

Numerical and Algebraic Evaluation of Chebyshev Polynomial Representations for Ring-LWE-Related Polynomial Arithmetic

Mohammad Asif

24230047000100@paruluniversity.ac.in

Parul University

Dr Sanjay Agal

Parul University

Article

Keywords:

Posted Date: October 26th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11270790/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Numerical and Algebraic Evaluation of Chebyshev Polynomial Representations for Ring-LWE-Related Polynomial Arithmetic

Mohammad Asif^{1*}, Dr Sanjay Agal²

¹Ph.D. Scholar in Computer Science and Engineering, Parul University, Vadodara, India
2423004700010@paruluniversity.ac.in

²Head of Artificial Intelligence and Data Science Department, Parul University, Vadodara, India
sanjayagal@yahoo.com

* Corresponding author: Mohammad Asif *

Abstract—This paper presents an extended numerical and algebraic evaluation of Chebyshev-polynomial representations for polynomial arithmetic associated with Ring Learning With Errors (RLWE). The central methodological principle is to separate a change of coordinates from a change of cryptographic problem. The underlying negacyclic ring is retained as $R_q = \mathbb{Z}_q[x]/(x^N + 1)$, while Chebyshev polynomials are investigated as a representation and computational basis. A staged experimental programme, EXP01–EXP27, evaluates exact polynomial identities, basis transformation, modular invertibility, multiplication equivalence, common-basis RLWE comparisons, canonical embeddings, transformation conditioning, numerical evaluation, repeated multiplication, structure-constant growth, independent high-precision validation, robustness, parameter sensitivity, and a final consolidated benchmark. At degree eight, the Chebyshev product identity is verified for all tested basis pairs and modular basis conversion is exact in the tested setting. At larger dimensions, however, the power-to-Chebyshev transformation becomes increasingly ill-conditioned: the measured condition number grows from approximately 6.34 at $N = 4$ to 3.47×10^{11} at $N = 32$. Independent high-precision experiments show that numerical behavior is governed by the complete computational pathway rather than by the polynomial basis alone. At $N = 64$ and multiplication depth eight, the final benchmark reports mean relative errors of approximately 7.39×10^5 for a structure-constant pathway, 9.89 for a conversion pathway, and 6.54×10^{-1} for an evaluation/interpolation pathway. The study therefore does not establish reduced RLWE noise, improved cryptographic security, or a superior production implementation. Instead, it establishes a reproducible representation-level result: Chebyshev coordinates can encode the same underlying algebra, but their numerical usefulness depends critically on dimension, conditioning, multiplication depth, and algorithmic realization.

Index Terms—Ring Learning With Errors, Chebyshev polynomials, polynomial bases, numerical stability, negacyclic rings, canonical embedding, basis transformation, post-quantum cryptography.

I. INTRODUCTION

Lattice-based cryptography is a major research direction in post-quantum cryptography because learning-with-errors assumptions connect efficient cryptographic constructions with the geometry of high-dimensional lattices. The original worst-case-to-average-case programme for lattice problems and its learning-with-errors formulations established the conceptual

basis for a large body of subsequent work [1]–[4]. Ring-LWE (RLWE) introduces additional algebraic structure by replacing generic vectors with elements of polynomial rings. This structure can reduce arithmetic cost and enables compact constructions, but it also makes the exact representation of polynomial elements an important implementation concern [5]–[8].

The standard computational object considered in this study is the negacyclic quotient

$$R_q = \mathbb{Z}_q[x]/(x^N + 1), \quad (1)$$

where q is an odd modulus and N is the polynomial dimension. In this setting, two coordinate systems can describe the same algebraic element. The conventional power basis uses $1, x, x^2, \dots, x^{N-1}$, whereas an alternative basis can be constructed from Chebyshev polynomials $T_0(x), T_1(x), \dots, T_{N-1}(x)$. The existence of a different coordinate system does not, by itself, alter the quotient ring, its ideals, its canonical embeddings, or its cryptographic hardness assumptions.

This distinction is the starting point of the present work. The research question is not whether replacing $x^N + 1$ with a Chebyshev polynomial automatically creates a secure cryptosystem. Such a claim would require a new and complete cryptographic analysis. Instead, the question is narrower: *when the same underlying algebraic object is represented using Chebyshev coordinates, how do exact arithmetic, coefficient representation, conditioning, and numerical error behave as dimension and multiplication depth increase?*

Chebyshev polynomials are a natural object for this investigation because they combine an explicit recurrence with a particularly simple product identity,

$$T_m(x)T_n(x) = \frac{1}{2} (T_{m+n}(x) + T_{|m-n|}(x)). \quad (2)$$

They also have a long history in numerical approximation, interpolation, and stable polynomial evaluation [9]–[11]. Numerical analysis has repeatedly shown that exact algebraic equivalence does not imply equivalent floating-point behavior: the basis, conditioning, evaluation scheme, and accumulation path can

all affect the observed error [12]–[17]. These observations make Chebyshev coordinates interesting for a controlled computational study even without making a cryptographic superiority claim.

The experimental programme was deliberately staged. EXP01–EXP07 establish polynomial identities, basis construction, modular arithmetic, and coefficient behavior. EXP08–EXP13 move to RLWE-related arithmetic and explicitly test whether coordinate-dependent quantities survive a common-basis comparison. EXP14–EXP17 investigate dimension scaling, canonical embedding, conditioning, and evaluation stability. EXP18–EXP23 examine repeated operations and fixed-dimensional multiplication pathways. EXP24–EXP27 provide independent high-precision validation, robustness, parameter sensitivity, and a consolidated benchmark. This progression is important because it prevents an observation at the coordinate level from being silently promoted into a statement about cryptographic noise or security.

The main contributions of this paper are therefore methodological and numerical. First, it gives an explicit algebraic framework for converting between power and Chebyshev coordinates while keeping the underlying RLWE-related ring fixed. Second, it separates representation-dependent coefficient magnitudes from common-basis quantities such as RLWE noise and canonical embedding norms. Third, it documents how transformation conditioning and direct structure constants grow with dimension. Fourth, it compares several computational pathways against independent high-precision references. Finally, it preserves the negative and superseded experimental results so that the final conclusions are auditable rather than selected only from successful trials.

II. BACKGROUND AND RELATED WORK

A. LWE, RLWE, and structured arithmetic

The security literature on lattice-based cryptography begins with constructions in which noisy linear relations are connected to hard lattice problems [1], [2]. Subsequent work developed worst-case hardness relationships and practical public-key encryption frameworks based on LWE and its variants [3], [18]. Ring-LWE transfers the learning-with-errors structure into polynomial rings, allowing multiplication and storage to be organized around polynomial operations [5], [6], [8]. The resulting algebraic structure is useful, but it also introduces additional assumptions about the chosen ring and its arithmetic.

The distinction between a ring representation and the security of the resulting problem is particularly important. Work on concrete LWE hardness shows that security depends on dimension, modulus, error distribution, secret distribution, and the attack model rather than on an informal measure of coefficient size alone [19]. Likewise, the study of lattice reduction and BKZ demonstrates that concrete estimates depend on the geometry of the instantiated lattice and the algorithmic cost model [20]. Module-lattice constructions and standardized post-quantum systems further illustrate that algebraic structure, implementation details, and security arguments must be analyzed together but not conflated [21]–[24].

This paper consequently adopts the conservative model in which the quotient ring in Eq. (1) remains unchanged.

Chebyshev coordinates are introduced only after the underlying ring element has been defined. When a ciphertext or error polynomial is compared, the comparison is eventually performed in a common representation. This design follows the same general discipline emphasized in RLWE parameter-selection literature: first specify the mathematical problem, then analyze the chosen representation and implementation [25]–[27].

B. Polynomial bases and Chebyshev structure

The first-kind Chebyshev polynomials satisfy

$$T_0(x) = 1, \quad T_1(x) = x, \quad (3)$$

and the three-term recurrence

$$T_{k+1}(x) = 2xT_k(x) - T_{k-1}(x). \quad (4)$$

They also admit the trigonometric representation $T_k(\cos \theta) = \cos(k\theta)$. Equation (2) follows directly from the product-to-sum identity for cosine. The combination of recurrence, product structure, and well-developed evaluation algorithms makes the basis attractive for numerical experimentation.

However, a useful basis is not necessarily a well-conditioned coordinate system for every operation. In the power basis, high-degree monomials can lead to large intermediate values during evaluation. In a Chebyshev basis, recurrence-based evaluation such as Clenshaw’s algorithm can be much more stable in many approximation problems [10]–[12]. At the same time, converting a polynomial between bases can be ill-conditioned as degree increases. The experiments in this paper therefore treat the basis transformation, multiplication algorithm, and evaluation method as separate components.

The numerical-analysis literature provides several additional reasons for this separation. Barycentric interpolation can be highly stable under appropriate node choices [14], while rational barycentric schemes provide another family of interpolation procedures [15]. Other work studies singularity-free evaluation and stability at Chebyshev points [16], [17]. The three-term Chebyshev recursion itself has been analyzed for mixed forward-backward stability [28]. These results motivate testing actual computational pathways rather than assuming that all Chebyshev-based computations inherit the stability of a particular textbook algorithm.

C. Chebyshev-related cryptographic literature

Chebyshev polynomials have also appeared in cryptographic proposals, including work based on the claimed security of polynomial-related problems [29]. Such proposals are not interchangeable with the RLWE model studied here. In particular, the present work does not rely on a Chebyshev discrete-logarithm assumption or on a new hardness problem. The Chebyshev basis is used as a representation inside a fixed RLWE-related polynomial ring. This distinction is essential because an algebraically convenient polynomial basis does not automatically supply a cryptographic reduction.

III. RESEARCH QUESTIONS AND SCOPE

The study is organized around five research questions.

- 1) **RQ1: Algebraic validity.** Can Chebyshev coordinates represent the same polynomial-ring elements as the power basis with exact or modularly exact conversion in the tested parameter regimes?
- 2) **RQ2: Arithmetic equivalence.** When multiplication is implemented in Chebyshev coordinates and then mapped to a common basis, does it agree with conventional power-basis multiplication?
- 3) **RQ3: Representation versus cryptographic noise.** Do apparent changes in coordinate magnitudes persist when the same RLWE-related quantity is expressed in a common canonical representation?
- 4) **RQ4: Numerical scaling.** How do transformation conditioning, structure constants, evaluation error, and repeated-operation error change with dimension and multiplication depth?
- 5) **RQ5: Reproducibility.** Do independent high-precision, robustness, and parameter-sensitivity experiments reproduce the qualitative trends observed in the primary stress tests?

The scope is intentionally narrower than the design of a new post-quantum cryptosystem. No claim is made that a Chebyshev representation lowers RLWE noise, increases lattice hardness, reduces attack probability, or improves the security level of an existing standardized scheme. The experiments instead address representation-level algebra and numerical behavior. This scope also determines how results are reported: coordinate magnitudes are described as coordinate magnitudes, common-basis error is described as common-basis error, and numerical stability is not translated into a security claim.

IV. ALGEBRAIC MODEL

A. Degree-eight construction

For the degree-eight demonstration, define

$$\beta = \cos(\pi/16). \quad (5)$$

Then

$$T_8(\beta) = \cos(8\pi/16) = \cos(\pi/2) = 0, \quad (6)$$

with

$$T_8(x) = 128x^8 - 256x^6 + 160x^4 - 32x^2 + 1. \quad (7)$$

The degree-eight Chebyshev coordinate basis is

$$B_T = \{T_0(\beta), T_1(\beta), \dots, T_7(\beta)\}, \quad (8)$$

while the corresponding power basis is

$$B_P = \{1, \beta, \beta^2, \dots, \beta^7\}. \quad (9)$$

The first terms illustrate the growth of the transformation coefficients:

$$T_0(x) = 1, \quad (10)$$

$$T_1(x) = x, \quad (11)$$

$$T_2(x) = 2x^2 - 1, \quad (12)$$

$$T_3(x) = 4x^3 - 3x, \quad (13)$$

$$T_4(x) = 8x^4 - 8x^2 + 1, \quad (14)$$

$$T_5(x) = 16x^5 - 20x^3 + 5x, \quad (15)$$

$$T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1, \quad (16)$$

$$T_7(x) = 64x^7 - 112x^5 + 56x^3 - 7x. \quad (17)$$

Let M contain the coefficients of $T_0, \dots, T_{N-1}$ in the power basis. If c_T is a column vector of Chebyshev coordinates and c_P is a column vector of power coordinates, the implemented convention is

$$c_P = M^T c_T. \quad (18)$$

Therefore, when M^T is invertible,

$$c_T = (M^T)^{-1} c_P. \quad (19)$$

This orientation matters in reproducibility: treating M and M^T as interchangeable produces a mathematically different transformation even though both matrices contain the same polynomial coefficients.

For $N = 8$, the determinant is $\det(M) = 2^{21} = 2,097,152$. With $q = 257$, the determinant is nonzero modulo q and $\gcd(\det(M), q) = 1$, so the transformation is invertible in the tested finite field. This verifies a representation property only. It does not imply that the resulting coordinate system is cryptographically harder or easier.

B. Relation to the negacyclic RLWE quotient

The Chebyshev construction and the RLWE quotient must be distinguished carefully. The identity $T_8(\beta) = 0$ describes the degree-eight Chebyshev construction used to generate a coordinate system. The RLWE-related arithmetic experiments, in contrast, retain

$$R_q = \mathbb{Z}_q[x]/(x^N + 1). \quad (20)$$

An element $a \in R_q$ is first generated in the standard quotient. It can then be expressed in Chebyshev coordinates whenever the selected transformation is invertible. Multiplication can be carried out through a Chebyshev-coordinate routine, after which the result is transformed back to the power basis and reduced according to the same $x^N + 1$ quotient.

This distinction prevents an important category error. Replacing the quotient polynomial $x^N + 1$ by $T_N(x)$ would define a different algebra and potentially a different cryptographic problem. The experiments reported as RLWE representation experiments do not make that replacement. Earlier native-Chebyshev experiments are retained as algebraic demonstrations but are not used to claim security properties of RLWE.

C. Common-basis comparison principle

Suppose e_P is an error polynomial represented in the power basis and e_T is the same algebraic error represented in Chebyshev coordinates. A coordinate norm such as

$$\|e_T\|_\infty = \max_i |(e_T)_i| \quad (21)$$

need not equal $\|e_P\|_\infty$. The two values are norms of different coordinate vectors, not necessarily different algebraic errors. Consequently, a meaningful comparison of RLWE-related noise requires converting both quantities into a common representation before calculating a norm or decoding margin.

EXP10 initially illustrated how misleading the raw coordinate comparison can be: the Chebyshev-coordinate values appeared substantially larger than power-basis values. EXP11 then converted the same ciphertext components and errors into a common basis and found exact equivalence in the tested cases. This experiment is one of the central methodological controls of the study.

V. EXPERIMENTAL METHODOLOGY

A. Experimental progression

The 27 experiments were organized as a sequence of validation layers rather than as independent attempts to find a favorable result. The first layer establishes mathematical identities and basis conversion. The second layer tests modular arithmetic and a toy RLWE baseline. The third layer tests whether Chebyshev coordinates can represent standard RLWE elements without changing the underlying quotient. The fourth layer moves from coefficient space to canonical embedding and conditioning. The fifth layer stresses numerical evaluation and repeated multiplication. The final layer performs independent reference validation, robustness, sensitivity analysis, and consolidation.

Table I summarizes the role of the principal experiments. The full package contains the experiment inventory and exclusions so that superseded results remain auditable.

B. Parameter regimes

The experiments use small and medium dimensions because the purpose is to expose algebraic and numerical behavior under controlled conditions. Degree-eight experiments use $q = 257$ and typically 1,000 trials for modular correctness. The corrected degree-16 study tests $q \in \{257, 769, 1229\}$ with 1,000 trials. Conditioning and canonical embedding studies use $N = 4, 8, 16, 32$, while numerical stress tests extend to $N = 64$ and $N = 128$. High-precision reference experiments use 150–200 decimal digits where required.

The use of multiple dimensions is important. A basis transformation that is harmless at $N = 4$ may become difficult at $N = 32$, and a numerical method that is accurate for a single multiplication may fail after repeated multiplication. Similarly, a coefficient bound that appears influential in one dimension may be secondary to dimension and depth in another. The parameter-sensitivity experiments were therefore included to avoid drawing a single-parameter conclusion from one operating point.

C. Correctness and timing methodology

Correctness was tested by comparing independently computed algebraic results rather than merely checking whether an implementation returned without error. For modular arithmetic, equality was evaluated in the selected finite field. For representation experiments, the Chebyshev result was mapped back to the power basis before comparison. For numerical experiments, an independent high-precision computation served as the reference. This hierarchy is important because comparing two floating-point computations that share the same unstable pathway can conceal a common error.

Timing values are reported as prototype measurements, principally from Python/SymPy-style implementations. They are not claims about optimized C, C++, assembly, FPGA, GPU, or standardized KEM implementations. The timing experiments are therefore useful for identifying computational trends in the tested algorithms, but they should not be converted directly into cryptographic throughput or energy claims.

D. Independent-reference methodology

EXP24 and subsequent experiments were designed to address a specific threat: an error metric can look convincing when the reference computation shares the same algebraic pathway as the tested computation. The independent-reference experiments instead use higher precision and a separate evaluation strategy. EXP25 repeats selected regimes over independent seeds, EXP26 changes coefficient bounds, and EXP27 consolidates the final benchmark. Agreement across these experiments is treated as evidence of repeatability, not as a proof of generality beyond the tested regimes.

E. Experiment exclusions and corrections

Scientific reproducibility requires documenting unsuccessful or invalid approaches. EXP12 was superseded because the original decoder introduced a correctness issue at $N = 16$. EXP15 was excluded because its evaluation matrix did not implement the intended embedding. EXP15-C was excluded because its modular-centered coordinate embedding did not provide the intended canonical comparison. EXP18 is retained as supplementary evidence because unrestricted multiplication allows degree growth and therefore does not maintain a fixed-dimensional RLWE quotient. EXP22 in its first form was excluded because the evaluation method did not implement the same $x^N + 1$ quotient; EXP22-C corrected the root set and interpolation procedure. EXP23 is used for structure statistics, but its numerical error columns are not used because the reference and working calculations shared the same structure-constant pathway.

These exclusions are not cosmetic. They define the boundary between evidence that supports the final conclusions and experiments that are retained only to document the research process. The supplementary package contains the exclusion rationale.

VI. RESULTS

A. Algebraic equivalence at low dimension

The initial experiments establish that the Chebyshev basis can be constructed and used as a coordinate system. EXP05 and

TABLE I
EXPERIMENTAL ARCHITECTURE AND EVIDENTIARY ROLE.

Exp.	Theme	Primary validation target	Role in final evidence
01–05	Polynomial and basis construction	Chebyshev identities, transformation, exact arithmetic, representation-level timing and coefficient behavior	Algebraic foundation
06–07	Native and modular Chebyshev arithmetic	Reduction, product identity, modular invertibility, modular multiplication and coefficient wrapping	Algebraic/modular validation
08–11	RLWE-related representation	Toy baseline, standard-ring representation, controlled encryption/decryption, common-basis comparison	Noise/representation control
13–15-D	Dimension, embedding, conditioning	$N = 16$ corrected decoding, transformation determinants, canonical embedding and conditioning	Structural scaling
16–17	Evaluation stress	Direct evaluation versus Chebyshev/Clenshaw under high precision and increasing dimension	Numerical stability
19–23	Fixed-dimensional multiplication	Repeated multiplication, structure constants, precision effects, corrected evaluation/interpolation	Pathway analysis
24–27	Independent validation	High-precision reference, repeated seeds, parameter sensitivity, consolidated benchmark	Final quantitative evidence

EXP06 verify basis conversion and multiplication equivalence at $N = 8$. The degree-eight product identity in Eq. (2) was verified for all 64 pairs (m, n) with $m, n \in \{0, \dots, 7\}$. In EXP06, 1,000 multiplication tests passed without an arithmetic mismatch. The direct Chebyshev implementation took 3.7245 s over the benchmark set, compared with 7.7965 s for the corresponding power-basis benchmark and 8.6372 s for a conversion-based Chebyshev pathway. These values are implementation-specific and are useful mainly because they demonstrate that a structured multiplication rule can reduce the operation count in a small symbolic prototype.

EXP06 also recorded a large difference in raw coordinate magnitudes: the average maximum coefficient was approximately 7,806.746 in the power representation and 130.990 in the direct Chebyshev representation. The ratio was approximately 59.60. This is an interesting algebraic representation observation, but it cannot be interpreted as a reduction in RLWE noise. The same element can have very different coordinate vectors under two bases. The later common-basis experiments were specifically designed to test this point.

EXP07 extends the arithmetic into a modular setting with $q = 257$. The transformation determinant is invertible modulo q , 1,000 modular basis conversions pass, and 1,000 modular multiplication tests pass. The 64 Chebyshev product identities also remain valid in the modular representation. The average maximum centered coefficient is approximately 113.993 in the power basis and 114.223 in the Chebyshev representation, illustrating that modular reduction can substantially change the appearance of coefficient comparisons. The prototype direct Chebyshev modular multiplication took 0.2407 s compared with 0.1309 s for the power-basis pathway.

B. RLWE representation and common-basis noise

EXP08 establishes a small toy RLWE baseline with $N = 8$, $q = 257$, and error bound two. The public-key relation, encoding, and 1,000 correctness trials passed. The experiment is intentionally treated as a baseline rather than a cryptographic benchmark. EXP09 then represents standard RLWE elements using Chebyshev coordinates while keeping the quotient $x^N + 1$ unchanged. Basis conversion, multiplication, cross-representation multiplication, and product round-trip checks all pass in 1,000 trials.

EXP10 makes the comparison more explicit by encrypting and decrypting with controlled parameters. The standard and Chebyshev representations produce equivalent ciphertext components after conversion. However, raw coordinate noise appears very different before conversion: the average L_∞ value is approximately 14.187 in the standard power coordinates and 109.967 in raw Chebyshev coordinates. This difference could be misleading if reported as a cryptographic noise change.

EXP11 resolves the issue by expressing both ciphertext and noise quantities in a common basis. The u ciphertext components are equivalent in all tested cases, the v components are equivalent in all tested cases, and the recovered noise is identical after conversion. The resulting interpretation is unambiguous within the experiment: the large raw-coordinate difference in EXP10 is a coordinate effect, not evidence that the underlying RLWE error distribution has changed.

This finding is central to the paper. Any future claim about noise reduction would require a comparison of the same algebraic quantity in a common norm or embedding, together with the complete secret/error distribution and decoding procedure. A basis-dependent coefficient norm alone is insufficient.

C. Dimension scaling and corrected $N = 16$ validation

EXP13 extends the common-basis experiment to $N = 16$ and three moduli, $q = 257, 769, 1229$. The corrected experiment records standard and Chebyshev correctness of 1.0, exact ciphertext equivalence, and exact noise equality in all tested settings. For fixed decoding scale at $q = 257$, the average L_∞ noise is approximately 23.383 with average L_2 norm 44.8111. Comparable values occur for $q = 769$ and $q = 1229$, with small differences caused by the selected sampling and decoding parameters. Scaling the decoding factor produces similar values, reinforcing that the representation change itself is not responsible for the observed common-basis noise.

EXP14 examines the determinant of the basis transformation. The determinants are 2^3 , 2^{21} , 2^{105} , and 2^{465} for $N = 4, 8, 16, 32$, respectively. Although these determinants establish invertibility for the selected odd modulus, their rapid growth signals that the integer transformation itself becomes increasingly large. This is a warning sign for numerical implementations, even though exact modular arithmetic can still perform the conversion correctly.

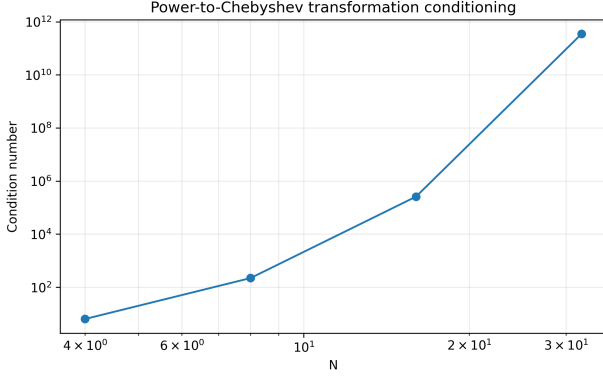


Fig. 1. Growth of the power-to-Chebyshev transformation condition number with dimension.

TABLE II
CANONICAL EMBEDDING AND TRANSFORMATION CONDITIONING
(EXP15-D).

N	$\ \sigma(a)\ _\infty$	$\ \sigma(a)\ _2$	$\kappa(M)$
4	3.0038	3.8643	6.34
8	4.3378	6.4987	2.21×10^2
16	6.3147	11.0331	2.58×10^5
32	8.9281	18.6721	3.47×10^{11}

D. Canonical embedding and conditioning

The next question is whether the representation difference survives a canonical embedding. EXP15-D uses an exact integer/rational canonical embedding and compares corresponding algebraic elements. The measured embedding magnitudes are identical between the power and Chebyshev representations within the exact construction. For $N = 4, 8, 16, 32$, the representative L_∞ embedding magnitudes are 3.0038, 4.3378, 6.3147, and 8.9281, while the corresponding L_2 magnitudes are 3.8643, 6.4987, 11.0331, and 18.6721.

At the same time, the condition number of the power-to-Chebyshev transformation increases dramatically. It is approximately 6.34 at $N = 4$, 220.825 at $N = 8$, 2.584×10^5 at $N = 16$, and 3.468×10^{11} at $N = 32$. Figure 1 illustrates this growth. The important interpretation is that transformation conditioning and algebraic element magnitude are different quantities. An ill-conditioned coordinate transformation can amplify floating-point perturbations even when the exact embedded element has not changed.

E. Direct evaluation versus Chebyshev/Clenshaw evaluation

EXP16 and EXP17 separate the basis from the evaluation algorithm. A power-basis polynomial can be evaluated with Horner's rule, while a Chebyshev expansion can be evaluated using a backward recurrence such as Clenshaw's algorithm. The purpose is not to claim that one representation is universally stable, but to determine whether a known stable evaluation procedure changes the numerical behavior in the selected stress regimes.

EXP17 provides the clearest separation. At $N = 16$ with coefficient bound two, the mean relative error for power/Horner is approximately 4.979×10^{-12} , while the Chebyshev/Clenshaw

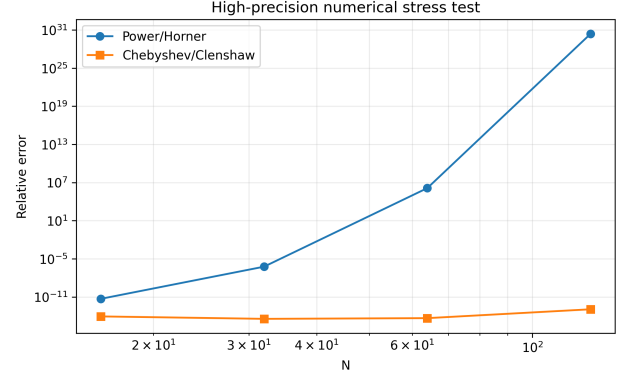


Fig. 2. Independent high-precision stress comparison of power/Horner and Chebyshev/Clenshaw evaluation.

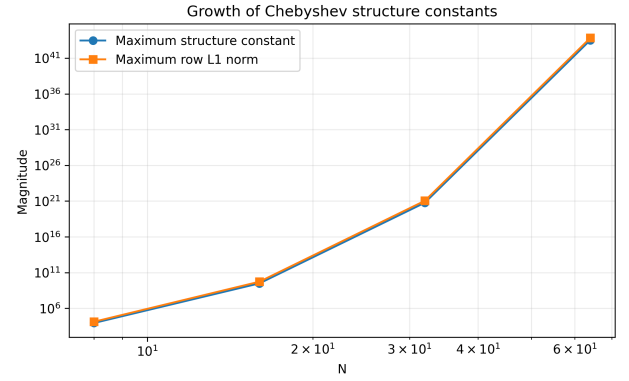


Fig. 3. Growth of Chebyshev structure constants with polynomial dimension.

error is approximately 8.516×10^{-15} . At $N = 32$, the corresponding values are 5.723×10^{-7} and 3.528×10^{-15} . At $N = 64$, the power/Horner error reaches approximately 1.316×10^6 , while Chebyshev/Clenshaw remains approximately 4.554×10^{-15} . At $N = 128$, the difference becomes even larger, with approximately 2.491×10^{30} for power/Horner and 1.131×10^{-13} for Chebyshev/Clenshaw.

These observations are consistent with the classical numerical-analysis motivation for Chebyshev expansions, but they must be scoped correctly. The result concerns evaluation of polynomial representations. It does not imply that every Chebyshev multiplication algorithm is stable, and it does not imply a cryptographic advantage.

F. Structure-constant growth

A direct Chebyshev multiplication framework can precompute structure constants that describe products of basis elements after reduction. EXP20 shows that these constants grow very rapidly with dimension. The maximum absolute structure constant is approximately 8.88×10^3 at $N = 8$, 3.09×10^9 at $N = 16$, 5.89×10^{20} at $N = 32$, and 3.23×10^{43} at $N = 64$. The maximum row- L_1 magnitude grows from approximately 1.35×10^4 to 6.54×10^{43} over the same range.

The structure-constant growth explains why exact algebraic identities can coexist with poor floating-point behavior. If a multiplication is expressed as a large sum of products weighted

by coefficients of enormous magnitude, cancellation may become severe. Increasing arithmetic precision can postpone the onset of visible error, but it does not remove the underlying conditioning of the representation.

G. Fixed-dimensional repeated multiplication

EXP19 maintains a fixed-dimensional quotient while increasing multiplication depth. This is an important control because unrestricted polynomial multiplication can increase degree and therefore change the computational object. The fixed-dimensional experiment instead reduces after every multiplication so that the dimension remains N .

The results show mixed behavior across dimensions and depths. At moderate dimension and shallow depth, high-precision evaluation can remain extremely accurate. At $N = 64$, however, repeated multiplication exposes the sensitivity of the structure-constant pathway. This confirms that a one-step correctness test is not enough to characterize a representation intended for repeated cryptographic arithmetic.

EXP21 adds arithmetic precision as a variable. The comparison across 53, 100, and 200 decimal digits shows that precision can substantially reduce some errors, particularly when the underlying computation is otherwise well conditioned. However, the relationship is not uniformly monotone across all dimensions and depths because different pathways have different sources of amplification and cancellation. Precision is therefore a mitigation variable rather than a replacement for algorithmic stability.

H. Corrected evaluation/interpolation pathway

EXP22-C corrects an earlier evaluation experiment by using the roots appropriate to the $x^N + 1$ quotient. This correction is essential because an interpolation experiment that uses the wrong root set does not implement the same algebra. With the corrected roots, low-dimensional cases reach extremely small errors, on the order of 10^{-76} in the high-precision reference setting.

At $N = 32$ and depth eight, the three principal pathways exhibit approximately 2.21×10^{-9} , 2.42×10^{54} , and 5.73×10^{-11} error behavior in the corrected benchmark. At $N = 64$, the evaluation/interpolation pathway remains much more stable than the structure-constant pathway, but its absolute error is no longer negligible: values around 5.8×10^{-1} to 7.2×10^{-1} occur in the tested high-depth regimes. This is an important result because it prevents the paper from replacing one overclaim with another. Chebyshev evaluation is not described as universally stable; it is described as substantially more stable than the tested alternatives in specified regimes.

I. Independent final benchmark

Table III summarizes EXP27. The final benchmark uses an independent high-precision reference and reports mean relative errors for three computational pathways: structure constants, conversion, and evaluation/interpolation. At $N = 16$, all three remain near the high-precision floor across the tested depths. At $N = 32$, the depth-eight case begins to separate, with

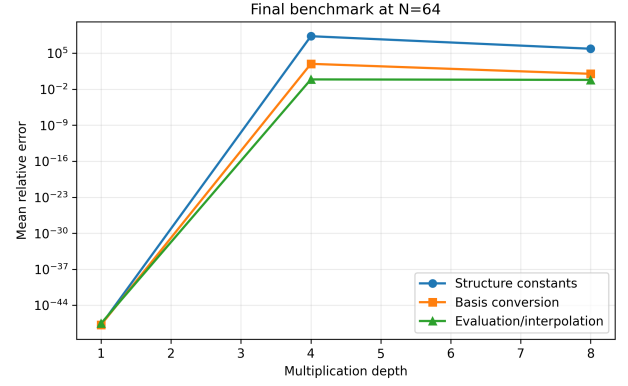


Fig. 4. EXP27 error comparison at $N = 64$ across the final computational pathways.

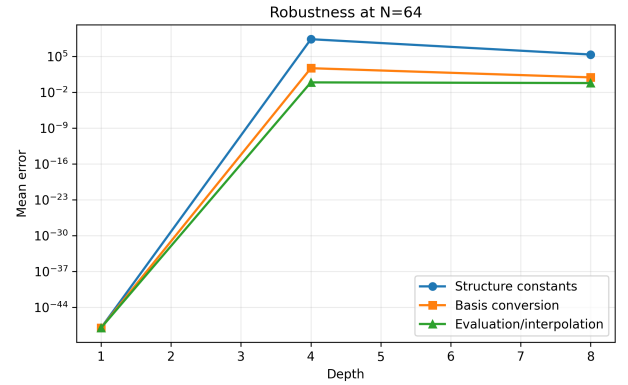


Fig. 5. Robustness of the high-dimensional numerical behavior across independent seeds (EXP25).

the structure pathway reaching approximately 6.25×10^{-8} while conversion and evaluation/interpolation remain around 2.01×10^{-9} and 6.57×10^{-10} .

The separation becomes dramatic at $N = 64$. At depth four, the structure-constant pathway has mean relative error about 2.02×10^8 , the conversion pathway about 8.63×10^2 , and evaluation/interpolation about 8.06×10^{-1} . At depth eight, the corresponding values are approximately 7.39×10^5 , 9.89, and 6.54×10^{-1} . All final trials were marked as completed without a non-finite failure, but completion is not equivalent to accuracy. An error of 0.654 is numerically large even though the program did not report an overflow or NaN.

J. Robustness across independent seeds

EXP25 repeats selected high-dimensional regimes over independent random seeds. At $N = 64$ and depth four, the mean structure-constant, conversion, and evaluation errors are approximately 2.29×10^8 , 4.98×10^2 , and 8.46×10^{-1} , respectively. At depth eight, they are approximately 2.33×10^5 , 8.06, and 6.28×10^{-1} . These values reproduce the qualitative ordering observed in EXP24 and EXP27: the structure-constant pathway is the most sensitive in the high-dimensional regimes, while evaluation/interpolation is substantially less unstable but still not exact.

TABLE III
FINAL CONSOLIDATED BENCHMARK (EXP27): MEAN RELATIVE ERROR BY DIMENSION AND MULTIPLICATION DEPTH.

N	depth	Structure constants	Conversion	Evaluation/interpolation	Failures
16	1	2.69×10^{-54}	2.55×10^{-54}	2.55×10^{-54}	0
16	4	2.53×10^{-66}	6.85×10^{-67}	6.85×10^{-67}	0
16	8	2.69×10^{-54}	2.55×10^{-54}	2.55×10^{-54}	0
32	1	5.02×10^{-68}	1.69×10^{-67}	1.69×10^{-67}	0
32	4	2.43×10^{-44}	5.59×10^{-44}	5.59×10^{-44}	0
32	8	6.25×10^{-8}	2.01×10^{-9}	6.57×10^{-10}	0
64	1	1.60×10^{-48}	1.60×10^{-48}	2.99×10^{-48}	0
64	4	2.02×10^8	8.63×10^2	8.06×10^{-1}	0
64	8	7.39×10^5	9.89	6.54×10^{-1}	0

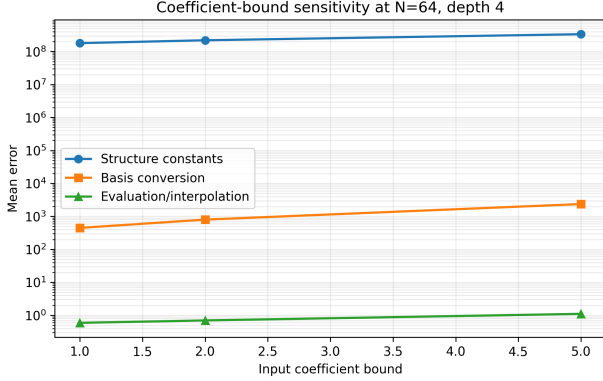


Fig. 6. Sensitivity of numerical error to coefficient-bound changes in EXP26.

K. Parameter sensitivity

EXP26 varies coefficient bounds while retaining dimensions and depths that are already known to be difficult. At $N = 64$ and depth four, the structure-constant error remains in the approximate range 1.8×10^8 – 3.36×10^8 across the tested bounds, while conversion errors range from approximately 4.48×10^2 to 2.37×10^3 . Evaluation errors range from roughly 5.92×10^{-1} to 1.11. At depth eight, structure errors range from approximately 3.14×10^5 to 8.61×10^5 , conversion errors from 5.10 to 15.9, and evaluation errors from 5.47×10^{-1} to 7.53×10^{-1} .

The parameter-sensitivity results are non-monotone. Increasing the coefficient bound does not simply increase every error metric in every pathway. This suggests that cancellation, scaling, and conditioning interact in a way that cannot be summarized by a single coefficient-growth rule. The result also supports reporting multiple dimensions, depths, and random seeds rather than one stress configuration.

VII. CROSS-EXPERIMENT SYNTHESIS

A. From exact identities to numerical failure modes

The progression from EXP01 to EXP27 provides a useful hierarchy of evidence. The first stage establishes that the mathematical objects are implemented correctly. The second stage establishes that the representation can be used inside a fixed modular ring. The third stage establishes that apparent changes in coordinate magnitude do not necessarily survive conversion to a common basis. Only after these controls

are in place does the numerical-stability analysis become interpretable.

This hierarchy also explains why the final results are not reducible to a single “Chebyshev versus power” comparison. There are at least four computational operations in the complete workflow: basis construction, basis conversion, polynomial multiplication, and numerical evaluation or interpolation. Each operation has a different error mechanism. Basis construction is exact when performed symbolically. Basis conversion is sensitive to the transformation matrix. Direct multiplication is sensitive to structure-constant magnitude and cancellation. Evaluation/interpolation is sensitive to node placement, recurrence stability, and finite-precision arithmetic. A single benchmark number therefore cannot characterize the entire representation.

B. Interpretation of the high-dimensional threshold

The final experiments suggest a practical transition in the tested numerical regimes. At $N = 16$, the independent high-precision reference errors remain extremely small, often below 10^{-50} . At $N = 32$, shallow computations remain close to the reference, while depth-eight computations begin to show visible separation. At $N = 64$, the direct structure-constant and conversion pathways become severely unstable at depths four and eight, while evaluation/interpolation remains below one in mean relative error but is no longer highly accurate.

This transition should not be interpreted as a universal threshold at $N = 64$. The threshold depends on precision, coefficient distribution, implementation, multiplication ordering, and the exact numerical pathway. What can be stated from the experiments is that the tested $N = 64$ regimes expose instability that is not visible at $N = 16$ and is much less pronounced at $N = 32$. The result is consequently best viewed as evidence of dimension-dependent sensitivity rather than as a fixed failure boundary.

C. Relationship between conditioning and observed error

The conditioning results and the final error results are consistent at a qualitative level. The transformation condition number increases by many orders of magnitude between $N = 8$ and $N = 32$, while structure constants continue to grow into the 10^{43} range at $N = 64$. These quantities provide mechanisms through which small arithmetic perturbations can become large coordinate errors. However, conditioning alone does not predict the exact error observed in every experiment. For example, the

TABLE IV
EVIDENCE MATRIX FOR PRINCIPAL CONCLUSIONS.

Claim	Evidence	Status
Chebyshev coordinates can represent tested ring elements	EXP05–EXP07, EXP09, EXP13	Directly demonstrated in tested regimes
Multiplication can agree after common-basis conversion	EXP06–EXP11, EXP13	Directly demonstrated
Raw coordinate size is representation-dependent	EXP06, EXP07, EXP10–EXP11	Directly demonstrated
Canonical embedding magnitude is unchanged by basis choice	EXP15-D	Directly demonstrated for tested samples
Transformation conditioning grows with dimension	EXP14–EXP17	Directly demonstrated in tested dimensions
Chebyshev/Clenshaw can outperform power/Horner in stress evaluation	EXP17	Demonstrated for specified stress regimes
Direct structure constants become numerically difficult at high dimension	EXP20, EXP24–EXP27	Strongly supported by independent validation
Chebyshev representation reduces RLWE noise	EXP10–EXP13	Not supported; common-basis noise is equivalent
Chebyshev representation improves RLWE security	All experiments	Not established
Chebyshev representation is a production-ready optimization	All experiments	Not established

EXP27 structure-constant error at depth eight is smaller than the corresponding depth-four value at $N = 64$, despite the larger multiplication depth. This non-monotonicity is evidence that cancellation and the particular sampled inputs also matter.

The appropriate interpretation is therefore mechanistic rather than predictive. Large transformation condition numbers and large structure constants identify numerical risk factors. They do not determine a unique error value without specifying the input, arithmetic precision, operation ordering, and evaluation algorithm. This is another reason the independent-reference and multi-seed experiments are important.

D. Evidence matrix for the principal claims

Table IV summarizes the relationship between the principal claims and the experiments supporting them. The table deliberately distinguishes claims that are directly demonstrated from claims that remain outside the scope of the study.

The evidence matrix is useful for preventing accidental overinterpretation. In particular, the negative entries are not failed research outcomes. Showing that a representation change does not alter the common-basis noise is itself an important result because it removes a misleading interpretation suggested by raw coordinate measurements. Likewise, identifying high-dimensional numerical instability is useful even when the representation does not yield a direct implementation advantage.

VIII. DISCUSSION

A. Three levels of equivalence

The experiments reveal three different notions of equivalence that should be kept separate. The first is *algebraic equivalence*: two coordinate vectors represent the same element of the same quotient ring. The second is *cryptographic/common-basis equivalence*: ciphertext and error quantities are identical after conversion to a common representation. The third is *floating-point equivalence*: two algorithms produce numerically close approximations to a high-precision reference.

These levels do not imply one another in both directions. Exact basis conversion establishes algebraic equivalence, but it does not guarantee stable floating-point conversion. A common-basis equality establishes that a representation change has not altered the tested RLWE-related element, but it does not show that a particular implementation is efficient. A stable evaluation algorithm can reduce numerical error without changing the cryptographic problem. Much of the apparent contradiction in early Chebyshev experiments disappears once these levels are distinguished.

B. Why raw coefficient reductions are insufficient

EXP06 reports a large reduction in maximum coefficient magnitude when the same low-dimensional arithmetic is written in Chebyshev coordinates. Such a result is mathematically legitimate as a statement about coordinate vectors. It becomes misleading only when the coordinate magnitude is renamed “RLWE noise.” The error distribution in an RLWE scheme is defined relative to the algebraic sampling and decoding process, not by whichever coordinate system happens to be convenient for display.

EXP10 and EXP11 provide a direct demonstration. The raw Chebyshev coordinate noise can be much larger than the power-basis vector, yet the common-basis noise is exactly equivalent. The appropriate conclusion is therefore not that Chebyshev coordinates reduce or increase RLWE noise, but that coordinate norms are representation-dependent and must be normalized before they are used to support a cryptographic interpretation.

C. Conditioning as a bridge between algebra and numerics

The transformation condition number provides a useful bridge between exact algebra and numerical behavior. At small dimensions, conversion can be carried out with essentially no observed error in the high-precision experiments. As dimension increases, the condition number becomes enormous. This does not make the exact transformation invalid; it makes finite-precision perturbations potentially more consequential.

The distinction resembles standard numerical linear algebra: an exact matrix may be perfectly invertible while an implementation using finite precision remains sensitive to perturbations. The present results therefore support a practical design principle: if Chebyshev coordinates are used in a high-dimensional implementation, the transformation itself should be treated as a numerical object whose conditioning must be measured, not merely as an algebraic identity.

D. Structure constants versus evaluation/interpolation

The final benchmark suggests that different Chebyshev-based pathways have fundamentally different numerical behavior. Structure constants provide a direct algebraic multiplication rule, but their coefficients grow extremely rapidly with dimension. Conversion methods repeatedly move between coordinate systems and can therefore inherit the conditioning of the transformation. Evaluation/interpolation avoids some of the explicit large structure constants and performs substantially better in the tested high-dimensional regimes.

However, evaluation/interpolation is not exact in finite precision. At $N = 64$, the observed errors around 0.65–0.81 are too large for a claim of high numerical accuracy. The correct conclusion is therefore comparative rather than absolute: among the tested pathways, evaluation/interpolation is substantially more stable at the difficult $N = 64$ settings, but it still requires improved numerical design before it could be treated as a reliable high-precision arithmetic primitive.

E. Dimension and depth dominate the difficult regimes

Across EXP19–EXP27, dimension and multiplication depth emerge as the dominant stress variables. At $N = 16$, many computations remain close to the high-precision reference even after repeated operations. At $N = 32$, depth eight begins to reveal measurable error. At $N = 64$, both dimension and repeated multiplication can push structure-constant and conversion pathways into severe instability.

The depth dependence is especially relevant for cryptographic applications because multiplication is not necessarily a one-shot operation. Key generation, encryption, decryption, and more advanced lattice-based computations can contain multiple polynomial operations. A representation that is accurate for one multiplication but accumulates large errors over a sequence is not equivalent, from an implementation perspective, to a representation that maintains accuracy throughout the computation.

F. Implications for implementation design

The experiments suggest several implementation-level considerations. First, exact modular arithmetic should be preferred whenever the target computation is inherently modular; floating-point Chebyshev structure constants are unnecessary if exact finite-field operations can express the same mapping. Second, if real or complex evaluation is required, recurrence-based algorithms should be preferred over naive expansion whenever the numerical analysis supports that choice. Third, transformations should be minimized when their conditioning is poor. Fourth, independent high-precision validation should be included in research prototypes so that a shared numerical error is not mistaken for correctness.

These observations do not imply that a Chebyshev representation should replace the arithmetic used by standardized lattice-based schemes. Rather, they identify the components that would have to be optimized and formally analyzed before such a replacement could be considered.

G. Relationship to prior numerical-analysis results

The observed behavior is consistent with classical results on polynomial approximation and numerical stability. Chebyshev representations are well known for reducing the difficulties associated with monomial evaluation, particularly when coupled with stable recurrence algorithms [10], [11]. Barycentric interpolation and its stability analyses similarly show that node selection and algorithmic form can be as important as the underlying polynomial basis [14], [15], [17]. The present study adds a specific RLWE-related context in which these numerical issues must coexist with modular arithmetic, common-basis comparisons, and cryptographic interpretation constraints.

IX. COMPUTATIONAL COMPLEXITY AND PRACTICAL CONSIDERATIONS

A representation-level comparison should include more than a single timing value. Let N denote the polynomial dimension. Conventional negacyclic multiplication can be implemented in several ways, including schoolbook convolution, Karatsuba-like methods, or structured transforms. A direct Chebyshev-coordinate multiplication using precomputed structure constants can be viewed as a dense bilinear map whose storage and arithmetic cost depend on the number and magnitude of nonzero structure coefficients. The experiments do not attempt to optimize this map, so the reported prototype timing should be interpreted only as evidence about the tested implementation.

The basis conversion in Eq. (18) is a matrix-vector operation. If implemented densely, its arithmetic cost is quadratic in N , while storing a full transformation matrix also requires quadratic storage. Sparse parity structure in the Chebyshev coefficient matrix can reduce some operations, but the inverse transformation may not preserve the same sparsity pattern. More importantly, arithmetic complexity alone does not capture conditioning. A theoretically inexpensive conversion can still be unsuitable if it amplifies finite-precision error.

Evaluation/interpolation introduces a different trade-off. Evaluating at a structured set of roots can avoid explicitly materializing large structure constants, but the interpolation step introduces its own numerical considerations. EXP22-C and EXP24 show that this pathway is attractive in the difficult high-dimensional regimes tested here, but the absolute error at $N = 64$ remains too large to support a claim of production readiness.

The timing evidence also illustrates why direct comparisons with cryptographic libraries would be inappropriate. EXP06 found a direct Chebyshev prototype faster than the power-basis symbolic benchmark at $N = 8$, whereas EXP07 found the direct modular Chebyshev prototype slower than the power-basis implementation. These differences arise because the algorithms and arithmetic domains are different. A meaningful implementation comparison would require equivalent low-level languages, identical hardware, optimized modular reduction, vectorization, memory accounting, and standardized parameter sets.

X. THREATS TO VALIDITY AND REPRODUCIBILITY

A. Internal validity

The principal internal-validity threat is an incorrect implementation of the algebra. The experiment sequence addresses this through exact identities, round-trip conversion, modular multiplication checks, and independent references. The corrected EXP13 and EXP22-C experiments demonstrate why such controls are necessary: an implementation can produce plausible numerical output while representing the wrong mathematical object.

A second threat is reference contamination. If the reference computation uses the same structure constants as the test computation, both can share the same error. EXP23 is explicitly limited for this reason. EXP24 replaces the shared pathway with an independent high-precision reference, and EXP25–EXP27 provide further validation.

A third threat is parameter overfitting. Because numerical instability can depend strongly on dimension, depth, coefficient bound, and random seed, selecting one favorable regime would provide weak evidence. The final package therefore includes multiple dimensions, depths, seeds, and bounds. The resulting non-monotone behavior is reported rather than smoothed into a single trend.

B. External validity

The experiments use small to moderate dimensions compared with production post-quantum cryptosystems, and the implementations are research prototypes. Therefore, the numerical observations should not be extrapolated directly to standardized KEMs or to hardware implementations. The results are best interpreted as evidence about the mathematical and numerical mechanisms observed in the tested range.

Likewise, the toy RLWE correctness experiments do not constitute a security evaluation. They use controlled parameters and limited trials and do not estimate concrete security against lattice attacks. A cryptographic deployment study would need a fully specified parameter set, security estimator, secret and error distributions, side-channel model, implementation model, and comparison against an established baseline.

C. Reproducibility practices

Reproducibility is supported by retaining random seeds, trial counts, output tables, generated figures, experiment exclusions, and the final consolidated data. The final manuscript uses only the validated key-result tables from the package. The package also retains the earlier generated research package as an audit archive. The artifact-generation script regenerates selected figures from packaged CSV data without silently rerunning or changing the underlying experiments.

XI. LIMITATIONS AND THREATS TO CRYPTOGRAPHIC INTERPRETATION

The most important limitation is that the work does not provide a cryptographic security proof. It does not define a new hardness assumption, derive a reduction, estimate attack cost,

or propose a standardized parameter set. The phrase “RLWE-related” in the title is therefore intentional: the experiments study arithmetic and representation around an RLWE ring rather than claiming a new secure RLWE construction.

A second limitation is the use of numerical arithmetic in experiments that are ultimately motivated by exact modular cryptography. Floating-point analysis is useful for understanding conditioning and evaluation, but modular cryptographic arithmetic can often be performed exactly. Future implementations should therefore determine which numerical pathways are actually necessary. If the intended application can remain entirely in finite-field or integer arithmetic, some of the floating-point instabilities observed here may be avoidable.

A third limitation is the choice of Chebyshev basis itself. The first-kind basis is mathematically convenient, but other orthogonal polynomial families or alternative structured bases may have different transformation properties. The present results should not be generalized to all polynomial bases. Similarly, the structure-constant approach is only one possible Chebyshev multiplication algorithm.

A fourth limitation is that the experiments focus on arithmetic correctness and numerical stability rather than memory hierarchy, parallelism, vectorization, cache behavior, or hardware accelerators. These factors could substantially alter practical performance. The prototype timing measurements are therefore included as contextual evidence, not as implementation claims.

XII. FUTURE RESEARCH DIRECTIONS

Several directions follow naturally from the results. The first is to construct an exact modular Chebyshev arithmetic library that avoids floating-point structure constants altogether. Such a library could test whether the representation has any meaningful operation-count or memory advantage when all arithmetic is performed exactly.

The second direction is to investigate sparse or structured transformation algorithms. The raw transformation matrix has algebraic patterns arising from parity and the recurrence relation. Exploiting those patterns could reduce conversion cost and may also permit better-conditioned intermediate computations.

The third direction is to compare several evaluation/interpolation schemes. EXP22-C indicates that evaluation/interpolation can outperform direct structure constants numerically at high dimension, but its error remains non-negligible. Different node choices, barycentric formulations, compensated arithmetic, and arbitrary-precision strategies could be evaluated against the same independent reference framework [14]–[17].

The fourth direction is to study exact cryptographic parameters only after the arithmetic representation is understood. Such work would need to define the exact ring, secret distribution, error distribution, modulus, decoding rule, and security target. Concrete lattice-attack estimates would then be required before any statement about security could be made [19], [25], [26].

Finally, a useful follow-up would be a hardware-aware implementation study. The appropriate baseline would use the same dimension, modulus, language, compiler, hardware,

and optimization level for both representations. Measurements should include throughput, latency, memory, conversion overhead, and constant-time behavior. Only such a controlled study could determine whether the numerical observations reported here translate into practical computational benefits.

XIII. CONCLUSION

This work provides a controlled and reproducible evaluation of Chebyshev polynomial representations for polynomial arithmetic associated with an RLWE-style negacyclic ring. The experiments establish that Chebyshev coordinates can represent the same underlying algebra and that exact modular conversion and multiplication can be validated in the tested settings. They also show that representation-dependent coefficient magnitudes should not be confused with RLWE noise: common-basis comparisons recover equivalent ciphertext and error quantities.

The more consequential result is numerical. The power-to-Chebyshev transformation becomes increasingly ill-conditioned with dimension, while direct structure constants grow extremely rapidly. Under independent high-precision stress tests, Chebyshev/Clenshaw evaluation can be dramatically more stable than direct power/Horner evaluation. Nevertheless, high-dimensional fixed-dimensional multiplication remains challenging, and even the comparatively stable evaluation/interpolation pathway shows substantial absolute error at $N = 64$ and high multiplication depth.

The final conclusion is therefore deliberately narrow. Chebyshev representations are a viable and experimentally interesting coordinate system for structured polynomial arithmetic, but their usefulness depends on the interaction among basis conditioning, dimension, multiplication depth, and computational pathway. The evidence does not establish reduced RLWE noise, increased security, or superior cryptographic efficiency. Instead, it identifies a concrete numerical research problem and provides a reproducible framework for evaluating it without conflating representation-level observations with cryptographic guarantees.

ACKNOWLEDGEMENTS

The authors would like to thank Parul University, Vadodara, India, for providing the academic environment and computational facilities required to conduct this study.

FUNDING

This research was carried out as part of doctoral work at Parul University. The journal has granted a full Article Processing Charge (APC) waiver for this submission. No external funding was received.

AUTHOR CONTRIBUTIONS

Mohammad Asif: Conceptualization, methodology, mathematical analysis, software implementation, experimental investigation, data analysis, visualization, and writing—original draft.

Dr. Sanjay Agal: Supervision, research guidance, validation, critical review, and writing—review and editing.

Both authors contributed to the interpretation of the results, discussed the findings, approved the final version of the manuscript, and agreed to be accountable for their respective contributions.

DATA AVAILABILITY

The datasets generated and analysed during the current study are available from the corresponding author on reasonable request. The experimental procedures, parameter configurations, and statistical methodology required to reproduce the reported results are described in the manuscript.

DECLARATIONS

Ethics, Consent to Participate, and Consent to Publish

Ethics, Consent to Participate, and Consent to Publish declarations: not applicable.

Clinical Trial Registration

Not applicable. This study does not involve a clinical trial.

Competing Interests

The authors declare no competing interests.

REFERENCES

- [1] M. Ajtai, “Generating hard instances of lattice problems,” in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 1996, pp. 99–108.
- [2] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, 2005, pp. 84–93.
- [3] —, “On lattices, learning with errors, random linear codes, and cryptography,” *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, 2009.
- [4] D. Micciancio and O. Regev, “Lattice-based cryptography,” in *Post-Quantum Cryptography*. Springer, 2009, vol. 4956, pp. 147–191.
- [5] V. Lyubashevsky, C. Peikert, and O. Regev, “On ideal lattices and learning with errors over rings,” in *Advances in Cryptology—EUROCRYPT 2010*, vol. 6110. Springer, 2010, pp. 1–23.
- [6] —, “On ideal lattices and learning with errors over rings,” *Journal of the ACM*, vol. 60, no. 6, pp. 43:1–43:35, 2013.
- [7] —, “A toolkit for ring-lwe cryptography,” in *Advances in Cryptology—EUROCRYPT 2013*, vol. 7881. Springer, 2013, pp. 35–54.
- [8] L. Ducas and A. Durmus, “Ring-lwe in polynomial rings,” in *Public Key Cryptography—PKC 2012*, vol. 7293. Springer, 2012, pp. 34–51.
- [9] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*. CRC Press, 2002.
- [10] L. N. Trefethen, *Spectral Methods in MATLAB*. SIAM, 2000.
- [11] —, *Approximation Theory and Approximation Practice*, extended ed. SIAM, 2019.
- [12] N. J. Higham, *Accuracy and Stability of Numerical Algorithms*, 2nd ed. SIAM, 2002.
- [13] N. J. Higham and T. Mary, “A new approach to probabilistic rounding error analysis,” *SIAM Journal on Scientific Computing*, vol. 41, no. 5, pp. A2815–A2835, 2019.
- [14] J.-P. Berrut and L. N. Trefethen, “Barycentric lagrange interpolation,” *SIAM Review*, vol. 46, no. 3, pp. 501–517, 2004.
- [15] M. S. Floater and K. Hormann, “Barycentric rational interpolation with no poles and high rates of approximation,” *Numerische Mathematik*, vol. 107, no. 2, pp. 315–331, 2007.
- [16] R. C. Kirby, “Singularity-free evaluation of collapsed-coordinate orthogonal polynomials,” *ACM Transactions on Mathematical Software*, vol. 37, no. 1, pp. 1–16, 2010.
- [17] W. Mascarenhas, “The stability of barycentric interpolation at the chebyshev points of the second kind,” *Numerische Mathematik*, vol. 128, no. 2, pp. 265–300, 2014.

- [18] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem: extended abstract," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, 2009, pp. 333–342.
- [19] M. R. Albrecht, R. Player, and S. Scott, "On the concrete hardness of learning with errors," *Journal of Mathematical Cryptology*, vol. 9, no. 3, pp. 169–203, 2015.
- [20] Y. Chen and P. Q. Nguyen, "Bkz 2.0: Better lattice security estimates," in *Advances in Cryptology—ASIACRYPT 2011*, vol. 7073. Springer, 2011, pp. 1–20.
- [21] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.
- [22] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: A cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy*, 2018, pp. 353–367.
- [23] J. W. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the ring! practical, quantum-secure key exchange from lwe," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1006–1018.
- [24] D. J. Bernstein and T. Lange, "Post-quantum cryptography," in *Nature*, vol. 549, 2017, pp. 188–194.
- [25] C. Peikert, "How (not) to instantiate ring-lwe," in *Security and Cryptography for Networks*, vol. 9841. Springer, 2016, pp. 411–430.
- [26] C. Peikert, O. Regev, and N. Stephens-Davidowitz, "Pseudorandomness of ring-lwe for any ring and modulus," in *Proceedings of the Forty-Ninth Annual ACM SIGACT Symposium on Theory of Computing*, 2017, pp. 461–473.
- [27] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.
- [28] A. Smoktunowicz *et al.*, "On numerical stability of chebyshev polynomial evaluation," *Numerical Algorithms*, 2015.
- [29] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on chebyshev polynomials," *IEEE Transactions on Circuits and Systems I*, vol. 52, no. 7, pp. 1382–1393, 2005.