $G \approx 0.916$ is Catalan's constant.

Proof. Let $\tau = \lfloor t/2\rfloor$. From Theorem 3.8, the product of the trigonometric bounds gives:

$$B_2 \cdot B_3 \leq 2^{\lceil\log t\rceil}\cdot N\cdot P(\tau) \ ,$$

where the trigonometric product $P(\tau)$ is defined as:

$$P(\tau) = \frac{1}{\sin^2\left(\pi\frac{\tau}{2N}\right)}\prod_{k\in[\tau-1]}\cot^2\left(\pi\frac{k}{2N}\right) \ .$$

Using the identity $1/\sin^2(x) = 1 + \cot^2(x)$, we eliminate the isolated sine term by distributing the product:

$$P(\tau) = \left(1 + \cot^2\left(\pi\frac{\tau}{2N}\right)\right) \prod_{k\in[\tau-1]} \cot^2\left(\pi\frac{k}{2N}\right)$$
$$= \prod_{k\in[\tau-1]} \cot^2\left(\pi\frac{k}{2N}\right) + \prod_{k\in[\tau]} \cot^2\left(\pi\frac{k}{2N}\right) \ .$$

Let $C_m = \prod_{k\in[m]} \cot^2(\pi k/(2N))$. We bound $\ln C_m = 2\sum_{k\in[m]} \ln\cot(\pi k/(2N))$. Since the function $x \mapsto \ln\cot(\pi x/(2N))$ is strictly decreasing on the interval $(0, N)$, its right Riemann sum is strictly bounded from above by the convergent improper integral starting from 0:

$$\ln C_m < 2\int_0^m \ln\cot\left(\pi\frac{x}{2N}\right)\mathrm{d}x = \frac{4N}{\pi}\int_0^{\frac{\pi m}{2N}} \ln\cot(y)\mathrm{d}y \ .$$

Let $H(\theta) = \int_0^\theta \ln\cot(y)\mathrm{d}y$. Its unique maximum occurs at $\theta = \pi/4$, where $H(\pi/4) = G$. Since $H''(\theta) = -2/\sin(2\theta) \leq -2$ for all $\theta \in (0, \pi/2)$, integrating twice gives that $H(\theta) \leq G - (\theta - \pi/4)^2$. Substituting $\theta = \pi m/(2N)$, we obtain:

$$C_m < \exp\left(\frac{4GN}{\pi} - \frac{\pi}{N}\left(m - \frac{N}{2}\right)^2\right) \ .$$

Now, substituting $m = \tau - 1$ and $m = \tau$ back into $P(\tau) = C_{\tau-1} + C_\tau$, we have:

$$P(\tau) < \exp\left(\frac{4GN}{\pi}\right)\left[\exp\left(-\frac{\pi}{N}\left(\tau - 1 - \frac{N}{2}\right)^2\right) + \exp\left(-\frac{\pi}{N}\left(\tau - \frac{N}{2}\right)^2\right)\right] \ .$$

To combine these two exponential terms, we define $x = \tau - (N+1)/2$. The expression between the square brackets becomes:

$$\exp\left(-\frac{\pi}{N}\left(x - \frac{1}{2}\right)^2\right) + \exp\left(-\frac{\pi}{N}\left(x + \frac{1}{2}\right)^2\right)$$
$$= 2\exp\left(-\frac{\pi}{N}x^2 - \frac{\pi}{4N}\right)\cosh\left(\frac{\pi x}{N}\right) \ .$$

Using the inequality $\cosh(z) \leq \exp(z^2/2)$ for all $z \in \mathbb{R}$, we obtain the bound $\cosh(\pi x/N) \leq \exp(\pi^2 x^2/(2N^2))$. Absorbing this into the quadratic exponential term yields:

$$P(\tau) < 2\exp\left(\frac{4GN}{\pi} - \frac{\pi}{4N} - \frac{\pi}{N}\left(1 - \frac{\pi}{2N}\right)x^2\right) \ .$$

Replacing x with $\tau - (N+1)/2$, dropping the negative term $-\pi/(4N)$, and substituting $P(\tau)$ back into the initial inequality for $B_2 \cdot B_3$ gives the claimed bound. □

As a consequence of Corollary 3.11, we have the absolute bound $B_2 \cdot B_3 \leq 4N^2 \cdot 3.212^N$ for all t. The trigonometric, Clausen and quadratic bounds are compared and their tightness is experimentally studied in Section 6.1.

4 The Second Construction

In this section, we present the second threshold construction targeting strong simulation security (Definition 2.10).

We first observe that the first construction fails to achieve strong simulation security. For $t = n = 2$ with secret key shares $\mathsf{sk} = \mathsf{sk}_1 + \mathsf{sk}_2$, an adversary without corrupting any user can recover the plaintext of a target ciphertext $\mathsf{ct} = (a, b)$ by querying partial decryptions across related ciphertexts. Specifically, querying ct to user 1 yields $p_1 \approx a \cdot \mathsf{sk}_1$, while querying a second ciphertext $\mathsf{ct}' = (a', b')$ and the homomorphic sum $\mathsf{ct} + \mathsf{ct}'$ to user 2 yields $p_2 \approx a' \cdot \mathsf{sk}_2$ and $p_3 \approx (a + a') \cdot \mathsf{sk}_2$, respectively. Computing:

$$b + p_1 + p_3 - p_2 \approx b + a \cdot (\mathsf{sk}_1 + \mathsf{sk}_2)$$

reveals the underlying plaintext. This attack relies on the linearity of homomorphic addition and the property that the sum of noise flooding terms still permits correct decryption. Strong simulation security inherently precludes such attacks. As formalized in Definition 2.10, any partial decryption query for a ciphertext ct that does not reach the reconstruction threshold ($|\mathsf{P}[\mathsf{ct}]| < t$) is handled by the simulator Sim_1. Because Sim_1 outputs partial decryption shares whose joint distribution is computationally independent of plaintexts and uncorrupted secret key shares, linear combinations of these shares yield computationally uniform values, effectively preventing message recovery. We describe and prove our second construction for BFV, and discuss its adaptation to BGV and CKKS in Section 4.3.

4.1 Construction

Let $(\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Eval}', \mathsf{Dec}')$ be a BFV scheme with ciphertexts $\mathsf{ct} = (a, b) \in R_q^2$ satisfying

$$b + a \cdot \mathsf{sk} = \left\lceil \frac{q}{p} \right\rfloor \cdot \mu + e \bmod q,$$

where $e \in R$ denotes the centered noise representative and $\|e\|_\infty \leq B_{\mathsf{eval}}$.

Throughout the second construction, n is positive, $t \in [n]$, N is a power of two, and $p, q \geq 2$. Fix Shamir interpolation points $\mathcal{I} = \{\alpha_0, \ldots, \alpha_n\} \subset R_q$, where α_0 is the reconstruction point. The second construction also uses two scaling parameters $C_{\mathsf{dec}}, C_{\mathsf{sim}} \in R$, a smudging bound $B_{\mathsf{sm}} \geq 1$, a distribution χ over R, and random oracles $H : \{0,1\}^* \to R_q$ and $H_\chi : \{0,1\}^* \to R$, where H_χ outputs samples distributed as χ. In the strong simulation security experiments, the adversary and all scheme algorithms have access to the same random oracles. In particular, repeated queries to either random oracle on the same input receive the same answer.

The threshold fully homomorphic encryption scheme $\Pi_{\mathsf{StThFHE}} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{PartDec}, \mathsf{FinDec})$ uses the same encryption and evaluation algorithms Enc' and Eval' as the underlying FHE scheme; hence, we focus on the algorithms KeyGen, $\mathsf{PartDec}$, and FinDec, which are given in Figure 4.

$\mathsf{KeyGen}(1^\lambda, 1^n, 1^t)$:

1 $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}'(1^\lambda)$
2 $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n) \leftarrow \mathsf{Share}(\mathsf{sk}; n, t, \mathcal{I})$
3 $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(0; n, t, \mathcal{I})$
4 **return** $((\mathsf{sk}_i, s_i)_{i\in[n]}, \mathsf{pk})$

$\mathsf{FinDec}(\mathsf{ct}, (\mathsf{p}_i)_{i\in\mathcal{S}})$:

1 parse ct as $(a, b) \in R_q^2$
2 $x \leftarrow C_{\mathsf{dec}} \cdot b + \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\to\alpha_0} \cdot \mathsf{p}_i \bmod q$
3 $y \leftarrow \left\lceil x \cdot \frac{p}{q} \right\rfloor \bmod p$
4 **return** $C_{\mathsf{dec}}^{-1} \cdot y \bmod p$

$\mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$:

1 parse ct as $(a, b) \in R_q^2$
2 $e_{\mathsf{fl},i} \leftarrow U(R^{B_{\mathsf{sm}}})$
3 $e_{\mathsf{RLWE},i} \leftarrow H_\chi((\mathsf{sk}_i, s_i), \mathsf{ct})$
4 **return** $\mathsf{p}_i \leftarrow C_{\mathsf{dec}} \cdot (a \cdot \mathsf{sk}_i + H(\mathsf{ct}) \cdot s_i + e_{\mathsf{RLWE},i}) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q$

Fig. 4: The second construction Π_{StThFHE}. Enc and Eval are respectively Enc' and Eval'.

Note that our strong threshold FHE construction also does not require the underlying FHE scheme to satisfy special properties, unlike the generic frameworks of [BGG+18,CKL24,BFM+25]. As in the synchronous setting [CPS26, App. B], our construction admits a context-dependent variant in the spirit of [BBN+25]. In this setting, $\mathsf{PartDec}$ accepts an explicit decryption context dc, ensuring that partial decryptions of the same ciphertext generated under distinct contexts cannot be combined to reconstruct the plaintext. This property is achieved via a minimal modification: appending dc to the input of H within $\mathsf{PartDec}$.

4.2 Analysis

We now state correctness and strong simulation security theorems for Π_{StThFHE}. Note that compactness is inherited from that of the underlying FHE scheme, as we alter neither the encryption nor the evaluation algorithms.

Theorem 4.1. *Let $B_\chi \geq 1$ be a bound on the infinity norm of samples from χ. Assume that the following two conditions hold.*

(C1) Decryption Invertibility. *Parameter $C_{\mathsf{dec}} \in R$ is invertible modulo p.*
(C2) Decryption Correctness. *For any authorized set $\mathcal{S} \in \mathbb{A}_{n,t}$,*

$$\begin{aligned}\|C_{\mathsf{dec}} \bmod q\|_1 \cdot \big(B_{\mathsf{eval}} + p/4\big) + t \cdot B_\chi \cdot \max_{i\in\mathcal{S}} \big\|(C_{\mathsf{dec}} \cdot \lambda_i^{\mathcal{S}\to\alpha_0}) \bmod q\big\|_1 \\ + t \cdot B_{\mathsf{sm}} \cdot \max_{i\in\mathcal{S}} \big\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to\alpha_0}) \bmod q\big\|_1 \\ < q/(2p) \ .\end{aligned}$$

Then Π_{StThFHE} is well-defined and correct.

Proof. Fix an authorized set $\mathcal{S} \in \mathbb{A}_{n,t}$ of size t, a circuit f of arity $\ell \geq 1$ with input plaintexts $\mu_1, \ldots, \mu_\ell$, and write $\hat{\mu} = f(\mu_1, \ldots, \mu_\ell)$ for the target plaintext and $\hat{\mathsf{ct}} = (a, b)$ for the evaluated ciphertext. All computations are carried out in R, identifying elements of R_q and R_p with their centered representatives, of $\|\cdot\|_\infty$ at most $q/2$ and $p/2$ respectively. Accordingly, $q \bmod p$ denotes the unique integer in $(-p/2, p/2]$ congruent to q modulo p, so that $p\lceil q/p \rfloor = q - (q \bmod p)$. We write $\lambda_i := \lambda_i^{\mathcal{S} \to \alpha_0}$ throughout.

Since Π_{StThFHE} leaves the encryption and evaluation algorithms unchanged, BFV correctness yields $b + a \cdot \mathsf{sk} = \left\lceil \frac{q}{p} \right\rfloor \cdot \hat{\mu} + \hat{e} \bmod q$ for some $\hat{e} \in R$ with $\|\hat{e}\|_\infty \leq B_{\mathsf{eval}}$, where the noise bound holds with overwhelming probability over the random coins of Enc' and Eval'. By construction of $\mathsf{PartDec}$,

$$\mathsf{p}_i \;=\; C_{\mathsf{dec}} \cdot \left(a \cdot \mathsf{sk}_i + H(\hat{\mathsf{ct}}) \cdot s_i + e_{\mathsf{RLWE},i}\right) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q,$$

with $\|e_{\mathsf{RLWE},i}\|_\infty \leq B_\chi$ and, by definition of $U(R^{B_{\mathsf{sm}}})$, $\|e_{\mathsf{fl},i}\|_\infty \leq B_{\mathsf{sm}}$ with probability 1. The Shamir reconstruction identities at $\alpha_0 = 0$ give $\sum_i \lambda_i \cdot \mathsf{sk}_i = \mathsf{sk}$ and $\sum_i \lambda_i \cdot s_i = 0$, so substituting the BFV equation into the partial-decryption combination yields

$$\begin{aligned} x \;&=\; C_{\mathsf{dec}} \cdot b + \sum_{i \in \mathcal{S}} \lambda_i \cdot \mathsf{p}_i \\ &\equiv\; \left\lceil \frac{q}{p} \right\rfloor \cdot C_{\mathsf{dec}} \cdot \hat{\mu} + C_{\mathsf{dec}} \cdot \hat{e} + C_{\mathsf{dec}} \sum_{i \in \mathcal{S}} \lambda_i e_{\mathsf{RLWE},i} + C_{\mathsf{sim}} \sum_{i \in \mathcal{S}} \lambda_i e_{\mathsf{fl},i} \pmod q. \end{aligned} \tag{2}$$

To analyze the rounding step $y = \lceil x \cdot p/q \rfloor \bmod p$, we lift (2) to R without reducing modulo q and use the identity $p \cdot \lceil q/p \rfloor / q = 1 - (q \bmod p)/q$ to write $x \cdot p/q$ in $\mathbb{Q} \otimes R$ as $x \cdot p/q = C_{\mathsf{dec}} \cdot \hat{\mu} + F/q$, where

$$\begin{aligned} F \;:=\; &- (q \bmod p) \cdot C_{\mathsf{dec}} \cdot \hat{\mu} + p \cdot C_{\mathsf{dec}} \cdot \hat{e} \\ &+ p \cdot C_{\mathsf{dec}} \cdot \sum_{i \in \mathcal{S}} \lambda_i \cdot e_{\mathsf{RLWE},i} + p \cdot C_{\mathsf{sim}} \cdot \sum_{i \in \mathcal{S}} \lambda_i \cdot e_{\mathsf{fl},i}. \end{aligned} \tag{3}$$

Since $C_{\mathsf{dec}} \cdot \hat{\mu}$ has integer coefficients, coordinate-wise rounding gives $\lceil x \cdot p/q \rfloor = C_{\mathsf{dec}} \cdot \hat{\mu} + \lceil F/q \rfloor$. Whenever $\|F\|_\infty < q/2$, each coefficient of F/q lies in $(-1/2, 1/2)$, so $\lceil F/q \rfloor = 0$ and $y = C_{\mathsf{dec}} \cdot \hat{\mu} \bmod p$. It therefore suffices to bound $\|F\|_\infty$.

We rely on the polynomial product bound $\|f \cdot g\|_\infty \leq \|f\|_1 \cdot \|g\|_\infty$ for $f, g \in R$ together with the triangle inequality.

The two scalar terms of F admit a direct bound. Using $|q \bmod p| \leq p/2$, $\|\hat{\mu}\|_\infty \leq p/2$, and $\|C_{\mathsf{dec}} \bmod q\|_\infty \leq q/2$, the product bound gives $\|C_{\mathsf{dec}} \cdot \hat{\mu}\|_\infty \leq \|C_{\mathsf{dec}} \bmod q\|_1 \cdot p/2$, and hence

$$\begin{aligned} \left\|(q \bmod p) \cdot C_{\mathsf{dec}} \cdot \hat{\mu}\right\|_\infty &\leq \|C_{\mathsf{dec}} \bmod q\|_1 \cdot p^2/4 \;, \\ \left\|p \cdot C_{\mathsf{dec}} \cdot \hat{e}\right\|_\infty &\leq p \cdot \|C_{\mathsf{dec}} \bmod q\|_1 \cdot B_{\mathsf{eval}} \;. \end{aligned}$$

For the two summation terms, the triangle inequality combined with the product bound and with the uniform noise bounds $\|e_{\mathsf{RLWE},i}\|_\infty \le B_\chi$, $\|e_{\mathsf{fl},i}\|_\infty \le B_{\mathsf{sm}}$ for $i \in \mathcal{S}$ yields

$$\left\|p \cdot C_{\mathsf{dec}} \cdot \sum_{i\in\mathcal{S}} \lambda_i \cdot e_{\mathsf{RLWE},i}\right\|_\infty \le p \cdot t \cdot B_\chi \cdot \max_{i\in\mathcal{S}} \|(C_{\mathsf{dec}} \cdot \lambda_i) \bmod q\|_1 \ ,$$

$$\left\|p \cdot C_{\mathsf{sim}} \cdot \sum_{i\in\mathcal{S}} \lambda_i \cdot e_{\mathsf{fl},i}\right\|_\infty \le p \cdot t \cdot B_{\mathsf{sm}} \cdot \max_{i\in\mathcal{S}} \|(C_{\mathsf{sim}} \cdot \lambda_i) \bmod q\|_1 \ .$$

Summing these four bounds and factoring out p,

$$\begin{aligned}\|F\|_\infty \ \le \ p \cdot \Big[& \|C_{\mathsf{dec}} \bmod q\|_1 \cdot (B_{\mathsf{eval}} + p/4) \\ & + t \cdot B_\chi \cdot \max_{i\in\mathcal{S}} \|(C_{\mathsf{dec}} \cdot \lambda_i) \bmod q\|_1 \\ & + t \cdot B_{\mathsf{sm}} \cdot \max_{i\in\mathcal{S}} \|(C_{\mathsf{sim}} \cdot \lambda_i) \bmod q\|_1 \Big].\end{aligned}$$

By Condition **(C2)** the bracket is strictly less than $q/(2p)$, hence $\|F\|_\infty < q/2$ and $y = C_{\mathsf{dec}} \cdot \hat{\mu} \bmod p$. Condition **(C1)** then gives $C_{\mathsf{dec}}^{-1} \in R_p$, so FinDec outputs $C_{\mathsf{dec}}^{-1} \cdot y \bmod p = \hat{\mu}$. The only step relying on a probabilistic event is the BFV noise bound $\|\hat{e}\|_\infty \le B_{\mathsf{eval}}$; all other bounds hold with probability 1. Correctness of Π_{StThFHE} therefore holds with overwhelming probability over the randomness of Enc' and Eval'. □

The rest of this section proves that Π_{StThFHE} satisfies strong simulation security according to Definition 2.10.

Theorem 4.2. *Let $B_\chi \ge 1$ be a bound on the infinity norm of samples from χ. Assume that the underlying FHE scheme is* IND-CPA*-secure, that the* $\mathrm{RLWE}_{q,\chi}$ *hardness assumption holds, and that the following two conditions are satisfied.*

(C3) Simulation Invertibility. *Parameter $C_{\mathsf{sim}} \in R$ is invertible modulo q.*

(C4) Simulation Flooding. *For any maximal unauthorized set $T \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, letting $\mathcal{S}^* := \{0\} \cup T$, for any $i \in [n] \setminus T$ and any $\ell \in \mathcal{S}^*$, we have:*

$$(B_{\mathsf{eval}} + B_\chi) \cdot 2^\lambda \cdot t \cdot N \cdot \left(\left\| \frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \bmod q \right\|_1 + \left\| \frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_\ell^{\mathcal{S}^*\to\alpha_i} \bmod q \right\|_1 \right) \le B_{\mathsf{sm}} \ .$$

Then Π_{StThFHE} is strongly simulation-secure in the random-oracle model.

The proof of Theorem 4.2 follows a similar strategy to that from [CPS26, Theorem 5.1].

Remark 1. The deterministic term $e_{\mathsf{RLWE},i}$ can be omitted in implementation. Indeed, Condition **(C4)** implies $\Delta(C_{\mathsf{dec}} e_{\mathsf{RLWE},i} + C_{\mathsf{sim}} e_{\mathsf{fl},i},\, C_{\mathsf{sim}} e_{\mathsf{fl},i}) \le 2^{-\Omega(\lambda)}$. Therefore, the variant without $e_{\mathsf{RLWE},i}$ is covered by first adding $C_{\mathsf{dec}} \cdot e_{\mathsf{RLWE},i}$ through this flooding argument and then applying Theorem 4.2. We keep $e_{\mathsf{RLWE},i}$ in the main construction only to make the proof explicit.

Proof. Let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ denote a PPT adversary. On input pk, algorithm $\mathcal{A}_0$ returns an unauthorized set of users $\mathcal{S}_{\mathsf{cor}}$ to corrupt, with $|\mathcal{S}_{\mathsf{cor}}| < t$.

We recall that a partial decryption share p_i of a ciphertext $\mathsf{ct}_j = (a_j, b_j)$ has the form:

$$\mathsf{p}_i = C_{\mathsf{dec}} \cdot (a_j \cdot \mathsf{sk}_i + H(\mathsf{ct}_j) \cdot s_i + e_{\mathsf{RLWE},i}) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \ .$$

We define $\mathsf{p}_i^{\mathrm{det}}$ as the deterministic part of this partial decryption share, i.e.:

$$\mathsf{p}_i^{\mathrm{det}} := C_{\mathsf{dec}} \cdot (a_j \cdot \mathsf{sk}_i + H(\mathsf{ct}_j) \cdot s_i + e_{\mathsf{RLWE},i}) \ ,$$

where $e_{\mathsf{RLWE},i} \leftarrow H_\chi((\mathsf{sk}_i, s_i), \mathsf{ct})$. Further note that $\mathsf{p}_i^{\mathrm{det}}$ can be computed by the adversary if it has corrupted party P_i since it then knows (sk_i, s_i). For a fixed pair (ct, i), this deterministic component is fixed because the random-oracle answers are consistent. By contrast, every invocation of $\mathsf{PartDec}$ samples a fresh $e_{\mathsf{fl},i}$. Thus repeated partial-decryption queries for the same (ct, i) return the same deterministic component masked by independently sampled smudging noise. Algorithm Sim_1 reuses the $\mathsf{p}_i^{\mathrm{det}}$ stored for (ct, i), whereas Sim_2 reuses T_{ct} and the deterministic components indexed by T_{ct}; both algorithms sample a fresh $e_{\mathsf{fl},i}$ on every invocation.

We specify the simulator $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1, \mathsf{Sim}_2)$ required by Definition 2.10; its three components are given in Figure 5.

We next make explicit when each simulator is used and where the sharing of zero enters the proof. Fix a ciphertext ct. The set $\mathsf{P}[\mathsf{ct}]$ is initialized to $\mathcal{S}_{\mathsf{cor}}$, and the queried index is added before its cardinality is compared with t. It follows that Sim_1 handles at most $t - 1 - |\mathcal{S}_{\mathsf{cor}}|$ distinct non-corrupted parties for ct. Queries to corrupted parties are answered by running $\mathsf{PartDec}$ with their known shares, and repeated queries do not increase this number because $\mathsf{P}[\mathsf{ct}]$ is a set.

Let $g \in R_q[Y]$ be the Shamir polynomial of degree $t-1$ with $g(\alpha_0) = 0$ and $s_i = g(\alpha_i)$. Conditioned on $(s_i)_{i \in \mathcal{S}_{\mathsf{cor}}}$, this polynomial has $t - 1 - |\mathcal{S}_{\mathsf{cor}}|$ uniformly random degrees of freedom. Hence, for any set $J \subseteq [n] \setminus \mathcal{S}_{\mathsf{cor}}$ with $|J| \leq t - 1 - |\mathcal{S}_{\mathsf{cor}}|$, $(s_i)_{i \in J}$ is uniform over $R_q^{|J|}$ conditioned on the corrupted shares.

In particular, if $|\mathcal{S}_{\mathsf{cor}}| = t-1$, then Sim_1 never handles a non-corrupted query: the first such query makes $|\mathsf{P}[\mathsf{ct}]| = t$ and is answered by Sim_2. If $|\mathcal{S}_{\mathsf{cor}}| = t-2$, the first query to a distinct non-corrupted party is answered by Sim_1, while the next such query is answered by Sim_2. If $|\mathcal{S}_{\mathsf{cor}}| \leq t-3$, then Sim_1 can handle up to $t-1-|\mathcal{S}_{\mathsf{cor}}|$ distinct non-corrupted parties before the next distinct non-corrupted query is answered by Sim_2. Thus the term $H(\mathsf{ct}) \cdot s_i$ is used as a RLWE mask for the pre-threshold replies precisely when $|\mathcal{S}_{\mathsf{cor}}| \leq t-2$; it is not needed for a non-corrupted Sim_1 reply when $|\mathcal{S}_{\mathsf{cor}}| = t-1$, because no such reply occurs.

On the first query for which $|\mathsf{P}[\mathsf{ct}]| = t$, the current index i is a new non-corrupted index and $T_{\mathsf{ct}} := \mathsf{P}[\mathsf{ct}] \setminus \{i\}$ has cardinality exactly $t-1$. This set consists of $\mathcal{S}_{\mathsf{cor}}$ and the distinct non-corrupted indices previously handled by Sim_1, and it is then fixed for all later queries on ct. Algorithm Sim_2 computes the deterministic components indexed by $T_{\mathsf{ct}} \cap \mathcal{S}_{\mathsf{cor}}$ from the corrupted shares and retrieves those indexed by $T_{\mathsf{ct}} \setminus \mathcal{S}_{\mathsf{cor}}$ from st. It then uses the plaintext associated

with ct and interpolation on $\{0\} \cup T_{\mathsf{ct}}$ to produce a consistent partial decryption share.

$\mathsf{Sim}_0(\mathsf{pk}, \mathcal{S}_{\mathsf{cor}})$:

1 $(\mathsf{sk}_1, \ldots, \mathsf{sk}_n) \leftarrow \mathsf{Share}(0; n, t, \mathcal{I})$
2 $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(0; n, t, \mathcal{I})$
3 $\mathsf{st} \leftarrow \{(\mathsf{pk}, (\mathsf{sk}_i, s_i)_{i \in \mathcal{S}_{\mathsf{cor}}})\}$
4 **return** $(\mathsf{st}, (\mathsf{sk}_i, s_i)_{i \in \mathcal{S}_{\mathsf{cor}}})$

$\mathsf{Sim}_1(\mathsf{st}, \mathsf{ct}, i)$:

1 Find $(\mathsf{pk}, (\mathsf{sk}_i, s_i)_{i \in \mathcal{S}_{\mathsf{cor}}})$ in st
2 **if** $i \in \mathcal{S}_{\mathsf{cor}}$ **then**
3 **return** $\mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$
4 **if** $\nexists \mathsf{p}_i^{\det} : (\mathsf{ct}, i, \mathsf{p}_i^{\det}) \in \mathsf{st}$ **then**
5 $\mathsf{p}_i^{\det} \leftarrow U(C_{\mathsf{dec}} \cdot R_q)$
6 $\mathsf{st} \leftarrow \mathsf{st} \cup \{(\mathsf{ct}, i, \mathsf{p}_i^{\det})\}$
7 **else**
8 Retrieve $\mathsf{p}_i^{\det}$ from st
9 $e_{\mathsf{fl},i} \leftarrow U(R^{B_{\mathsf{sm}}})$
10 $\mathsf{p}_i \leftarrow \mathsf{p}_i^{\det} + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}$
11 **return** $(\mathsf{st}, \mathsf{p}_i)$

$\mathsf{Sim}_2(\mathsf{st}, \mathsf{ct}, i, \mu)$:

1 Find $(\mathsf{pk}, (\mathsf{sk}_\ell, s_\ell)_{\ell \in \mathcal{S}_{\mathsf{cor}}})$ in st
2 **if** $i \in \mathcal{S}_{\mathsf{cor}}$ **then**
3 **return** $\mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$
4 Parse ct as (a, b)
5 Retrieve T_{ct} from st and set $\mathcal{S}^* \leftarrow \{0\} \cup T_{\mathsf{ct}}$
6 **for** $\ell \in T_{\mathsf{ct}} \cap \mathcal{S}_{\mathsf{cor}}$ **do**
7 $e_{\mathsf{RLWE},\ell} \leftarrow H_\chi((\mathsf{sk}_\ell, s_\ell), \mathsf{ct})$
8 $\mathsf{p}_\ell^{\det} \leftarrow C_{\mathsf{dec}} \cdot (a \cdot \mathsf{sk}_\ell + H(\mathsf{ct}) \cdot s_\ell + e_{\mathsf{RLWE},\ell}) \bmod q$
9 **for** $\ell \in T_{\mathsf{ct}} \setminus \mathcal{S}_{\mathsf{cor}}$ **do**
10 Retrieve $\mathsf{p}_\ell^{\det}$ such that $(\mathsf{ct}, \ell, \mathsf{p}_\ell^{\det}) \in \mathsf{st}$
11 $e_{\mathsf{fl},i} \leftarrow U(R^{B_{\mathsf{sm}}})$
12 $\mathsf{p}_i \leftarrow C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \left(\left\lceil \frac{q}{p} \right\rfloor \mu - b \right) + \sum_{\ell \in T_{\mathsf{ct}}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{p}_\ell^{\det} + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}$
13 **return** $(\mathsf{st}, \mathsf{p}_i)$

Fig. 5: The Simulator $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1, \mathsf{Sim}_2)$.

We now show that $\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)$ and $\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Ideal}}(1^\lambda, 1^n, 1^t)$ are computationally indistinguishable via a sequence of hybrid experiments. Each hybrid tweaks the decryption oracle, and we describe the decryption oracles of these hybrids in Figure 6. In all hybrid experiments, we assume st is initialized at setup with the public key pk as well as the set of all corrupted partial decryption keys $(\mathsf{sk}_i, s_i)_{i \in \mathcal{S}_{\mathsf{cor}}}$ after $\mathcal{A}_0$ returns its set of corrupted users $\mathcal{S}_{\mathsf{cor}}$.

Hybrid H_0. This is the real experiment $\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Real}}(1^\lambda, 1^n, 1^t)$.

Hybrid H_1. In this experiment, we only make a syntactical change to distinguish decryption queries on a ciphertext ct that allow the attacker to recover the

$\mathsf{ODec}_0(j, i)$:

1 **if** $j \notin [\mathsf{ctr}] \vee i \notin [n]$ **then**
2 **return** $\perp$
3 $(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
4 $\mathsf{p}_i \leftarrow \mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$
5 **return** p_i

$\mathsf{ODec}_1(j, i)$:

1 **if** $j \notin [\mathsf{ctr}] \vee i \notin [n]$ **then**
2 **return** $\perp$
3 $(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
4 **if** $\mathsf{P}[\mathsf{ct}]$ *is undefined* **then**
5 $\mathsf{P}[\mathsf{ct}] \leftarrow \mathcal{S}_{\mathsf{cor}}$
6 $\mathsf{P}[\mathsf{ct}] \leftarrow \mathsf{P}[\mathsf{ct}] \cup \{i\}$
7 **if** $|\mathsf{P}[\mathsf{ct}]| \geq t$ **then**
8 $\mathsf{p}_i \leftarrow \mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$
9 **else**
10 $\mathsf{p}_i \leftarrow \mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$
11 **return** p_i

$\mathsf{ODec}_2(j, i)$:

1 **if** $j \notin [\mathsf{ctr}] \vee i \notin [n]$ **then**
2 **return** $\perp$
3 $(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
4 **if** $\mathsf{P}[\mathsf{ct}]$ *is undefined* **then**
5 $\mathsf{P}[\mathsf{ct}] \leftarrow \mathcal{S}_{\mathsf{cor}}$
6 $\mathsf{P}[\mathsf{ct}] \leftarrow \mathsf{P}[\mathsf{ct}] \cup \{i\}$
7 **if** $|\mathsf{P}[\mathsf{ct}]| \geq t$ **then**
8 **if** T_{ct} *is undefined* **then**
9 $T_{\mathsf{ct}} \leftarrow \mathsf{P}[\mathsf{ct}] \setminus \{i\}$;
  $\mathsf{st} \leftarrow \mathsf{st} \cup \{(\mathsf{ct}, T_{\mathsf{ct}})\}$
10 $(\mathsf{st}, \mathsf{p}_i) \leftarrow \mathsf{Sim}_2(\mathsf{st}, \mathsf{ct}, i, \mu)$
11 **else**
12 $e_{\mathsf{RLWE},i} \leftarrow H_\chi((\mathsf{sk}_i, s_i), \mathsf{ct})$
13 $\mathsf{p}_i^{\mathrm{det}} \leftarrow C_{\mathsf{dec}} \cdot (a \cdot \mathsf{sk}_i + H(\mathsf{ct}) \cdot s_i + e_{\mathsf{RLWE},i}) \bmod q$
14 $\mathsf{st} \leftarrow \mathsf{st} \cup \{(\mathsf{ct}, i, \mathsf{p}_i^{\mathrm{det}})\}$
15 $\mathsf{p}_i \leftarrow \mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct})$
16 **return** p_i

$\mathsf{ODec}_3(j, i)$:

1 **if** $j \notin [\mathsf{ctr}] \vee i \notin [n]$ **then**
2 **return** $\perp$
3 $(\mu, \mathsf{ct}) \leftarrow \mathsf{L}[j]$
4 **if** $\mathsf{P}[\mathsf{ct}]$ *is undefined* **then**
5 $\mathsf{P}[\mathsf{ct}] \leftarrow \mathcal{S}_{\mathsf{cor}}$
6 $\mathsf{P}[\mathsf{ct}] \leftarrow \mathsf{P}[\mathsf{ct}] \cup \{i\}$
7 **if** $|\mathsf{P}[\mathsf{ct}]| \geq t$ **then**
8 **if** T_{ct} *is undefined* **then**
9 $T_{\mathsf{ct}} \leftarrow \mathsf{P}[\mathsf{ct}] \setminus \{i\}$;
  $\mathsf{st} \leftarrow \mathsf{st} \cup \{(\mathsf{ct}, T_{\mathsf{ct}})\}$
10 $(\mathsf{st}, \mathsf{p}_i) \leftarrow \mathsf{Sim}_2(\mathsf{st}, \mathsf{ct}, i, \mu)$
11 **else**
12 $(\mathsf{st}, \mathsf{p}_i) \leftarrow \mathsf{Sim}_1(\mathsf{st}, \mathsf{ct}, i)$
13 **return** p_i

Fig. 6: Partial decryption oracles for the hybrid experiments.

underlying plaintext (i.e., $|\mathsf{P}[\mathsf{ct}]| \geq t$) from decryption queries that do not enable it (yet). This is done by replacing the decryption oracle ODec_0 by ODec_1 (see Figure 6). This change does not affect the view of the adversary, hence games H_0 and H_1 are identically distributed.

Hybrid H_2. In this experiment, we change how a partial decryption query on a ciphertext ct is answered when $|\mathsf{P}[\mathsf{ct}]| \geq t$. We now rely on the ODec_2 algorithm

described in Figure 6, which replies to such queries using Sim_2 described in Figure 5. In addition, ODec_2 updates the state st when decryption queries are made for a ciphertext ct such that $|\mathsf{P}[\mathsf{ct}]| < t$. The latter change is only syntactical.

Let us now analyze the change resulting from relying on Sim_2. Consider a partial decryption query (j, i), where the index j determines a previously generated ciphertext $\mathsf{ct}_j = (a_j, b_j)$.

In Hybrid H_1, the challenger returns $\mathsf{p}_i^{(j)} := \mathsf{PartDec}((\mathsf{sk}_i, s_i), \mathsf{ct}_j)$, which is defined as (modulo q):

$$\begin{aligned}\mathsf{p}_i^{(j)} &= C_{\mathsf{dec}} \cdot \left(a_j \cdot \mathsf{sk}_i + H(\mathsf{ct}_j) \cdot s_i + e_{\mathsf{RLWE},i}^{(j)}\right) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} \\ &= \mathsf{p}_i^{\mathrm{det},(j)} + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} \ ,\end{aligned}$$

with $e_{\mathsf{fl},i}^{(j)} \leftarrow U(R^{B_{\mathsf{sm}}})$ and $e_{\mathsf{RLWE},i}^{(j)} \leftarrow H_\chi((\mathsf{sk}_i, s_i), \mathsf{ct}_j)$.

In Hybrid H_2, when $|\mathsf{P}[\mathsf{ct}_j]| \geq t$ (and $i \notin \mathcal{S}_{\mathsf{cor}}$), the challenger outputs a partial decryption share which is defined differently by Sim_2. Let $T_{\mathsf{ct}_j} \subseteq [n]$ denote the set fixed on the first query for which $|\mathsf{P}[\mathsf{ct}_j]| = t$, and let $\mathcal{S}^* := \{0\} \cup T_{\mathsf{ct}_j}$. By construction, $T_{\mathsf{ct}_j} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ and $|\mathcal{S}^*| = t$. The simulator returns (see Step 12 of Figure 5):

$$\mathsf{p}_i^{(j)} \leftarrow C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \left(\left\lceil \frac{q}{p} \right\rfloor \mu_j - b_j\right) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} + \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{p}_\ell^{\mathrm{det}} \ .$$

Now, recall that $\mathsf{ct}_j = (a_j, b_j)$ satisfies:

$$a_j \cdot \mathsf{sk} + b_j = \left\lceil \frac{q}{p} \right\rfloor \cdot \mu_j + e_j \bmod q \ ,$$

for some error $e_j \in R_q$ with $\|e_j\|_\infty \leq B_{\mathsf{eval}}$. Then, defining $\mathsf{sk}_0 = \mathsf{sk}$, we have:

$$\begin{aligned}\mathsf{p}_i^{(j)} &= C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \left(\left\lceil \frac{q}{p} \right\rfloor \mu_j - b_j\right) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} + \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{p}_\ell^{\mathrm{det}} \\ &= C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot (a_j \cdot \mathsf{sk} - e_j) + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} + \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{p}_\ell^{\mathrm{det}} \\ &= C_{\mathsf{dec}} \cdot a_j \cdot \sum_{\ell \in \mathcal{S}^*} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \mathsf{sk}_\ell - C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot e_j + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} \\ &\qquad + C_{\mathsf{dec}} \cdot \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot \left(H(\mathsf{ct}_j) \cdot s_\ell + e_{\mathsf{RLWE},\ell}^{(j)}\right) \\ &= C_{\mathsf{dec}} \cdot a_j \cdot \mathsf{sk}_i + C_{\mathsf{dec}} \cdot H(\mathsf{ct}_j) \cdot s_i + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} \\ &\qquad + C_{\mathsf{dec}} \cdot \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot e_{\mathsf{RLWE},\ell}^{(j)} - C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot e_j \ ,\end{aligned}$$

where the last equality results from the fact that the s_ℓ's are shares of 0, i.e., with $s_0 = 0$, we have $s_i = \sum_{\ell \in \mathcal{S}^*} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot s_\ell = \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot s_\ell$. This gives

$$\begin{aligned} \mathsf{p}_i^{(j)} = \mathsf{p}_i^{\mathrm{det},(j)} &+ C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i}^{(j)} - C_{\mathsf{dec}} \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot e_j - C_{\mathsf{dec}} \cdot e_{\mathsf{RLWE},i}^{(j)} \\ &+ C_{\mathsf{dec}} \cdot \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot e_{\mathsf{RLWE},\ell}^{(j)} \ . \end{aligned}$$

Notice that the challenger no longer relies on knowledge of sk_i to compute $\mathsf{p}_i^{(j)}$, but only on the ciphertext ct_j, the underlying plaintext μ_j, and the (deterministic) partial decryption shares $(\mathsf{p}_\ell^{\mathrm{det}})_{\ell \in \mathcal{S}^* \setminus \{0\}}$ of ct_j fixed by prior partial decryption queries. Lemma 4.3 below shows that H_2 is statistically indistinguishable from H_1.

Lemma 4.3. *Assuming Conditions* **(C3)** *and* **(C4)** *hold, Hybrids* H_1 *and* H_2 *are statistically indistinguishable.*

Proof. For $i \in \mathcal{S}_{\mathsf{cor}}$, both hybrids call $\mathsf{PartDec}$ with the corrupted share. Now let $i \notin \mathcal{S}_{\mathsf{cor}}$. If $i \in T_{\mathsf{ct}_j}$, evaluation of the Lagrange basis at its interpolation point gives

$$\lambda_i^{\mathcal{S}^* \to \alpha_i} = 1 \quad \text{and} \quad \lambda_\ell^{\mathcal{S}^* \to \alpha_i} = 0 \quad \text{for all } \ell \in \mathcal{S}^* \setminus \{i\}.$$

Therefore Sim_2 returns the stored $\mathsf{p}_i^{\mathrm{det},(j)}$ plus fresh smudging noise, exactly as in H_1. It remains to consider $i \in [n] \setminus T_{\mathsf{ct}_j}$, which is precisely the range of i covered by Condition **(C4)**.

The difference between the two experiments is that, in H_1, we have:

$$\mathsf{p}_i^{(j)} = \mathsf{p}_i^{\mathrm{det},(j)} + C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \bmod q \ ,$$

while in H_2, it is set to:

$$\begin{aligned} \mathsf{p}_i^{(j)} = \mathsf{p}_i^{\mathrm{det},(j)} &+ C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \\ &+ C_{\mathsf{dec}} \cdot \Big(\sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot e_{\mathsf{RLWE},\ell}^{(j)} - e_{\mathsf{RLWE},i}^{(j)} - \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot e_j \Big) \bmod q \ . \end{aligned}$$

Since $\mathsf{p}_i^{\mathrm{det},(j)}$ is identically distributed in both experiments, it suffices to bound:

$$\begin{aligned} \Delta\Big(& C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} \ , \\ & C_{\mathsf{sim}} \cdot e_{\mathsf{fl},i} + C_{\mathsf{dec}} \cdot \Big(\sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \cdot e_{\mathsf{RLWE},\ell}^{(j)} - e_{\mathsf{RLWE},i}^{(j)} - \lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot e_j \Big) \Big) \ , \end{aligned}$$

over the randomness of $e_{\mathsf{fl},i}$, where both sides are computed modulo q. As C_{sim} is invertible modulo q (by Condition **(C3)**), and by the probability preservation property, it suffices to bound

$$\begin{aligned} \Delta\Big(& e_{\mathsf{fl},i} \ , e_{\mathsf{fl},i} + \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \lambda_\ell^{\mathcal{S}^* \to \alpha_i} \bmod q \right) \cdot e_{\mathsf{RLWE},\ell}^{(j)} \\ & - \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \bmod q \right) \cdot e_{\mathsf{RLWE},i}^{(j)} - \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \lambda_0^{\mathcal{S}^* \to \alpha_i} \bmod q \right) \cdot e_j \Big) \ . \end{aligned}$$

Lemma 2.4 ensures that the above quantity is at most $2^{-\lambda}$ as soon as we have:

$$B_{\mathsf{sm}} \geq N{\cdot}2^{\lambda} \cdot \left(\left\| \sum_{\ell \in \mathcal{S}^* \setminus \{0\}} \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \lambda_{\ell}^{\mathcal{S}^* \to \alpha_i} \bmod q \right) \cdot e^{(j)}_{\mathsf{RLWE},\ell} \right\|_{\infty} \right.$$
$$\left. + \left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \bmod q \right) \cdot e^{(j)}_{\mathsf{RLWE},i} \right\|_{\infty} + \left\| \left(\lambda_0^{\mathcal{S}^* \to \alpha_i} \cdot \frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \bmod q \right) \cdot e_j \right\|_{\infty} \right) \ ,$$

which is implied by Condition **(C4)**. □

Hybrid H_3. In this experiment, we change how a partial decryption query on a ciphertext ct is answered when $|\mathsf{P}[\mathsf{ct}]| < t$. We now rely on the ODec_3 algorithm described in Figure 6, which replies to such queries using Sim_1 described in Figure 5.

Let us analyze the change resulting from replacing ODec_2 with ODec_3. The difference only concerns queries to non-corrupted parties, i.e., for $i \notin \mathcal{S}_{\mathsf{cor}}$, and the subsequent reuse of their deterministic shares by Sim_2. In that case, in Hybrid H_2, the challenger returns $\mathsf{p}_i^{(j)} = \mathsf{p}_i^{\mathrm{det},(j)} + C_{\mathsf{sim}} \cdot e^{(j)}_{\mathsf{fl},i}$ with

$$\mathsf{p}_i^{\mathrm{det},(j)} = C_{\mathsf{dec}} \cdot \left(a_j \cdot \mathsf{sk}_i + H(\mathsf{ct}_j) \cdot s_i + e^{(j)}_{\mathsf{RLWE},i} \right) \bmod q \ ,$$

where $e^{(j)}_{\mathsf{RLWE},i} \leftarrow H_{\chi}((\mathsf{sk}_i, s_i), \mathsf{ct}_j)$. Hybrid H_3 instead returns $\mathsf{p}_i^{(j)} = \mathsf{p}_i^{\mathrm{det},(j)} + C_{\mathsf{sim}} \cdot e^{(j)}_{\mathsf{fl},i}$ with $\mathsf{p}_i^{\mathrm{det},(j)}$ sampled uniformly in $C_{\mathsf{dec}} \cdot R_q$.

Fix a ciphertext ct_j, and consider the distinct non-corrupted indices for which the reply on ct_j is produced by Sim_1. As shown above, there are at most $t - 1 - |\mathcal{S}_{\mathsf{cor}}|$ such indices, and their zero shares are jointly uniform conditioned on the corrupted zero shares. For each such index, the pair

$$\left(H(\mathsf{ct}_j),\ H(\mathsf{ct}_j) \cdot s_i + e^{(j)}_{\mathsf{RLWE},i} \right)$$

has the form of a RLWE sample: $H(\mathsf{ct}_j)$ is uniform in R_q, and $e^{(j)}_{\mathsf{RLWE},i}$ has distribution χ. The $\mathrm{RLWE}_{q,\chi}$ assumption and a hybrid argument over the polynomially many first queries to such pairs therefore allow these values to be replaced by uniform elements of R_q. Repeated queries to the same (ct_j, i) do not add another RLWE sample, because both the real oracle and Sim_1 reuse the same deterministic component and only resample the smudging noise. When $|\mathcal{S}_{\mathsf{cor}}| = t - 1$, there are no such non-corrupted Sim_1 queries, so this change is vacuous.

Multiplying by C_{dec} and adding the fixed term $C_{\mathsf{dec}} \cdot a_j \cdot \mathsf{sk}_i$ shows that the deterministic components replaced in this hybrid are computationally indistinguishable from uniform elements of $C_{\mathsf{dec}} \cdot R_q$. This argument uses the conditional joint distribution of at most $t - 1 - |\mathcal{S}_{\mathsf{cor}}|$ zero shares associated with any fixed ciphertext; it does not assume that all non-corrupted zero shares are independent across all parties and ciphertexts. Consequently, when Sim_2 later utilizes these simulated values from st, the resulting partial decryptions form a consistent transcript that correctly reconstructs the plaintext μ under FinDec.

Hybrid H_4. This experiment is as H_3, except that the corrupted partial-decryption keys are generated by

$$(\mathsf{st}, (\mathsf{sk}'_\ell, s'_\ell)_{\ell \in \mathcal{S}_{\mathsf{cor}}}) \leftarrow \mathsf{Sim}_0(\mathsf{pk}, \mathcal{S}_{\mathsf{cor}}),$$

and $(\mathsf{sk}'_\ell, s'_\ell)_{\ell \in \mathcal{S}_{\mathsf{cor}}}$ is given to the adversary. By the privacy of Shamir secret sharing, H_4 is statistically indistinguishable from H_3.

Finally, H_4 is identical to $\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Ideal}}(1^\lambda, 1^n, 1^t)$. Indeed, the adversary receives exactly the corrupted partial-decryption keys output by Sim_0; the encryption and evaluation oracles are the same as in the ideal experiment; and the partial-decryption oracle ODec_3 performs the same state updates and calls to Sim_1 and Sim_2 as the ideal partial-decryption oracle. Hence $\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Real}}$ and $\mathsf{Exp}^{\mathsf{StSim}}_{\mathsf{Ideal}}$ are computationally indistinguishable. □

4.3 Extensions to BGV and CKKS

The BGV and CKKS adaptations of Section 3.3 extend directly to the second construction. For BGV, the ciphertext is first converted to BFV form as in Section 3.3, after which the masking terms in $\mathsf{PartDec}$ are applied unchanged.

For CKKS, the modifications to FinDec and Condition **(C1)** are identical to those of Section 3.3. Condition **(C2)** additionally contains the term $tB_\chi \max_{i \in \mathcal{S}} \|(C_{\mathsf{dec}} \lambda_i^{\mathcal{S} \to \alpha_0}) \bmod q\|_1$, corresponding to the errors sampled from χ. Conditions **(C3)** and **(C4)** remain unchanged; in Sim_2, the term $\lceil q/p \rceil \mu - b$ is replaced by $\Delta\mu - b$.

4.4 Bounding the Ciphertext Modulus

In this subsection, we derive a lower bound on the ciphertext modulus q for Π_{StThFHE}, governed by Condition **(C2)** of Theorem 4.1 and Condition **(C4)** of Theorem 4.2.

Given an interpolation set $\mathcal{I} = \{\alpha_0, \alpha_1, \ldots, \alpha_n\}$ and scaling factors $C_{\mathsf{dec}}, C_{\mathsf{sim}} \in R$, define

$$B_1 := \|C_{\mathsf{dec}} \bmod q\|_1 \ ,$$

$$B_2 := \max_{i,\mathcal{S}} \left\|(C_{\mathsf{sim}} \lambda_i^{\mathcal{S} \to \alpha_0}) \bmod q\right\|_1 \ , \qquad \widetilde{B}_2 := \max_{i,\mathcal{S}} \left\|(C_{\mathsf{dec}} \lambda_i^{\mathcal{S} \to \alpha_0}) \bmod q\right\|_1,$$

$$B_3 := \max_{i,\ell,\mathcal{S}^*} \left\|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \lambda_\ell^{\mathcal{S}^* \to \alpha_i}) \bmod q\right\|_1 \ , \quad \widetilde{B}_3 := \left\|(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \bmod q\right\|_1 \ .$$

Here $\mathcal{S}$ ranges over authorized sets of size t with $i \in \mathcal{S}$. In the definition of B_3, we take $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, where $\mathcal{S}_{\mathsf{cor}}$ ranges over maximal unauthorized sets of size $t-1$, and maximize over $i \in [n] \setminus \mathcal{S}_{\mathsf{cor}}$ and $\ell \in \mathcal{S}^*$.

To satisfy Condition **(C4)**, we set B_{sm} throughout our analysis to:

$$B_{\mathsf{sm}} = (B_{\mathsf{eval}} + B_\chi) \cdot 2^\lambda \cdot t \cdot N \cdot (\widetilde{B}_3 + B_3) \ .$$

Substituting B_{sm} into Condition **(C2)** yields the following sufficient lower bound on q:

$$q > 2p \cdot \Big((B_{\mathsf{eval}} + p/4)B_1 + t \cdot B_\chi \cdot \widetilde{B}_2 + t^2 \cdot (B_{\mathsf{eval}} + B_\chi) \cdot 2^\lambda \cdot N \cdot (B_2\widetilde{B}_3 + B_2 B_3) \Big) \ . \tag{4}$$

In what follows, we analyze the monomial interpolation set $\mathcal{I}_{\mathrm{mon}}$. In this setting, the inequality $\widetilde{B}_2 \le B_2\widetilde{B}_3$ holds by writing $C_{\mathsf{dec}} = (C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot C_{\mathsf{sim}}$ and applying the product bound for the L_1-norm. Consequently, $tB_\chi\widetilde{B}_2$ is dominated by the $B_2\widetilde{B}_3$ term in (4). Moreover, B_1 grows only polynomially in t. Thus, the interpolation-dependent growth of the modulus bound is governed by the sum $B_2\widetilde{B}_3 + B_2B_3$, which is exactly the quantity appearing in (4). Therefore, the rest of this analysis focuses on obtaining a tight upper bound on this sum.

4.5 The Monomial Interpolation Set

Consider the monomial interpolation set $\mathcal{I}_{\mathrm{mon}} := \{0, 1, x, x^2, \ldots, x^{n-1}\}$. We use the clearing factors $C_{\mathsf{dec}} = 4^{\lceil \log t \rceil}$ and $C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$.

Theorem 4.4. *Let $C_{\mathsf{dec}} = 4^{\lceil \log t \rceil}$ and $C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, and assume that $p, q > 2$ are odd, $n \le 2N$ and $3 \le t \le \min\{n, N\}$. Then:*

- *the Lagrange reconstruction coefficients associated to $\mathcal{I}_{\mathrm{mon}}$ are well-defined over R_q;*
- *Conditions* **(C1)** *and* **(C3)** *hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, the quantity $\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}) \bmod q\|_1$ is bounded from above by*

$$2^{-t+\lceil \log t \rceil + 1} \cdot \sqrt{N} \cdot \prod_{k=1}^{\lfloor t/2 \rfloor} \frac{1}{\sin^2(\pi k/(2N))} \ , \tag{5}$$

  and the quantity $\|(C_{\mathsf{dec}} \cdot \lambda_i^{\mathcal{S}\to 0}) \bmod q\|_1$ is bounded from above by $2^{\lceil \log t \rceil}$ times the quantity (5);
- *for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, $i \in [n] \setminus \mathcal{S}_{\mathsf{cor}}$ and $\ell \in \mathcal{S}^*$ with $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, the quantity $\|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_\ell^{\mathcal{S}^*\to x^{i-1}}) \bmod q\|_1$ is bounded from above by*

$$2^{\lceil \log t \rceil} \cdot \sqrt{N} \cdot \prod_{k=1}^{\lfloor (t-1)/2 \rfloor} \frac{1}{\sin^2(\pi k/(2N))} \ ; \tag{6}$$

- *the quantity $\|(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \bmod q\|_1$ satisfies*

$$\|(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \bmod q\|_1 \le 2^{\lceil \log t \rceil} \ . \tag{7}$$

Proof. For $\mathcal{S} \in \mathbb{A}_{n,t}$, $i \in \mathcal{S}$, a maximal unauthorized set $\mathcal{S}_{\mathsf{cor}}$, and $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, they are

$$\lambda_i^{\mathcal{S}\to 0} = \pm \prod_{j \in \mathcal{S}\setminus\{i\}} \frac{1}{x^{i-j} - 1}, \qquad \lambda_0^{\mathcal{S}^*\to x^{i-1}} = \pm \prod_{j \in \mathcal{S}_{\mathsf{cor}}} (1 - x^{i-j}),$$

and, for $\ell \in \mathcal{S}_{\mathsf{cor}}$,

$$\lambda_\ell^{\mathcal{S}^* \to x^{i-1}} = x^{i-\ell} \cdot \prod_{j \in \mathcal{S}_{\mathsf{cor}} \setminus \{\ell\}} \frac{x^{i-j}-1}{x^{\ell-j}-1}.$$

These coefficients are well-defined over R_q, as the ideal $\langle x^k - 1 \rangle$ can only divide powers of the ideal $\langle 2 \rangle$ (by Lemma 2.2) and q is assumed odd.

The denominator of $\lambda_0^{\mathcal{S}^* \to x^{i-1}}$ is a unit in R, while the denominators of $\lambda_i^{\mathcal{S} \to 0}$ and of $\lambda_\ell^{\mathcal{S}^* \to x^{i-1}}$ for $\ell \in \mathcal{S}_{\mathsf{cor}}$ are products of at most $t-1$ factors of the form $x^k - 1$. As in the proof of Theorem 3.8, it follows from [AL21, Theorem 1] that each such product divides $2^{\lceil \log t \rceil}$ in R. Since $C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, $C_{\mathsf{dec}} = C_{\mathsf{sim}}^2$ and $C_{\mathsf{dec}}/C_{\mathsf{sim}} = C_{\mathsf{sim}}$, it follows that $C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}$, $C_{\mathsf{dec}} \cdot \lambda_i^{\mathcal{S} \to 0}$ and $(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_\ell^{\mathcal{S}^* \to x^{i-1}}$ all belong to R. Finally, C_{dec} and C_{sim} are powers of 2, so they are invertible modulo the odd integers p and q, respectively; this establishes Conditions **(C1)** and **(C3)**.

We now bound the coefficient norms. By Lemma 2.3, it suffices to bound the complex embeddings. Throughout, for an embedding $\zeta = \exp(\pi \mathsf{i} r/N)$, we use

$$|\zeta^k - 1| = 2|\sin(\pi r k/(2N))|.$$

Since r is coprime to $2N$, multiplication by r permutes the nonzero residue classes modulo $2N$.

Fix $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$. Applying the embedding identity above to $C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}$ gives

$$\left|\sigma\left(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}\right)\right| = 2^{-t+\lceil \log t \rceil + 1} \prod_{j \in \mathcal{S} \setminus \{i\}} \frac{1}{|\sin(\pi r(i-j)/(2N))|}.$$

It remains to maximize the inverse-sine product over the $t-1$ nonzero distances $r(i-j) \bmod 2N$. Since multiplication by r is a permutation and each distance can occur at most twice, the worst case is obtained by taking the nearest-distance configuration $\{1, 1, 2, 2, \ldots\}$. Hence

$$\left|\sigma\left(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}\right)\right| \le 2^{-t+\lceil \log t \rceil + 1} \prod_{k=1}^{\lfloor t/2 \rfloor} \frac{1}{\sin^2(\pi k/(2N))}.$$

Applying Lemma 2.3 gives

$$\left\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q\right\|_1 \le 2^{-t+\lceil \log t \rceil + 1} \cdot \sqrt{N} \cdot \prod_{k=1}^{\lfloor t/2 \rfloor} \frac{1}{\sin^2(\pi k/(2N))},$$

which is (5). Further, as $C_{\mathsf{dec}} = 2^{\lceil \log t \rceil} \cdot C_{\mathsf{sim}}$ and reduction modulo q cannot increase the absolute value of a coefficient, we have

$$\left\|(C_{\mathsf{dec}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q\right\|_1 \le 2^{\lceil \log t \rceil} \cdot \left\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q\right\|_1,$$

which is the claimed bound on $\|(C_{\mathsf{dec}} \cdot \lambda_i^{\mathcal{S} \to 0}) \bmod q\|_1$.

Fix a maximal unauthorized set $\mathcal{S}_{\mathsf{cor}}$, set $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, and fix $i \in [n] \setminus \mathcal{S}_{\mathsf{cor}}$. There are two cases, according to whether $\ell = 0$ or $\ell \in \mathcal{S}_{\mathsf{cor}}$.

First consider $\ell = 0$. In this case,

$$\lambda_0^{\mathcal{S}^* \to x^{i-1}} = \pm \prod_{j \in \mathcal{S}_{\mathsf{cor}}} (1 - x^{i-j}),$$

so there is no denominator. For an embedding $\sigma(x) = \zeta = \exp(\pi i r/N)$, we obtain

$$\left| \sigma\Big((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \to x^{i-1}} \Big) \right| = 2^{t-1+\lceil \log t \rceil} \prod_{j \in \mathcal{S}_{\mathsf{cor}}} |\sin(\pi r(i-j)/(2N))|.$$

Since multiplication by r permutes the residue classes modulo $2N$, this sine product is maximized by placing the distances as close as possible to N. Thus the worst case gives one factor 1, and then paired factors $\cos^2(\pi k/(2N))$. Applying Lemma 2.3, we get

$$\left\| ((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \to x^{i-1}}) \bmod q \right\|_1 \le T_0,$$

where $T_0 := 2^{t-1+\lceil \log t \rceil} \cdot \sqrt{N} \cdot \prod_{k=1}^{\lfloor t/2 \rfloor - 1} \cos^2(\pi k/(2N))$.

Now consider $\ell \in \mathcal{S}_{\mathsf{cor}}$. Here

$$\lambda_\ell^{\mathcal{S}^* \to x^{i-1}} = x^{i-\ell} \cdot \prod_{j \in \mathcal{S}_{\mathsf{cor}} \setminus \{\ell\}} \frac{x^{i-j} - 1}{x^{\ell-j} - 1}.$$

We bound the numerator sine factors by 1, while the denominator is minimized by the nearest-distance configuration $\{1, 1, 2, 2, \ldots\}$. Hence

$$\left\| ((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_\ell^{\mathcal{S}^* \to x^{i-1}}) \bmod q \right\|_1 \le T_\star,$$

where

$$T_\star := 2^{\lceil \log t \rceil} \cdot \sqrt{N} \cdot \prod_{k=1}^{\lfloor (t-1)/2 \rfloor} \frac{1}{\sin^2(\pi k/(2N))}.$$

It remains to compare the two bounds. Writing $\tau := \lfloor t/2 \rfloor$ and using $\sin(2\theta) = 2 \sin\theta \cos\theta$, we get

$$\frac{T_\star}{T_0} = \begin{cases} \dfrac{1}{2} \displaystyle\prod_{k=1}^{\tau-1} \csc^2(\pi k/N), & t \text{ even}, \\[2ex] \dfrac{1}{4\sin^2(\pi\tau/(2N))} \displaystyle\prod_{k=1}^{\tau-1} \csc^2(\pi k/N), & t \text{ odd}. \end{cases}$$

This ratio is at least 1 for $t \ge 3$ and $N \ge t$. Therefore, in both cases, the quantity $\|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_\ell^{\mathcal{S}^* \to x^{i-1}}) \bmod q\|_1$ is at most $T_\star$, which is (6).

Finally, since $C_{\mathsf{dec}}/C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$ is an integer and reduction modulo q cannot increase the absolute value, we have $\|(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \bmod q\|_1 \le 2^{\lceil \log t \rceil}$, which is (7). This completes the proof. □

Combining Theorem 4.4 with Theorems 4.1 and 4.2, we obtain correctness and strong simulation security. The quantity that governs the modulus bound (4) is the sum $B_2\widetilde{B}_3 + B_2B_3$, and the following corollary gives the bound on it in that setting.

Corollary 4.5. *Under the assumptions of Theorem 4.4,*

$$\begin{aligned} B_2\widetilde{B}_3 + B_2B_3 \;\leq\; & 2^{-t+2\lceil \log t\rceil+1}\cdot\sqrt{N}\cdot\prod_{k=1}^{\lfloor t/2\rfloor}\frac{1}{\sin^2(\pi k/(2N))} \\ & \cdot\left(1+\sqrt{N}\cdot\prod_{k=1}^{\lfloor (t-1)/2\rfloor}\frac{1}{\sin^2(\pi k/(2N))}\right). \end{aligned} \tag{8}$$

Proof. Recall that B_2, B_3 and $\widetilde{B}_3$ are defined in Section 4.4 as maxima over the ranges of $\mathcal{S}$ and i (resp. $\mathcal{S}_{\mathsf{cor}}$, i and ℓ) considered in Theorem 4.4. Hence Theorem 4.4 gives that B_2 is bounded from above by the quantity (5), that B_3 is bounded from above by the quantity (6), and, by (7), that $\widetilde{B}_3 \leq 2^{\lceil \log t\rceil}$. Multiplying the bound on B_2 by $2^{\lceil \log t\rceil}$ and by the quantity (6), respectively, gives

$$B_2\cdot\widetilde{B}_3 \leq 2^{-t+2\lceil \log t\rceil+1}\cdot\sqrt{N}\cdot\prod_{k=1}^{\lfloor t/2\rfloor}\frac{1}{\sin^2(\pi k/(2N))}$$

and

$$B_2\cdot B_3 \leq 2^{-t+2\lceil \log t\rceil+1}\cdot N\cdot\prod_{k=1}^{\lfloor t/2\rfloor}\frac{1}{\sin^2(\pi k/(2N))}\cdot\prod_{k=1}^{\lfloor (t-1)/2\rfloor}\frac{1}{\sin^2(\pi k/(2N))}.$$

Adding the two inequalities and factoring out the common terms gives (8). □

5 Optimizing the Interpolation Set

In this section, we present two techniques to optimize the lower bound on the ciphertext modulus q under the monomial interpolation set for our first and second constructions, respectively.

5.1 Spaced Evaluation Points and Virtual Points

First, we tighten the bounds for $\mathcal{I}_{\mathrm{mon}}$ by distributing the n evaluation points evenly among the $2N$ distinguished monomials. Define the set

$$\mathcal{N}_{n,N} \coloneqq \{2^k : k \in \mathbb{Z}_{\geq 0}\} \cap [n, 2N] \ .$$

Since $n \leq 2N$ and $2N$ is a power of two, $\mathcal{N}_{n,N}$ is non-empty. For $n' \in \mathcal{N}_{n,N}$ with $n' \geq 2$, we define the spaced interpolation set

$$\mathcal{I}^*_{\mathrm{mon}} \coloneqq \{0\} \cup \left\{x^{(i-1)\cdot\frac{2N}{n'}} : i \in [n]\right\} \ .$$

Second, we enlarge the interpolation set using public evaluation points, which we refer to as *virtual points*. This increases the size of the interpolation set while keeping both the threshold among real parties and the required number of partial decryptions unchanged. For any fixed $n' \in \mathcal{N}_{n,N}$ and integer c with $0 \le c \le n' - n$, we define the augmented interpolation set

$$\mathcal{I}^{\star}_{\mathrm{mon}}(n', c) \coloneqq \{0\} \cup \left\{ x^{(i-1)\cdot \frac{2N}{n'}} : i \in [n + c] \right\} \ .$$

The set $\mathcal{I}^{\star}_{\mathrm{mon}}(n', c)$ has cardinality $n + c + 1$. We interpret the first n indices as *real* parties and the remaining index set

$$V \coloneqq \{n + 1, \ldots, n + c\}$$

as *virtual* parties. The shares for virtual parties are public values and thus available to all participants without communication overhead.

Whenever interpolation is performed over a subset of t real parties, all c virtual points are additionally included. Thus, the effective interpolation size becomes $t' = t + c$, while preserving the underlying (t, n)-threshold access structure among the real parties. Accordingly, for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$ with $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}^{\mathsf{c\text{-}max}}_{n,t}$, all Lagrange interpolation coefficients are evaluated on the corresponding augmented point sets:

$$\lambda_i^{\mathcal{S}\to\alpha_0} \ \to \ \lambda_i^{\mathcal{S}\cup V\to\alpha_0} \qquad \text{and} \qquad \lambda_0^{\mathcal{S}^*\to\alpha_i} \ \to \ \lambda_0^{\mathcal{S}^*\cup V\to\alpha_i} \ .$$

During the execution of FinDec, any party can publicly derive the decryption shares associated with the virtual points. Consequently, virtual points introduce zero communication overhead during distributed decryption, requiring only the local computation of c additional decryption shares.

5.2 Optimizing Bounds for the First Construction

In this subsection, we quantify the impact of spaced evaluation and virtual points on our first construction to obtain optimized bounds.

Spaced evaluation points.

Corollary 5.1. *For $i \in [n]$, set $\alpha_i := x^{(i-1)\cdot 2N/n'}$. Let $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, and assume that $p, q > 2$ are odd. Then:*

- *the Lagrange reconstruction coefficients associated to $\mathcal{I}^{*}_{\mathrm{mon}}$ are well-defined over R_q;*
- *Conditions* **(C1)** *and* **(C3)** *hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, the quantity $\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0}) \bmod q\|_1$ is bounded from above by:*

$$2^{-t+\lceil \log t \rceil + 1} \cdot \sqrt{\frac{n'}{2}} \cdot \prod_{k \in [\lfloor t/2 \rfloor]} \frac{1}{\sin^2\left(\pi \frac{k}{n'}\right)} \ ;$$

- *for any* $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$ *and* $i \in [n] \setminus \mathcal{S}^*$ *with* $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$*, the quantity* $\|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \to \alpha_i}) \bmod q\|_1$ *is bounded from above by:*

$$2^{t-1} \cdot \sqrt{\frac{n'}{2}} \cdot \prod_{k \in [\lfloor t/2 \rfloor - 1]} \cos^2\left(\pi \frac{k}{n'}\right) \ .$$

Proof. Write $y := x^{2N/n'} \in R = \mathbb{Z}[x]/(x^N+1)$. Then we have $y^{n'/2} = -1$ and the set of all integer linear combinations of powers of y forms a subring R' of R that is isomorphic to $\mathbb{Z}[y]/(y^{n'/2}+1)$. By construction, all the elements of $\mathcal{I}^*_{\mathrm{mon}} \setminus \{0\}$ are powers of y.

As a result, we are exactly in the setting of Theorem 3.8, with ring degree $n'/2$, ring R', and generator y. Hence the same upper bounds that were proved for $\mathcal{I}_{\mathrm{mon}}$ apply to $\mathcal{I}^*_{\mathrm{mon}}$ after the substitution $N = n'/2$. □

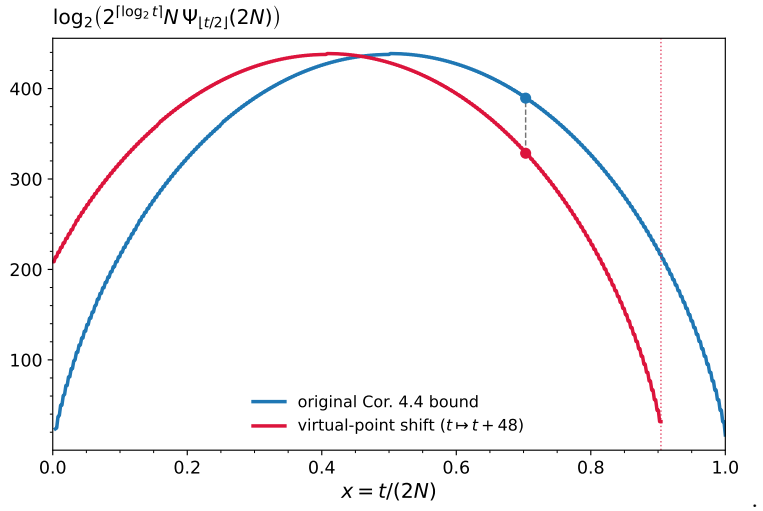


Fig. 7: Effect of adding $c = 48$ virtual parties on the first-construction trigonometric upper bound for B_2B_3.

Virtual points. As suggested by Figure 7, for fixed n', the dominant upper bound on $B_2 \cdot B_3$ associated with $\mathcal{I}^*_{\mathrm{mon}}$ is essentially unimodal as a function of the interpolation size: it is largest near $t = n'/2$ and decreases for larger t. Therefore, when the target threshold already lies on this decreasing branch, increasing the interpolation size can improve the bound rather than worsen it. We realize this without changing the underlying (t, n)-threshold structure among the real parties by introducing *virtual parties*, namely additional publicly known interpolation points whose shares are available to every party.

Corollary 5.2. *For $i \in [n]$, set $\alpha_i := x^{(i-1)\cdot 2N/n'}$. Let $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2^{\lceil \log t' \rceil}$, and assume that $p, q > 2$ are odd. Then:*

- *the Lagrange reconstruction coefficients associated to $\mathcal{I}^{\star}_{\mathrm{mon}}(n', c)$ are well-defined over R_q;*
- *Conditions* **(C1)** *and* **(C3)** *hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$, the quantity $\|(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \cup V \to 0}) \bmod q\|_1$ is bounded from above by:*

$$2^{-t' + \lceil \log t' \rceil + 1} \cdot \sqrt{\frac{n'}{2}} \cdot \prod_{k \in [\lfloor t'/2 \rfloor]} \frac{1}{\sin^2\left(\pi \frac{k}{n'}\right)} \ ;$$

- *for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}^{\mathsf{c\text{-}max}}_{n,t}$ and $i \in [n] \setminus \mathcal{S}^*$ with $\mathcal{S}^* = \{0\} \cup \mathcal{S}_{\mathsf{cor}}$, the quantity $\|((C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_0^{\mathcal{S}^* \cup V \to \alpha_i}) \bmod q\|_1$ is bounded from above by:*

$$2^{t'-1} \cdot \sqrt{\frac{n'}{2}} \cdot \prod_{k \in [\lfloor t'/2 \rfloor - 1]} \cos^2\left(\pi \frac{k}{n'}\right) \ .$$

Optimal choice of (n', c). For any fixed triple (n, N, t), Theorem 5.3 establishes the parameter selection that minimizes the product $B_2 B_3$, along with the explicit value of the minimum bound.

Theorem 5.3. *For any $n' \in \mathcal{N}_{n,N} := \{2^k : \ k \geq 2, \ n \leq 2^k \leq 2N\}$ and any integer c with $0 \leq c \leq n' - n$, set $t' := t + c$ and consider the interpolation set $\mathcal{I}^{\star}_{\mathrm{mon}}(n', c)$ defined in Section 5.1. For $0 \leq m \leq n'/2$, define*

$$\Psi_m(n') := \left(\prod_{k \in [m]} \frac{1}{\sin^2\left(\pi \frac{k}{n'}\right)} \right) \cdot \left(\prod_{k \in [m-1]} \cos^2\left(\pi \frac{k}{n'}\right) \right) \ .$$

Then we have

$$B_2 \cdot B_3 \leq 2^{\lceil \log t' \rceil} \cdot \frac{n'}{2} \cdot \Psi_{\lfloor t'/2 \rfloor}(n') \ .$$

Assume that $2 \leq t \leq n \leq 2N$, and let $n_0 = 2^{\lceil \log n \rceil}$. Define

$$c_0 := \begin{cases} 0 & \text{if } \left\lfloor \frac{t}{2} \right\rfloor + \left\lfloor \frac{t + n_0 - n}{2} \right\rfloor \leq \frac{n_0}{2} \\ n_0 - n & \text{otherwise.} \end{cases} ,$$

Then, among all admissible choices (n', c), the quantity $\Psi_{\lfloor t'/2 \rfloor}(n')$ is minimized by $(n', c) = (n_0, c_0)$.

Proof. The bound given for $B_2 \cdot B_3$ follows directly from Corollary 5.2. It remains to minimize the trigonometric factor $\Psi_{\tau'}(n')$, where $\tau' = \lfloor t'/2 \rfloor = \lfloor (t + c)/2 \rfloor$. We first assume that $n \geq 3$, implying that $n' \geq 4$, and will subsequently consider the case of $t = n = 2$.

We define $C_{-1}(n') := 0$ and, for $0 \leq m \leq n'/2$:

$$C_m(n') := \prod_{k\in[m]} \cot^2\left(\pi\frac{k}{n'}\right) \ .$$

For every m with $1 \leq m \leq n'/2$, we have the exact identity

$$\begin{aligned}\Psi_m(n') &= \frac{1}{\sin^2\left(\pi\frac{m}{n'}\right)} \prod_{k\in[m-1]} \cot^2\left(\pi\frac{k}{n'}\right) \\ &= \left(1+\cot^2\left(\pi\frac{m}{n'}\right)\right) \prod_{k\in[m-1]} \cot^2\left(\pi\frac{k}{n'}\right) \\ &= C_{m-1}(n') + C_m(n') \ .\end{aligned}$$

Note that the equality $\Psi_m(n') = C_{m-1}(n') + C_m(n')$ also holds for $m = 0$. Moreover, since $\cot(\pi/2) = 0$, we also have $C_{n'/2}(n') = 0$.

Step 1: Endpoint restriction for fixed n'. Fix n'. As the shift c ranges over $\{0, 1, \ldots, n' - n\}$, the integer $\tau' = \lfloor (t + c)/2 \rfloor$ ranges over $\{a, \ldots, b\}$ with

$$a \coloneqq \left\lfloor \frac{t}{2} \right\rfloor \ \text{ and } \ b \coloneqq \left\lfloor \frac{t+n'-n}{2} \right\rfloor \ .$$

We first study the shape of $m \mapsto \Psi_m(n')$. For every m with $1 \leq m < n'/2$, we have

$$\frac{\Psi_{m+1}(n')}{\Psi_m(n')} = \frac{\cos^2\left(\pi\frac{m}{n'}\right)}{\sin^2\left(\pi\frac{m+1}{n'}\right)} = \frac{\sin^2\left(\pi\left(\frac{1}{2}-\frac{m}{n'}\right)\right)}{\sin^2\left(\pi\frac{m+1}{n'}\right)} \ .$$

Since $x \mapsto \sin^2(x)$ increases on $[0, \pi/2]$, this ratio is > 1 if and only if

$$\frac{\pi}{2} - \pi\frac{m}{n'} > \pi\frac{m+1}{n'} \iff 2m+1 < \frac{n'}{2} \iff m \leq \frac{n'}{4} - 1 \ .$$

The last equivalency follows from the fact that $n'/4$ is an integer. Overall, for fixed n', we have $\Psi_{m+1}(n') > \Psi_m(n')$ for $m < n'/4$ and $\Psi_{m+1}(n') < \Psi_m(n')$ for $m \geq n'/4$.

Now, as $\cot(\pi k/n') \cdot \cot(\pi(n'/2 - k)/n') = \cot(\pi k/n') \tan(\pi k/n') = 1$ for all $k \in [n'/2]$, we have

$$\prod_{k\in[n'/2-1]} \cot^2\left(\pi\frac{k}{n'}\right) = 1 \ .$$

We then obtain that $C_{n'/2-m-1}(n') = C_m(n')$ holds for every $-1 \leq m \leq n'/2$. It implies the following, for every $0 \leq m \leq n'/2$:

$$\begin{aligned}\Psi_{n'/2-m}(n') &= C_{n'/2-m-1}(n') + C_{n'/2-m}(n') \\ &= C_m(n') + C_{m-1}(n') \\ &= \Psi_m(n') \ .\end{aligned}$$

At this point, we know that $m \mapsto \Psi_m(n')$ is symmetric around $n'/4$ and unimodal, with maximum at $m = n'/4$. Consequently, its minimum over the integer interval $[a, b]$ is reached at an endpoint, and the smaller endpoint is the one farther away from $n'/4$. It follows that

$$\min_{0 \le c \le n'-n} \Psi_{\tau'}(n') = \min\{\Psi_a(n'), \Psi_b(n')\} \quad ,$$

and

$$\Psi_a(n') \le \Psi_b(n') \iff a \le \frac{n'}{2} - b \iff a + b \le \frac{n'}{2} \ .$$

Step 2: Global minimization. Let $m_0 = \lfloor t/2 \rfloor$ and $m_1 = \lceil (n-t)/2 \rceil$. Since n' is even, we have

$$b = \left\lfloor \frac{t + n' - n}{2} \right\rfloor = \frac{n'}{2} + \left\lfloor \frac{t-n}{2} \right\rfloor = \frac{n'}{2} - m_1 \ .$$

Using the symmetry proved above, this gives $\Psi_b(n') = \Psi_{m_1}(n')$ and hence

$$\min_{0 \le c \le n'-n} \Psi(n', c) = \min\{\Psi_{m_0}(n'), \Psi_{m_1}(n')\} \quad .$$

Note that neither m_0 nor m_1 depends on n'.

Now fix $m \in \{m_0, m_1\}$. If $m = 0$, then $\Psi_m(n') = 1$ holds for all admissible n'. If $m \ge 1$, then

$$\Psi_m(n') = \frac{1}{\sin^2\left(\pi \frac{m}{n'}\right)} \prod_{k \in [m-1]} \cot^2\left(\pi \frac{k}{n'}\right).$$

Whenever $2n'$ is admissible, each angle $\pi k/(2n')$ is smaller than $\pi k/n'$ and still lies in $(0, \pi/2)$. Since the functions $x \mapsto 1/\sin^2 x$ and $x \mapsto \cot^2 x$ strictly decrease on $(0, \pi/2)$, every factor in the expression above strictly increases when n' is replaced by $2n'$. We thus obtain that $\Psi_m(2n') > \Psi_m(n')$ holds for every $m \ge 1$. This implies that both endpoint values are minimized at the smallest admissible power of two, namely $n_0 = 2^{\lceil \log n \rceil}$. Applying Step 1 with $n' = n_0$ completes the proof for $n \ge 3$.

The particular case of $t = n = 2$. In that case, the parameter n' can be any power of two in $[2, 2N]$. We observe that the above study works for any $n' \ge 4$, independently of the values of t and n. As a result, the smallest value of $\Psi_{\tau'}(n')$ for all values of (n', c) conditioned on $n' \ge 4$ is obtained for $n' = 4$. As a result, we have that $\min(\Psi_1(4), \Psi_2(4)) \ge \Psi_1(2) = 1$,[9] and the statement of Theorem 5.3 also holds for $t = n = 2$. □

5.3 Optimizing Bounds for the Second Construction

In this subsection, we quantify the impact of spaced evaluation and virtual points on our second construction to obtain optimized bounds.

[9] Note that $\Psi_1(4) = 2$, $\Psi_2(4) = 1$ and $\Psi_1(2) = 1$.

For the second construction, fix a power of two n' with $n \le n' \le 2N$ and an integer c with $0 \le c \le n'-n$. Set $t' := t+c$ and $V := \{n+1, \ldots, n+c\}$. The two Shamir polynomials used in KeyGen are sampled with degree less than t', and the share pairs $(\mathsf{sk}_v, s_v)_{v\in V}$ are included in the public key. Since fewer than t real shares together with the c public shares give fewer than t' evaluations of either Shamir polynomial, publishing the virtual shares preserves the (t,n)-threshold access structure among the real parties.

For a ciphertext $\mathsf{ct} = (a,b)$ and each $v \in V$, define the public partial decryption

$$\mathsf{p}_v^{\mathrm{pub}} := C_{\mathsf{dec}}\big(a\mathsf{sk}_v + H(\mathsf{ct})s_v\big) \bmod q.$$

Unlike a real partial decryption, $\mathsf{p}_v^{\mathrm{pub}}$ contains neither an H_χ-generated error nor smudging noise. Given partial decryptions from an authorized set $\mathcal{S} \subseteq [n]$ of t real parties, FinDec computes

$$\begin{aligned} x \leftarrow C_{\mathsf{dec}} b &+ \sum_{i\in\mathcal{S}} \lambda_i^{\mathcal{S}\cup V\to\alpha_0}\mathsf{p}_i \\ &+ \sum_{v\in V} \lambda_v^{\mathcal{S}\cup V\to\alpha_0}\mathsf{p}_v^{\mathrm{pub}} \pmod q, \end{aligned}$$

and then applies the same rounding step as in the second construction.

The strong-simulation security extends to this augmented interpolation set. Conditioned on the public virtual zero shares and the corrupted real zero shares, the degree-$(t'-1)$ zero-sharing polynomial has $t'-1-c-|\mathcal{S}_{\mathsf{cor}}| = t-1-|\mathcal{S}_{\mathsf{cor}}|$ uniformly random degrees of freedom. Hence the joint-uniformity and RLWE argument used for Sim_1 remains unchanged. At the threshold-reaching query, Sim_2 interpolates over $\{0\}\cup T_{\mathsf{ct}}\cup V$. Since the virtual partial decryptions contain neither H_χ-generated errors nor smudging noise, all noise sums still contain at most t real partial decryptions.

Corollary 5.4. *Let $n' \in [n, 2N]$ be a power of two, let $0 \le c \le n'-n$, and set $t' := t+c$ and $V := \{n+1, \ldots, n+c\}$. For $i \in [n+c]$, set $\alpha_i := x^{(i-1)\cdot 2N/n'}$. Let $C_{\mathsf{dec}} = 4^{\lceil \log t' \rceil}$ and $C_{\mathsf{sim}} = 2^{\lceil \log t' \rceil}$, and assume that $p, q > 2$ are odd and $3 \le t' \le n'/2$. Then:*

- *the Lagrange reconstruction coefficients associated with $\mathcal{I}^{\star}_{\mathrm{mon}}(n', c)$ are well-defined over R_q;*
- *Conditions **(C1)** and **(C3)** hold;*
- *for any $\mathcal{S} \in \mathbb{A}_{n,t}$ and $i \in \mathcal{S}$,*

$$\left\| \left(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\cup V\to\alpha_0} \right) \bmod q \right\|_1 \le 2^{-t'+\lceil \log t' \rceil + 1} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor t'/2 \rfloor} \frac{1}{\sin^2(\pi k/n')};$$

- *for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, $i \in [n] \setminus \mathcal{S}_{\mathsf{cor}}$, and $\ell \in \{0\} \cup \mathcal{S}_{\mathsf{cor}}$,*

$$\left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \lambda_\ell^{\{0\}\cup\mathcal{S}_{\mathsf{cor}}\cup V\to\alpha_i} \right) \bmod q \right\|_1 \le 2^{\lceil \log t' \rceil} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor (t'-1)/2 \rfloor} \frac{1}{\sin^2(\pi k/n')}.$$

Proof. Set $y := x^{2N/n'} \in R$. Then $y^{n'/2} = x^N = -1$, and the subring generated by y is isomorphic to $\mathbb{Z}[y]/(y^{n'/2}+1)$. Moreover, $\alpha_i = y^{i-1}$ for all $i \in [n+c]$.

For any $\mathcal{S} \in \mathbb{A}_{n,t}$, the augmented set $\mathcal{S} \cup V$ contains exactly $t + c = t'$ share indices. Likewise, for any $\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\mathsf{c\text{-}max}}$, the set $\{0\} \cup \mathcal{S}_{\mathsf{cor}} \cup V$ consists of the reconstruction point together with $(t-1)+c = t'-1$ share indices. Therefore, all Lagrange coefficients in the preceding expression belong to the set of coefficients established by Theorem 4.4, evaluated in the subring generated by y with parameters $N = \frac{n'}{2}$ and $t = t'$.

Under this substitution, the reconstruction-side bound of Theorem 4.4 becomes

$$\left\| \left(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\cup V \to \alpha_0} \right) \bmod q \right\|_1 \le 2^{-t'+\lceil \log t' \rceil + 1} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor t'/2 \rfloor} \frac{1}{\sin^2(\pi k/n')}.$$

Similarly, the strong-simulation-side bound, which holds uniformly over all interpolation indices, gives

$$\left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \lambda_\ell^{\{0\}\cup \mathcal{S}_{\mathsf{cor}} \cup V \to \alpha_i} \right) \bmod q \right\|_1 \le 2^{\lceil \log t' \rceil} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor (t'-1)/2 \rfloor} \frac{1}{\sin^2(\pi k/n')}.$$

The same argument shows that the required scaled Lagrange coefficients lie in R. Finally, C_{dec} and C_{sim} are powers of two, and hence are invertible modulo the odd moduli p and q, respectively. Thus Conditions **(C1)** and **(C3)** hold. □

We next optimize the upper bound on $B_2\widetilde{B}_3 + B_2 B_3$ over the choice of (n', c).

Theorem 5.5 (Optimal choice of (n', c)). *Assume that $3 \le t \le n \le 2N$ and $t \le N$. For any power of two $n' \in [n, 2N]$ and any integer $0 \le c \le n' - n$ satisfying $t' := t + c \le n'/2$, consider $\mathcal{I}^{\star}_{\mathrm{mon}}(n', c)$ with $C_{\mathsf{dec}} = 4^{\lceil \log t' \rceil}$ and $C_{\mathsf{sim}} = 2^{\lceil \log t' \rceil}$. Then*

$$B_2\widetilde{B}_3 + B_2 B_3 \le 2^{-t'+2\lceil \log t' \rceil + 1} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor t'/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right) \cdot \left(1 + \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor (t'-1)/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right)\right). \tag{9}$$

Among all admissible pairs (n', c), the upper bound in (9) is minimized at $c = 0$, and $n' = 2^{\lceil \log_2 \max\{n, 2t\} \rceil}$.

Proof. Fix an admissible pair (n', c) and set $t' := t + c$. We apply Corollary 5.4 to $\mathcal{I}^{\star}_{\mathrm{mon}}(n', c)$ with $C_{\mathsf{dec}} = 4^{\lceil \log t' \rceil}$ and $C_{\mathsf{sim}} = 2^{\lceil \log t' \rceil}$. The reconstruction-side bound gives

$$B_2 \le 2^{-t'+\lceil \log t' \rceil + 1} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor t'/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right).$$

Since $C_{\mathsf{dec}}/C_{\mathsf{sim}} = 2^{\lceil \log t' \rceil}$, we have $\widetilde{B}_3 \leq 2^{\lceil \log t' \rceil}$, and therefore

$$B_2 \widetilde{B}_3 \leq 2^{-t'+2\lceil \log t' \rceil+1} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor t'/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right).$$

The simulation-side bound of Corollary 5.4 gives

$$B_3 \leq 2^{\lceil \log t' \rceil} \sqrt{\frac{n'}{2}} \prod_{k=1}^{\lfloor (t'-1)/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right).$$

Combining this with the bound on B_2 yields

$$B_2 B_3 \leq 2^{-t'+2\lceil \log t' \rceil+1} \frac{n'}{2} \prod_{k=1}^{\lfloor t'/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right) \prod_{k=1}^{\lfloor (t'-1)/2 \rfloor} \csc^2\left(\frac{\pi k}{n'}\right).$$

Adding the two inequalities and factoring the common terms gives (9).

Fix n' and consider an admissible transition $t' \mapsto t'+1$. We show that the right-hand side of (9) is non-decreasing under every such transition.

Suppose first that $t' = 2s+1$ is odd. Since $t' \geq 3$, it is not a power of two, so

$$\frac{2^{-(t'+1)+2\lceil \log(t'+1) \rceil+1}}{2^{-t'+2\lceil \log t' \rceil+1}} = \frac{1}{2}.$$

The first inverse-sine product gains the factor $\csc^2(\pi(s+1)/n')$, whereas the second product is unchanged. Hence the ratio of the two right-hand sides of (9) is

$$\frac{1}{2} \csc^2\left(\frac{\pi(s+1)}{n'}\right).$$

Admissibility of the transition gives $2s+2 \leq n'/2$, and therefore $\pi(s+1)/n' \leq \pi/4$. Thus the ratio is at least 1.

Now suppose that $t' = 2s$ is even. If t' is a power of two, the power-of-two prefactor is multiplied by 2, while all remaining factors are non-decreasing. Hence the right-hand side strictly increases.

It remains to consider even t' that is not a power of two. In this case the prefactor is multiplied by $1/2$, the first inverse-sine product is unchanged, and the second product gains the factor $\csc^2(\pi s/n')$. Therefore the ratio between the right-hand sides at $t'+1$ and t' is

$$\frac{1}{2} \frac{1 + \sqrt{n'/2}\left(\prod_{k=1}^{s-1} \csc^2\left(\frac{\pi k}{n'}\right)\right) \csc^2\left(\frac{\pi s}{n'}\right)}{1 + \sqrt{n'/2} \prod_{k=1}^{s-1} \csc^2\left(\frac{\pi k}{n'}\right)}.$$

This ratio is at least 1 if

$$\sqrt{\frac{n'}{2}} \prod_{k=1}^{s-1} \csc^2\left(\frac{\pi k}{n'}\right)\left(\csc^2\left(\frac{\pi s}{n'}\right) - 2\right) \geq 1. \tag{10}$$

Admissibility gives $2s + 1 \le n'/2$. Since $n'/4$ is an integer, $s \le n'/4 - 1$. Writing $\theta := \pi s/n'$, we obtain

$$\begin{aligned}\csc^2\theta - 2 &= \frac{\cos(2\theta)}{\sin^2\theta} \\ &\ge 2\cos(2\theta) \\ &\ge 2\sin\left(\frac{2\pi}{n'}\right) \ge \frac{8}{n'}.\end{aligned}$$

Here the first inequality uses $\theta \le \pi/4$, the second uses $s \le n'/4 - 1$, and the last follows from $\sin x \ge 2x/\pi$ on $[0, \pi/2]$.

Since an even integer at least 3 that is not a power of two satisfies $t' \ge 6$, we have $s \ge 3$. Hence the product in (10) contains the factor indexed by $k = 1$, and $\sin x \le x$ gives

$$\prod_{k=1}^{s-1} \csc^2\left(\frac{\pi k}{n'}\right) \ge \csc^2\left(\frac{\pi}{n'}\right) \ge \frac{n'^2}{\pi^2}.$$

The left-hand side of (10) is therefore at least

$$\sqrt{\frac{n'}{2}}\frac{n'^2}{\pi^2}\frac{8}{n'} = \frac{4\sqrt{2}}{\pi^2}n'^{3/2}.$$

The smallest possible value in this case is $n' = 16$, since admissibility of the transition from $t' = 6$ to $t' = 7$ requires $n' \ge 14$ and n' is a power of two. Thus (10) holds. The right-hand side of (9) is therefore non-decreasing in t' for fixed n'. Since $t' = t + c$, it is minimized at $c = 0$.

It remains to optimize n' with $c = 0$. Then $t' = t$ is fixed, so the factor $2^{-t+2\lceil \log t \rceil + 1}$ is independent of n'. As n' increases, both $\sqrt{n'/2}$ and every factor $\csc^2(\pi k/n')$ appearing in (9) strictly increase. Hence the right-hand side of (9) is strictly increasing in n' over the admissible powers of two.

For $c = 0$, admissibility requires $n' \ge n$ and $n' \ge 2t$. Thus the smallest admissible power of two is

$$n' = 2^{\lceil \log_2 \max\{n, 2t\} \rceil}.$$

The assumptions $n \le 2N$ and $t \le N$ ensure that this value is at most $2N$. □

6 Experiments

In this section, we empirically evaluate the tightness of our theoretical bounds and compare them with those established in prior work.[10] For our first construction, in which $B_2 \cdot B_3$ is the dominant term in the ciphertext-modulus bound

[10] The scripts reproducing all tables and figures of this section are available at `https://anonymous.4open.science/r/JoC-5134`.

q, we examine the tightness of the bounds for both integer and monomial interpolation sets and compare them with the results of [BFM+25,CLW25] (see Section 3.4). For our second construction, in which $B_2 \cdot B_3 + B_2 \cdot \widetilde{B}_3$ dominates the bound on q, we evaluate the tightness of the monomial-coefficient bounds and compare the sizes of the partial-decryption elements with those reported in [EY24] (see Section 4.4).

6.1 First Construction: Tightness and Comparison

We construct reconstruction and simulation sets $\mathcal{S}$ and $\mathcal{S}_{\mathsf{cor}}$ that lead to large values of B_2 and B_3, respectively, and compare the resulting product $B_2 \cdot B_3$ with our theoretical bounds. Note that multiplying B_2 and B_3 corresponds to instantiating a reconstruction set $\mathcal{S}$ and a corrupted set $\mathcal{S}_{\mathsf{cor}}$: as these do not have to be identical, a worst configuration for B_2 can be combined with a worst configuration for B_3.

Integer Interpolation Set (Section 3.5). To demonstrate the tightness of our analytic bound for the integer interpolation set (Theorem 3.4), we construct explicit instances that are expected to be close to worst-case instances for B_2 and B_3.

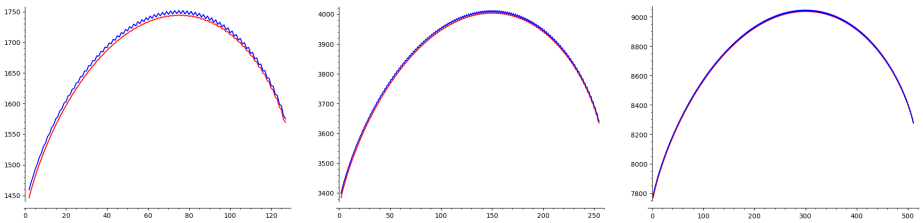
An instance for B_2. Recall from the proof of Theorem 3.4 that $B_2 = \max_{i,\,\mathcal{S}} |n! \cdot \prod_{j \in \mathcal{S}\setminus\{i\}} (-j)/(i-j)|$. We set $i = n - \lceil t/2 \rceil$ and choose $\mathcal{S} \setminus \{i\} = \{\, i-k : 1 \le k < \lfloor t/2 \rfloor \,\} \cup \{\, i+k : 1 \le k \le \lceil t/2 \rceil \,\}$. This selects the $t-1$ interpolation points so that they symmetrically surround i, to maximize the numerator while minimizing the denominator.

An instance for B_3. Recall that $B_3 = \max_{i,\,\mathcal{S}^*} |n! \cdot \prod_{j \in \mathcal{S}^*\setminus\{0\}} (i-j)/(-j)|$. We set $i = n$ and choose $\mathcal{S}^* \setminus \{0\} = [t-1]$. This choice maximizes the bound by selecting i as large as possible to maximize the numerator, while taking the elements of $\mathcal{S}^* \setminus \{0\}$ as small as possible to minimize the denominator.

We compare the theoretical bounds with $B_2 \cdot B_3$ for (a) $n = 128$, (b) $n = 256$, and (c) $n = 512$. The results are plotted on a logarithmic scale in Figure 8. We observe that the empirical values are remarkably close to our analytic bound, which suggests that our bound is tight (up to a small constant factor) in the tested parameter regimes.

Monomial Interpolation Set (Section 3.7). To study the tightness of the trigonometric bound from Corollary 3.9, the Clausen bound from Corollary 3.10, and the quadratic bound from Corollary 3.11 for the monomial interpolation set, we construct explicit instances that achieve worst-case values for B_2 and B_3. We fix $n = 2N$ for ease of comparison.

An instance for B_2. Recall that $B_2 = \max_{i,\,\mathcal{S}} \|2^{\lceil \log t \rceil} \prod_{j \in \mathcal{S}\setminus\{i\}} 1/(x^{i-j} - 1)\|_1$. An exact maximization over all $(i, \mathcal{S})$ is infeasible with exhaustive search for the parameter ranges of interest. Instead, we select a candidate motivated by the



(a) $n = 128$ (b) $n = 256$ (c) $n = 512$

Fig. 8: **(Integers)** Theorem 3.4 bound (blue) for $\log(B_2 \cdot B_3)$ and empirical lower bound (red).

analysis in Theorem 3.8.[11] For the sake of simplicity, we abuse notation and identify user k with the interpolation point x^{k-1} (and recall that $x^{-k} = x^{2N-k}$ for all k). Concretely, we take i corresponding to $x^0 = 1$ (i.e., $i = 1$) and choose $\mathcal{S}$ corresponding to the t monomials whose exponents are closest to 0:

$$\mathcal{S} = \begin{cases} \{x^0, x^{\pm 1}, x^{\pm 2}, \ldots, x^{\pm(\tau-1)}, x^{\pm\tau}\} & \text{for odd } t \ , \\ \{x^0, x^{\pm 1}, x^{\pm 2}, \ldots, x^{\pm(\tau-1)}, x^{\tau}\} & \text{for even } t \ , \end{cases}$$

where $\tau = \lfloor t/2 \rfloor$. With this choice, the factors occur in $\pm k$ pairs, with one unpaired factor when t is even, and up to multiplication by a monomial unit which does not affect the L_1-norm, we obtain:

$$C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S}\to 0} = 2^{\lceil \log t \rceil} \prod_{k\in[\tau]} (1 - x^k)^{-2} \ ,$$

where the last term of the product is just $(1 - x^\tau)^{-1}$ if t is even.

An instance for B_3. Recall that $B_3 = \max_{i,\, \mathcal{S}^*} \| \prod_{j\in\mathcal{S}^*\setminus\{0\}} (1 - x^{i-j}) \|_1$. As in the case of B_2, an exact maximization over all $(i, \mathcal{S}^*)$ is infeasible with exhaustive search, so we select a candidate motivated by the analysis in Theorem 3.8. We adopt the same worst-case configuration as in the embedding analysis by fixing i corresponding to x^N (i.e., $i = N + 1$) and taking

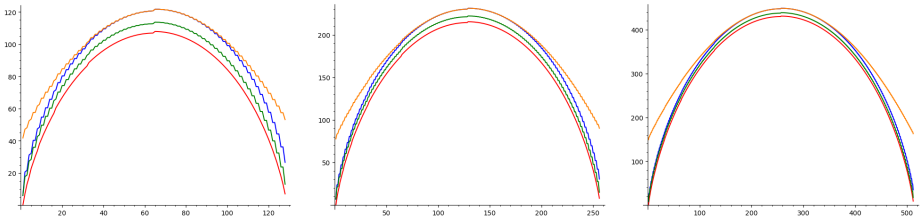
$$\mathcal{S}^* = \begin{cases} \{0\} \cup \{x^k : 0 \le k < \tau\} \cup \{x^{2N-k} : 1 \le k \le \tau\} & \text{for odd } t \ , \\ \{0\} \cup \{x^k : 0 \le k < \tau\} \cup \{x^{2N-k} : 1 \le k < \tau\} & \text{for even } t \ , \end{cases}$$

where $\tau = \lfloor t/2 \rfloor$. With this choice, each Lagrange factor $(1 - x^{i-j})$ has exponent $i - j \in \{N - k,\, N + k\}$ for $k \le \tau$. Up to multiplication by a monomial unit which does not affect the L_1-norm, we obtain

$$\lambda_0^{\mathcal{S}^*\to x^{i-1}} = \prod_{k\in[\tau]} (1 - x^{N-k})(1 - x^{N+k}) \ ,$$

where the last paired term is replaced by the single factor $(1 - x^{N-\tau})$ if t is even.

[11] Since $\|\sigma(f)\|_\infty \le \|f\|_1 \le \sqrt{N}\, \|\sigma(f)\|_\infty$ for $f \in R$ by Lemma 2.3, the two quantities $\|f\|_1$ and $\|\sigma(f)\|_\infty$ are comparable up to a $\sqrt{N}$ factor. Hence, up to this factor, maximizing $\|\sigma(f)\|_\infty$ is a reasonable approach to maximize $\|f\|_1$.



(a) $n = 128$ (b) $n = 256$ (c) $n = 512$

Fig. 9: **(Monomials)** Corollary 3.9 trigonometric bound (green), Corollary 3.10 Clausen bound (blue) for $\log(B_2 \cdot B_3)$, Corollary 3.11 quadratic bound (orange) and empirical lower bound (red).

We compare the theoretical bounds on $B_2 \cdot B_3$ with the concrete instantiations for (a) $n = 128$, (b) $n = 256$ and (c) $n = 512$. The empirical curves are generated by directly evaluating the explicit configurations described earlier. We then evaluate these empirical values against the trigonometric, Clausen, and quadratic bounds (Corollaries 3.9 to 3.11).

As illustrated in Figure 9, all four curves exhibit a similar overall trajectory, although a visible gap remains between the empirical values and the upper bounds. Moreover, as n increases, the *relative* gap among the three upper bounds—the trigonometric, Clausen, and quadratic bounds—narrows. This suggests that the Clausen bound becomes increasingly tight for larger ring degrees. The quadratic bound also becomes tighter when t is near the middle range, while it tends to be looser near the extreme values of t. Figure 9 also shows that the empirical curve nearly converges to the trigonometric and Clausen bounds, indicating that the gap is already small for the plotted values of n.

Comparison with [BFM$^+$25,CLW25]. We now compare our bounds on the quantity $\log(B_2 \cdot B_3)$ with those from prior works [BFM$^+$25,CLW25]. For the integer interpolation set, we use the bound obtained by multiplying the individual bounds on B_2 and B_3 given in Theorem 3.4. For the monomial interpolation set, we use Theorem 5.3.

Overall comparison. As illustrated in Figure 10, our trigonometric bound for the monomial interpolation set consistently yields the tightest upper bounds on $\log(B_2 \cdot B_3)$. Among the four analyses evaluated, it is the only one that remains uniformly low across the entire (n, t)-plane, thereby ensuring the smallest admissible ciphertext modulus q throughout the plotted region. For a fixed $n = 512$, Figure 11 plots the bounds of [BFM$^+$25] and our trigonometric bound as a function of t, showing a consistent gap that is particularly pronounced near the endpoints of the threshold range.

Behavior near the endpoints. Unlike the bounds of [BFM$^+$25,CLW25], which increase monotonically with t, our bounds for a value of t and the corresponding $n - t$ are (almost) the same. As a result, the advantage of our bounds is

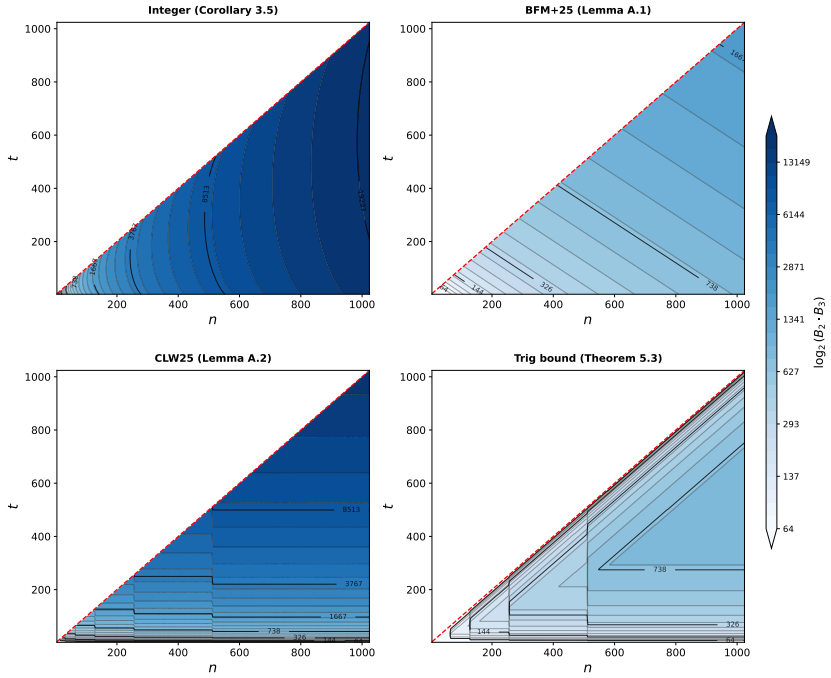


Fig. 10: **Heatmaps.** Upper bounds on $\log(B_2 \cdot B_3)$ over the (n, t) plane for four analyses: our bound for the *integer interpolation set* (Corollary 3.5); the prior bound of [BFM+25] (Lemma A.1); the prior bound of [CLW25] (Lemma A.2); and our trigonometric bound for the *monomial interpolation set* (Theorem 5.3).

most pronounced near both endpoints of the threshold range, as illustrated in Table 1: at $t = 500$, our trigonometric bound equals 86, whereas the corresponding bounds of [BFM+25] and [CLW25] are respectively 900 and 7524, yielding reductions of roughly 800 bits relative to [BFM+25] and more than 7400 bits relative to [CLW25].

Midpoint regime ($t \approx n/2$). The midpoint $t = 256$ represents the most pessimistic regime for our analysis, as the (almost) symmetric bounds are expected to attain their maximum near this point. Nevertheless, as shown in Table 1, at $t = 256$ our trigonometric bound is 438, compared to 656 in [BFM+25] and 3862 in [CLW25]. Thus, even at this most unfavorable point for our bound, the trigonometric bound improves $\log(B_2 \cdot B_3)$ by 218 bits over [BFM+25] and by 3424 bits over [CLW25].

Integer interpolation set. The integer interpolation set yields upper bounds that are larger by several orders of magnitude than those of monomial interpolation sets and exhibits a convex dependence on t, making it unsuitable in practice, as illustrated by $\log(B_2 \cdot B_3) = 7918$ at $t = 12$ and 9016 at $t = 256$ in Table 1.

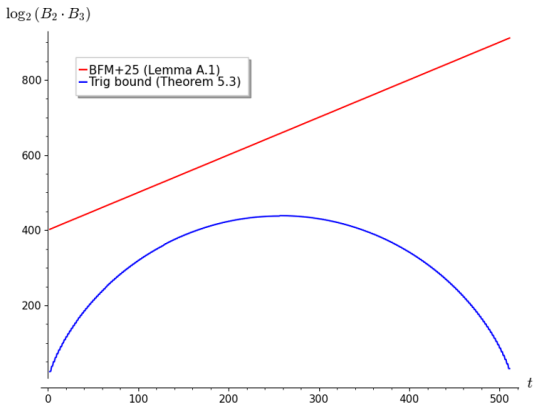


Fig. 11: Comparison of $\log(B_2 \cdot B_3)$ as a function of the threshold t for $n = 512$: the bound from [BFM+25] (Lemma A.1, red) and our trigonometric bound (Theorem 5.3, blue).

Global behavior on the (n, t)-plane. As illustrated in Figure 10, while all four bounds depend on both n and t, their qualitative shapes and scaling differ significantly. Our integer bound and our trigonometric monomial bound share a similar symmetric profile: for a fixed n, both bounds are smaller near the extremes of the threshold range and peak in the intermediate regime of t.

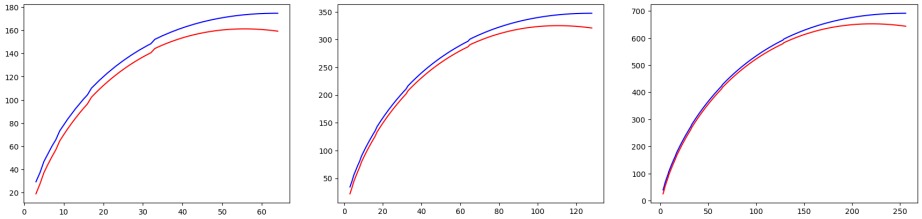
6.2 Second Construction: Tightness and Comparison

We construct reconstruction and simulation sets $\mathcal{S}$ and $\mathcal{S}_{\mathsf{cor}}$ that lead to large values of B_2 and B_3, respectively, and compare the resulting quantity $B_2 \cdot \widetilde{B}_3 + B_2 \cdot B_3$, which governs the modulus bound (4), with the bound (8) of Corollary 4.5. As in Section 6.1, a worst configuration for B_2 can be combined with a worst configuration for B_3.

Monomial Interpolation Set (Section 4.5). To study the tightness of the bound (8) for the monomial interpolation set, we construct explicit instances that achieve high values for B_2 and B_3. We fix $n = 2N$, $C_{\mathsf{dec}} = 4^{\lceil \log t \rceil}$, and $C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, and, as before, identify user k with the interpolation point x^{k-1}.

An instance for B_2. Recall that $B_2 = \max_{i,\, \mathcal{S}} \|C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0}\|_1$ with $C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, which coincides with the quantity B_2 of the first construction. We therefore reuse the instance for B_2 above, i.e., i corresponding to x^0 and $\mathcal{S}$ corresponding to the t monomials whose exponents are closest to 0.

An instance for B_3. Recall that $B_3 = \max_{i,\, \ell,\, \mathcal{S}^*} \|(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_\ell^{\mathcal{S}^* \to x^{i-1}}\|_1$ with $C_{\mathsf{dec}}/C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$, where the maximum is now also taken over the index $\ell \in \mathcal{S}^*$. As in the first construction, an exact maximization over all $(i, \ell, \mathcal{S}^*)$ is infeasible with exhaustive search, so we select candidates motivated by the analysis in Theorem 4.4. Following the case distinction $\ell = 0$ and $\ell \in \mathcal{S}_{\mathsf{cor}}$ in its proof,



(a) $n = 128$ (b) $n = 256$ (c) $n = 512$

Fig. 12: **(Monomials, second construction)** Corollary 4.5 bound (blue) for $\log(B_2 \cdot \widetilde{B}_3 + B_2 \cdot B_3)$ and empirical lower bound (red).

we evaluate two instances. For $\ell = 0$, we have $\lambda_0^{\mathcal{S}^* \to x^{i-1}} = \pm \prod_{j \in \mathcal{S}_{\mathsf{cor}}} (1 - x^{i-j})$, and we take the instance for B_3 of the first construction, scaled by $2^{\lceil \log t \rceil}$. For $\ell \in \mathcal{S}_{\mathsf{cor}}$, we fix ℓ corresponding to x^0 (i.e., $\ell = 1$) and i corresponding to x^N (i.e., $i = N + 1$), and choose the remaining $t - 2$ elements of $\mathcal{S}_{\mathsf{cor}}$ as the monomials whose exponents are closest to 0:

$$\mathcal{S}_{\mathsf{cor}} \setminus \{\ell\} = \begin{cases} \{x^{\pm 1}, x^{\pm 2}, \ldots, x^{\pm(\tau-1)}, x^{\tau}\} & \text{for odd } t \ , \\ \{x^{\pm 1}, x^{\pm 2}, \ldots, x^{\pm(\tau-1)}\} & \text{for even } t \ , \end{cases}$$

where $\tau = \lfloor t/2 \rfloor$. With this choice, the denominator factors $(1 - x^{\ell - j})$ are those of the instance for B_2, while the numerator factors $(1 - x^{i-j})$ have exponents $i - j \in \{N - k,\ N + k\}$ as in the instance for B_3 of the first construction. Up to multiplication by a monomial unit which does not affect the L_1-norm, we obtain

$$(C_{\mathsf{dec}}/C_{\mathsf{sim}}) \cdot \lambda_\ell^{\mathcal{S}^* \to x^N} = 2^{\lceil \log t \rceil} \prod_{k \in [\tau - 1]} \frac{(1 - x^{N-k})(1 - x^{N+k})}{(1 - x^k)^2} \ ,$$

with an additional factor $(1 - x^{N-\tau})/(1 - x^{\tau})$ if t is odd. For every evaluated value of t, the second instance gives the larger L_1-norm, and we use it as the constructed value of B_3.

We compare the bound (8) on $B_2 \cdot \widetilde{B}_3 + B_2 \cdot B_3$ with the constructed instances for (a) $n = 128$, (b) $n = 256$ and (c) $n = 512$, over the range $3 \le t \le N$. The empirical curves are obtained by directly evaluating the explicit configurations described above, and Figure 12 plots $\log_2\big(B_2 \cdot (2^{\lceil \log t \rceil} + B_3)\big)$ against the bound (8).

As illustrated in Figure 12, the bound (8) lies between 7.53 and 15.47 bits above the constructed value for $n = 128$, between 8.88 and 26.62 bits for $n = 256$, and between 10.22 and 47.94 bits for $n = 512$. This gap comes from the second summand $B_2 \cdot B_3$, which dominates the sum: in all evaluated cases, the constructed value of B_3 exceeds $\widetilde{B}_3 = 2^{\lceil \log t \rceil}$ by more than five bits. The gap is largest at $t = N$, since the proof of Theorem 4.4 bounds each numerator factor $1 - x^{i-j}$ by 2 in absolute value, whereas in the constructed instance these factors have magnitude $2\cos(\pi k/(2N))$, which drops to $\sqrt{2}$ as k approaches $N/2$.

Comparison with [EY24]. We now compare the modulus size and the per-party storage of our second construction with those of [EY24]. For our construction, we consider the spaced monomial interpolation set $\mathcal{I}^{\star}_{\mathrm{mon}}(n', 0)$ with the choice $c = 0$ and $n' = 2^{\lceil \log \max\{n, 2t\} \rceil}$ of Theorem 5.5, and let $Q(n, t)$ denote the right-hand side of (4) after bounding $\widetilde{B}_2 \leq B_2 \widetilde{B}_3$ and substituting the estimates of Corollary 5.4; for odd $q > Q(n, t)$, the second construction is correct and strongly simulation-secure under the assumptions of Theorems 4.1 and 4.2. For [EY24], we use the modulus $\log_2 q = 10.4 \log_2 n + \lambda$ of Corollary B.1 (Appendix B). Throughout, we fix $N = 2^{14}$, $B_{\mathsf{eval}} = 2^{40}$, $B_{\chi} = 6$, $\lambda = 128$, and $p = 257$.

n	$t = n/4$	$t = n/2$	$t = 3n/4$
16	212	219	241
32	233	243	286
64	273	289	372
128	350	378	542
256	500	553	878
512	798	899	1547
1024	1391	1589	2881

Table 3: Values of $\lceil \log_2 Q(n, t) \rceil$, the number of modulus bits sufficient for the second construction, on the spaced monomial interpolation set $\mathcal{I}^{\star}_{\mathrm{mon}}(n', 0)$ with $n' = 2^{\lceil \log \max\{n, 2t\} \rceil}$, at $N = 2^{14}$, $B_{\mathsf{eval}} = 2^{40}$, $B_{\chi} = 6$, $\lambda = 128$, and $p = 257$.

Modulus size of our construction. Table 3 lists $\lceil \log_2 Q(n, t) \rceil$ for $n \in \{16, 32, \ldots, 1024\}$ and $t \in \{n/4, n/2, 3n/4\}$. For a fixed n, $\log_2 Q(n, t)$ grows linearly in t, and for a fixed ratio t/n it grows linearly in n.

Per-party storage model. In [EY24], each party stores both FHE key shares and KHPRF keys, one component of each per row of the $\{0, 1\}$-LSSS assigned to it. With the monotone-majority LSSS of row dimension $\ell = O(n^{5.2})$ (Appendix B), each party is assigned $O(\ell/n) = O(n^{4.2})$ rows; for the concrete estimates below, we normalize this count to $n^{4.2}$, giving $2n^{4.2}$ stored elements per party. Our construction stores only sk_i and s_i, hence two ring elements per party. For E stored ring elements per party ($E = 2n^{4.2}$ for [EY24] and $E = 2$ for ours), we estimate the per-party storage as

$$\mathrm{size}(E, q) = E \cdot N \cdot \lceil \log_2 q \rceil / 8 \quad \text{bytes.}$$

Comparison. Table 4 reports the modulus size and the per-party storage of both constructions at the central threshold $t = \lceil n/2 \rceil$, and Figure 13 plots the per-party storage as n varies. The two constructions exhibit a clear trade-off. The construction of [EY24] has the smaller modulus: its $\{0, 1\}$-reconstruction

		[EY24]		Ours	
n	t	$\log_2 q$	storage	$\log_2 q$	storage
8	4	160	4.1 GB	205	840 KB
16	8	170	79 GB	219	897 KB
32	16	180	1.5 TB	243	995 KB
64	32	191	30 TB	289	1.18 MB
128	64	201	583 TB	378	1.55 MB
256	128	212	11 PB	553	2.27 MB
512	256	222	218 PB	899	3.68 MB
1024	512	232	4.2 EB	1589	6.51 MB

Table 4: Number of modulus bits $\lceil \log_2 q \rceil$ and the resulting per-party storage at $t = \lceil n/2 \rceil$, $N = 2^{14}$, $\lambda = 128$. For ours, q is the bound $Q(n, t)$ of Table 3; for [EY24], $\log_2 q$ is the estimate $10.4 \log_2 n + \lambda$ of Corollary B.1, rounded up to an integer. The storage columns give the per-party storage $E \cdot N \cdot \lceil \log_2 q \rceil / 8$ in bytes, with $E = 2 \cdot n^{4.2}$ for [EY24] and $E = 2$ for ours.

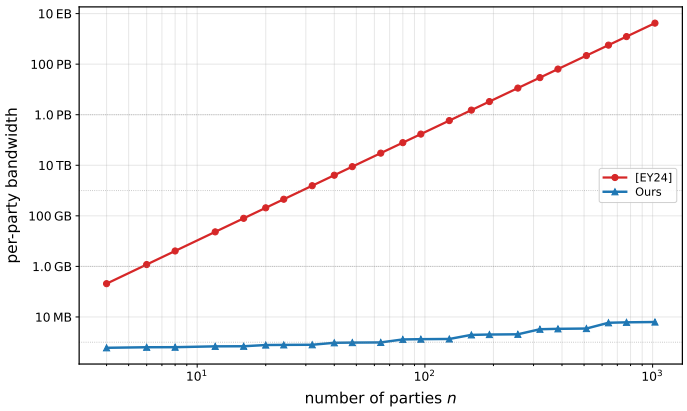


Fig. 13: Per-party storage versus n at $t = \lceil n/2 \rceil$, $N = 2^{14}$, $\lambda = 128$. The $2 \cdot n^{4.2}$ element-count blowup of [EY24] dominates our $\Theta(n)$ modulus growth at every sampled n, and the gap widens by roughly a factor of 10^4 per decade of n.

coefficients keep $\log_2 q$ logarithmic in n, from 160 bits at $n = 8$ to 232 bits at $n = 1024$, whereas our modulus grows linearly in t, from 205 to 1589 bits over the same range. This is however outweighed by the $n^{4.2}$-scale gap in the number of stored ring elements. Already at $n = 16$, the per-party storage drops from 79 GB in [EY24] to 897 KB in our construction, a factor of about 8.9×10^4; at $n = 1024$, despite our larger modulus, it is 6.5 MB compared with 4.2 EB for [EY24]. As illustrated in Figure 13, the gap widens by roughly a factor of 10^4 per decade of n.

References

AJLA+12. G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs. Multiparty computation with low communication, computation and interaction via threshold FHE. In *EUROCRYPT*, 2012.

AL21. M. R. Albrecht and R. W. F. Lai. Subtractive sets over cyclotomic rings: Limits of Schnorr-like arguments over lattices. In *CRYPTO*, 2021.

BBN+25. D. Boneh, B. Bünz, K. Nayak, L. Rotem, and V. Shoup. Context-dependent threshold decryption and its applications. In *ASIACRYPT*, 2025.

BFM+25. Zvika Brakerski, Offir Friedman, Avichai Marmor, Dolev Mutzari, Yuval Spiizer, and Ni Trieu. Threshold FHE with efficient asynchronous decryption. Cryptology ePrint Archive, Paper 2025/712, 2025.

BGG+18. D. Boneh, R. Gennaro, S. Goldfeder, A. Jain, S. Kim, P. M. R. Rasmussen, and A. Sahai. Threshold cryptosystems from threshold fully homomorphic encryption. In *CRYPTO*, 2018.

BGV12. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *ITCS*, 2012.

BLMR15. D. Boneh, K. Lewi, H. Montgomery, and A. Raghunathan. Key homomorphic PRFs and their applications. *IACR Cryptol. ePrint Arch., Report 2015/220*, 2015. Full version of *CRYPTO 2013*.

Bra12. Z. Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In *CRYPTO*, 2012.

BS23. K. Boudgoust and P. Scholl. Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus. In *ASIACRYPT*, 2023.

CKKS17. J. H. Cheon, A. Kim, M. Kim, and Y. S. Song. Homomorphic encryption for arithmetic of approximate numbers. In *ASIACRYPT*, 2017.

CKL24. W. Cho, J. Kim, and C. Lee. (In)security of threshold fully homomorphic encryption based on Shamir secret sharing. IACR eprint, 2024. Available at `https://eprint.iacr.org/2024/1858`.

CLW25. V. Cini, R. W. F. Lai, and I. K. Y. Woo. Pilvi: Lattice threshold PKE with small decryption shares and improved security. In *ASIACRYPT*, 2025.

CPS26. F. Colin de Verdière, A. Passelègue, and D. Stehlé. On threshold fully homomorphic encryption with synchronized decryptors. IACR eprint, 2026. Available at `https://eprint.iacr.org/2026/031`.

EY24. E. Ebrahimi and A. Yadav. Strongly secure universal thresholdizer. In *Advances in Cryptology – ASIACRYPT 2024*, volume 15486 of *Lecture Notes in Computer Science*, pages 207–239. Springer, 2024.

Feh98. S. Fehr. Span programs over rings and how to share a secret from a module. Master's thesis, ETH Zürich, 1998. Available at `https://crypto.ethz.ch/publications/Fehr98.html`.

FV12. J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR eprint, 2012. Available at `https://eprint.iacr.org/2012/144`.

LMSS22. B. Li, D. Micciancio, M. Schultz-Wu, and J. Sorrell. Securing approximate homomorphic encryption using differential privacy. In *CRYPTO*, 2022.

MBH23. Christian Mouchet, Elliott Bertrand, and Jean-Pierre Hubaux. An efficient threshold access-structure for RLWE-based multiparty homomorphic encryption. *Journal of Cryptology*, 36(2):10, 2023.

MS77. D. A. Marcus and E. Sacco. *Number fields*. Springer, 1977.

MTBH21. C. Mouchet, J. Troncoso-Pastoriza, J.-P. Bossuat, and J.-P. Hubaux. Multiparty homomorphic encryption from ring-learning-with-errors. *PETs*, 2021.

A Detailed Comparison to Prior Works

The interpolation points $\{0\} \cup \{x^i\}_{0 \le i < 2N}$ suggested in [AL21] and subsets thereof have been considered in two recent works [BFM+25,CLW25]. For the sake of comparison, we recall their analyses in our notational framework.

Analysis of [BFM+25]. The authors of [BFM+25] consider the interpolation points $\alpha_0 = 0$ and $\alpha_{i,b} = (-1)^b x^i$ for $b \in \{0,1\}$ and $i \in [n/2]$, where the number n of decryptors is divisible by six and satisfies $n < N$ in their stated parameter range.[12] These interpolation points are contained in $\{0\} \cup \{x^i\}_{0 \le i < 2N}$ and are in particular pairwise distinct if $n \le 2N$.

In the following result, the first two bounds come from [BFM+25, Corollary 1] and the third one is given in [BFM+25, Lemma 4]. As explained in Section 3, the Lagrange reconstruction coefficients should be taken over R_q rather than over K as in [BFM+25]. The denominator-clearing analysis from [BFM+25, Theorem 1] carries over.

Lemma A.1. *Let $6 \mid n$ and $1 \le t \le n < N$. The following bounds hold for $\mathcal{I}_{\mathrm{bfm}} = \{0\} \cup \{(-1)^b x^i : b \in \{0,1\}, 1 \le i \le n/2\}$ with $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2 \cdot \prod_{e \in [\frac{n}{2}]} (x^{2e} - 1) \cdot \prod_{e \in [\frac{n}{6}]} (x^{2e} - 1)$:*

$$\|C_{\mathsf{dec}} \bmod q\|_1 \le \frac{n^2}{3} \cdot 1.2^{\frac{2n}{3}} \ ,$$

$$\max_{\substack{\mathcal{S} \in \mathbb{A}_{n,t} \\ (i,b) \in \mathcal{S}}} \left\| \left(C_{\mathsf{sim}} \cdot \lambda_{(i,b)}^{\mathcal{S} \to 0} \right) \bmod q \right\|_1 \le \frac{n^2}{3} \cdot 2^{\frac{3}{4}n} \ ,$$

$$\max_{\substack{\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\text{c-max}} \\ (i,b) \notin \mathcal{S}_{\mathsf{cor}}}} \left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\{0\} \cup \mathcal{S}_{\mathsf{cor}} \to (-1)^b x^i} \right) \bmod q \right\|_1 \le 2^t \ .$$

Overall, this result imposes that q is larger than $\approx 2^{t+\lambda+3n/4}$.

Analysis of [CLW25]. The authors of [CLW25] consider any subset of size $n+1$ of $\{0\} \cup \{x^i\}_{0 \le i < 2N}$ that contains 0.[13] In their concrete instantiation, they consider a subset $\{0\} \cup \{x^{i \cdot 2N/n}\}_{0 \le i < n}$ for n dividing $2N$.

The following result is adapted from [CLW25, Lemma 3]. The first (resp. second) bounded quantity corresponds to ρ (resp. $\gamma C_{\mathsf{dec}}/C_{\mathsf{sim}}^2$) in the latter work. Note that [CLW25] considered the L_2-norm of the canonical embedding, whereas we consider the L_1-norm, explaining a loss of a factor $\sqrt{N}$ (by Lemma 2.3). Further, as explained in Section 3, the Lagrange reconstruction coefficients should be taken over R_q rather than over K as in [CLW25]. The denominator-clearing analysis from [CLW25, Lemma 1] (borrowed from [AL21, Theorem 1]) carries over.

[12] The ring degree and the number of parties are respectively denoted n and N in [BFM+25], i.e., these notations are swapped compared to ours.

[13] The ring degree and the number of parties are respectively denoted $2\mathfrak{f}$ and K in [CLW25]

Lemma A.2 (Adapted from [CLW25, Lemma 3]). *If $t \leq n \leq 2N$, the following bounds hold for any subset of size $n+1$ of $\{0\} \cup \{x^i\}_{0 \leq i < 2N}$ containing 0, with $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 2^{\lceil \log t \rceil}$:*

$$\max_{\substack{\mathcal{S} \in \mathbb{A}_{n,t} \\ i \in \mathcal{S}}} \left\| \left(C_{\mathsf{sim}} \cdot \lambda_i^{\mathcal{S} \to 0} \right) \bmod q \right\|_1 \leq C_{\mathsf{sim}} \cdot t \cdot \sqrt{N} \cdot \left(\frac{N}{\sqrt{2}} \right)^{t-1} ,$$

$$\max_{\substack{\mathcal{S}_{\mathsf{cor}} \in \mathbb{A}_{n,t}^{\text{c-max}} \\ i \notin \mathcal{S}_{\mathsf{cor}}}} \left\| \left(\frac{C_{\mathsf{dec}}}{C_{\mathsf{sim}}} \cdot \lambda_0^{\{0\} \cup \mathcal{S}_{\mathsf{cor}} \to x^{i-1}} \right) \bmod q \right\|_1 \leq t \cdot \sqrt{n} \cdot \sqrt{N} \cdot \left(\frac{N}{\sqrt{2}} \right)^{t-1} .$$

Overall, this imposes that q is larger than $\approx (N/\sqrt{2})^{2t} \cdot 2^{\lambda}$. When taking a subfield of degree $n/2$ as suggested in [CLW25, Section 7] (assuming that n divides $2N$), we obtain that q should be no smaller than $\approx (n/(2\sqrt{2}))^{2t} \cdot 2^{\lambda}$.

Note that Lemma A.2 applies to the interpolations considered in [BFM+25], while the converse does not hold a priori. The analysis from [BFM+25] is specialized to a particular choice of n values in $\{x^i\}_{0 \leq i < 2N}$ as

$$\{x^i\}_{0 < i < \frac{n}{2}} \cup \{x^i\}_{N < i < N + \frac{n}{2}},$$

whereas that of [CLW25] works for any subset of $\{x^i\}_{0 \leq i < 2N}$. Asymptotically, we note that the bound from [BFM+25] outperforms that of [CLW25] specialized to the degree-$n/2$ subfield choice of interpolation points, when t is sufficiently large compared to $n/\ln n$.

B Analysis of [EY24]

We now explain the parameter constraints of the strongly secure threshold-FHE construction of [EY24] used in our comparison. Unlike the Shamir-based constructions analyzed above, [EY24] uses a $\{0,1\}$-linear secret sharing scheme together with an almost key-homomorphic PRF to mask partial decryptions. Its reconstruction coefficients are therefore either 0 or 1, so no denominator-clearing factor is needed. In the notation of our framework, this corresponds to $C_{\mathsf{dec}} = C_{\mathsf{sim}} = 1$.

Let ℓ denote the row dimension of the $\{0,1\}$-LSSS used in [EY24], and let δ be the error bound of the almost key-homomorphic PRF. The row dimension ℓ counts how many share components may be summed during reconstruction, while $\delta\ell$ bounds the residual error accumulated when the almost key-homomorphic PRF masks are combined. Accordingly, [EY24] uses two flooding widths: one for the FHE decryption error and one for the PRF residual error.

We now restate the resulting parameter constraints of [EY24].

Corollary B.1 (Parameter constraints of [EY24], reformulated). *Assume the setting of [EY24], with FHE evaluation-error bound B_{eval}, $\{0,1\}$-LSSS row dimension ℓ, and a δ-almost key-homomorphic PRF. Correctness and strong*

simulation security are obtained under the flooding conditions $B_{\mathsf{sm}} \geq B_{\mathsf{eval}} \cdot 2^{\lambda}$ *and* $E_{\mathsf{sm}} \geq \delta\ell \cdot 2^{\lambda}$*, together with the correctness condition*

$$B_{\mathsf{eval}} + \delta\ell + \ell B_{\mathsf{sm}} + \ell E_{\mathsf{sm}} < q/4 \ .$$

Consequently, it suffices to choose q *so that*

$$\frac{q}{4} > B_{\mathsf{eval}} + \delta\ell + \ell B_{\mathsf{eval}} \cdot 2^{\lambda} + \delta\ell^2 \cdot 2^{\lambda} \ .$$

For the $\{0,1\}$*-LSSS instantiated from the monotone-majority formula of [BGG*$^{+}$*18, Section 5.4], we use* $\ell = O(n^{5.2})$*. Hence, with the hidden constants normalized to one for the concrete comparison and with the remaining FHE- and PRF-dependent terms fixed with respect to* n*, the dominant* ℓ^2 *term gives*

$$\log_2 q = 10.4 \log_2 n + \lambda$$

up to fixed additive terms, as used in Table 4.