INTERNATIONAL JOURNAL OF ADVANCED RESEARCH
International Peer-Reviewed Research Journal
ISSN (Online): 3106-7980 | ISSN (Print): 3106-7972
Volume 3 • Issue 7 • November 2026

ALGEBRAIC AND TOPOLOGICAL PERSPECTIVES ON POST-QUANTUM CRYPTOGRAPHY AND QUANTUM ERROR CORRECTION

K. Hassan[*1], S. Siddiqui[*2], T. Mukhtar[*3], M. Noman Nasir[*4], M. Thakur[*5]

[*1,2,3,4]*Department of Basic Sciences, The Superior University, Lahore, Pakistan*
[*5]*Department of Physics, Tribhuvan University, Kathmandu, Nepal*

[*1]kamalhassan0034@gmail.com, orcid: 0009-0002-0054-393x, [*4]mnomannasir708@outlook.com
[*5]scientistmithileshthakur56@gmail.com

DOI: https://doi.org/10.5281/zenodo.24000123

Keywords
Post-quantum cryptography, module lattices, quantum error correction, stabilizer codes, homological codes, algebraic topology, fault tolerance, hardware co-design.

Article History
Received: 05 August 2026
Accepted: 19 October 2026
Published: 05 November 2026

Copyright @Author
Corresponding Author: *
M. Noman Nasir

Abstract

Post-quantum cryptography (PQC) and fault-tolerant quantum computing are conventionally treated as disjoint engineering disciplines. This paper establishes a disciplined algebraic and topological comparison between them and reports completed, reproducible results. We address three research questions: (i) which algebraic structures genuinely recur across both domains; (ii) where formally similar expressions serve divergent operational purposes; and (iii) what concrete, actionable conclusions follow. We provide a transparent literature-selection account and a comparison table contrasting prior reviews with the specific gap addressed here. Two fully worked examples are developed–a Module-LWE instance over $R_q = \mathbb{Z}_{17}[X]/(X^4+1)$ *and a homological surface code with explicit maps, kernels, quotient spaces, and distance metrics–and we prove a structural correspondence demonstrating that the two quotient constructions constitute the same inverse problem with inverted design objectives. A synthesis table separates exact isomorphisms, useful structural analogies, and relationships that do not hold. We then apply the framework to a concrete co-design decision: a fault-tolerant cryptographic coprocessor in which PQC polynomial multipliers and QEC decoders must be decoupled. We report measured ML-KEM benchmarks, measured surface-code Monte Carlo results, and a measured coprocessor decoupling experiment, all generated by released code. The framework correctly predicts the observed decoupling requirement. We do not claim that the two domains are the same mathematical problem; rather, we identify precisely where their abstractions intersect and where they diverge.*

I. INTRODUCTION

Large-scale quantum computation fundamentally alters the assumptions underlying classical public-key cryptography. Shor's algorithms solve integer factorization and discrete logarithms in polynomial time on an ideal fault-tolerant quantum computer [1], so the security of RSA, finite-field Diffie–Hellman, and elliptic-curve cryptography cannot rest solely on the classical hardness of their underlying problems. Concurrently, a practical quantum computer must itself overcome decoherence, gate errors,

measurement errors, leakage, correlated noise, and fabrication variability. Quantum error correction (QEC) and fault tolerance are therefore the physical and computational foundation on which the quantum threat model depends [14], [16].

These observations produce an apparent paradox. Cryptography must be redesigned so that an adversary equipped with a quantum computer cannot efficiently recover protected information, while the quantum computer required to create that adversary must be engineered from noisy components using algebraic and topological error-correction methods. The two subjects are usually studied independently: PQC focuses on computational hardness, parameter selection, reductions, implementation security, and migration [8]; QEC focuses on error models, code distance, syndrome extraction, decoders, logical operations, and resource overhead [17].

Thesis

We do not claim that a cryptographic lattice is equivalent to a quantum code, nor that topological QEC automatically yields a cryptographic primitive. Our thesis is narrower and testable: both areas repeatedly use a small set of structural operations—constructing algebraic objects, defining local constraints, taking kernels and images, passing to quotient structures, measuring distance, and analyzing the computational cost of recovering hidden structure from noisy or incomplete observations.

Three Core Research Questions

The paper is organized around three questions:

Q1. Which algebraic structures genuinely recur in both domains?

Q2. Where do similar mathematical expressions serve different operational purposes?

Q3. What useful conclusions follow from comparing them?

Q1 is answered in Sections IV–V; **Q2** in Section VI (Proposition 1) and Table II; and **Q3** in Section VIII, where the comparison drives a concrete co-design decision validated by measurement.

Contributions

1.A transparent literature-selection account (Section II) and a comparison table contrasting prior reviews with the gap addressed here (Table I).

2.Two fully worked examples with explicit maps, kernels, quotient spaces, and distance metrics: Module-LWE over $\mathbb{Z}_{17}[X]/(X^4+1)$(Section V-A) and a homological surface code (Section V-B).

3.A formal proposition with proof establishing that the two quotient constructions are the same inverse problem with inverted objectives (Section VI).

4.A synthesis table separating exact isomorphisms, useful analogies, and relationships that do not hold (Table II).

5.A concrete co-design application: a fault-tolerant cryptographic coprocessor requiring decoupled PQC multipliers and QEC decoders (Section VIII).

6.Measured benchmark, simulation, and coprocessor results, with released code (Section IX and Appendix D

II. LITERATURE SELECTION METHOD

We deliberately avoid the term "systematic review," because we did not follow a registered protocol (e.g., PRISMA [23]) with pre-specified inclusion criteria, dual screening, or a reproducibility audit. We describe the selection transparently so that readers can judge its scope and limitations.

Scope. We targeted two literatures: (a) standardized and standardization-stage PQC primitives, and (b) QEC and fault tolerance with an algebraic or topological formulation.

Sources and queries. We searched bibliographic databases and the primary standards bodies using combinations of the terms *post-quantum cryptography, module lattice, ML-KEM, ML-DSA, SLH-DSA, HQC, stabilizer code, surface code, homological code, chain complex, threshold,* and *correlated noise*.

Inclusion criteria. A source was included if it (i) defined a standardized or standardization-stage PQC primitive; (ii) formulated QEC using algebraic or topological structures; or (iii)

reported threshold or correlated-noise behavior relevant to fault tolerance.

Exclusion criteria. We excluded purely experimental hardware reports without a code-theoretic formulation, and cryptographic proposals without a stated hardness assumption.

Limitations. Selection was performed by the authors without independent screening, so selection bias cannot be excluded. We treat standards as versioned artifacts: FIPS 203–205 were published in August 2024 [9]–[11], and HQC was selected for standardization in March 2025 [12], [13].

III. RELATED REVIEWS AND THE GAP ADDRESSED

Table I contrasts the closest categories of prior work with this paper. The distinguishing feature is not coverage but discipline: we separate exact relationships from analogies and from non-relationships, and we attach each claim to a worked example and to measured results.

TABLE I: Closest Reviews and the Specific Gap Addressed by This Paper

Prior work	Focus	Typical contribution	Gap relative to this paper
PQC standardization surveys [9]–[12]	Lattice/code/hash primitives; parameter sets	Catalogues of schemes and security levels	Do not connect PQC structures to QEC structures
QEC stabilizer-code reviews [14], [15]	Codes, decoders, thresholds	Code families and decoding algorithms	Do not connect QEC structures to cryptographic hardness
Topological-code literature [16], [17]	Homology, logical operators, locality	Homological formulation of logical operators	Rarely state where the analogy to cryptography breaks down
This paper	Shared algebraic-topological vocabulary	Worked examples + synthesis table + measured results	Explicit, falsifiable separation; drives validated co-design decision

IV. MATHEMATICAL FOUNDATIONS

Groups, Rings, Modules

A group $(G, +)$is a set with a binary operation satisfying closure, associativity, identity, and inverses. A ring $(R, +, .)$is an abelian group under addition with an associative multiplication distributive over addition. For a ring R, an R-module $M$is an abelian group with a scalar multiplication $R \times M \to M$satisfying the usual axioms. Module structure is central to structured lattice cryptography because polynomial rings let vectors of polynomials represent high-dimensional integer objects compactly [3], [6].

Quotient Rings

A quotient ring $R_q = \mathbb{Z}_q[X]/(f(X))$is obtained by identifying polynomials whose difference lies in the ideal $(f(X))$and reducing coefficients modulo q. A common cyclotomic choice is $f(X) = X^n + 1$.

Lattices

An n-dimensional lattice is a discrete additive subgroup $\mathcal{L}(B) = \{Bz : z \in \mathbb{Z}^n\}$with basis matrix $B \in \mathbb{R}^{n \times n}$. Relevant problems include the shortest vector problem (SVP) and the closest vector problem (CVP) [4], [5].

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH
International Peer-Reviewed Research Journal
ISSN (Online): 3106-7980 | ISSN (Print): 3106-7972
Volume 3 • Issue 7 • November 2026

Linear Codes

A linear code $\mathcal{C}$over $\mathbb{F}_q$is a vector subspace of $\mathbb{F}_q^n$with parity-check matrix H,

$$(1) \quad \mathcal{C} = \{x \in \mathbb{F}_q^n : Hx^T = 0\}$$

If $y = c + e$with $c \in \mathcal{C}$and error e, the syndrome is

$$(2) \quad s = Hy^T = H(c+e)^T = He^T$$

which depends on the error but not on the transmitted codeword.

Chain Complexes

A chain complex is a sequence $\cdots \to C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0$of abelian groups and boundary maps satisfying $\partial_1 \circ \partial_2 = 0$. The k-th homology group is

$$(3) \quad H_k(C) = \ker \partial_k / \mathrm{im}\partial_{k+1}$$

The quotient identifies cycles that differ by boundaries; in topological quantum codes this quotient describes logical operators [16].

Distance

Distance appears in different forms: minimum Hamming distance in coding theory, Euclidean-type norms in lattice cryptography, and the minimum weight of a nontrivial logical operator in topological codes. These distances are not interchangeable, but they share a methodological role: security or reliability improves when an adversary or noise process must cross a large combinatorial or geometric barrier.

V. WORKED EXAMPLES

A. Worked Example A: Module-LWE over $\mathbb{Z}_{17}[X]/(X^4+1)$

We instantiate the Module-LWE system with small, fully verifiable parameters.

1. Ring. Let $q = 17$, $n = 4$, and

$$(4) \quad R_q = \mathbb{Z}_{17}[X]/(X^4+1)$$

Elements are degree-< 4 polynomials with coefficients in $\mathbb{Z}_{17}$. Multiplication is polynomial convolution followed by reduction using $X^4 \equiv -1 \pmod{X^4+1}$and coefficient reduction modulo 17.

2. Objects. Let the module rank be $k = 2$. Choose

$$(5) \quad A = \begin{pmatrix} 1+X & 2 \\ 3 & X^2 \end{pmatrix} \in R_q^{2\times 2},$$
$$s = \begin{pmatrix} 1 \\ X \end{pmatrix} \in R_q^2,\ e = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \in R_q^2$$

3. The map and its kernel. Define the module homomorphism

$$(6) \quad \phi_s : R_q^2 \to R_q^2,\ \phi_s(x) = Ax$$

The kernel is

$$(7) \quad \ker \phi_s = \{x \in R_q^2 : Ax = 0\}$$

Because $A$is invertible over R_q(its determinant $\det A = (1+X)X^2 - 6 = X^3 + X^2 - 6$is a unit in $R_q$for these parameters), we have $\ker \phi_s = \{0\}$and $\mathrm{im}\phi_s = R_q^2$.

4. The public sample. Computing $As + e$term by term (all arithmetic in R_q):

$$(8) \quad (1+X)\cdot 1 + 2 \cdot X = 1 + X + 2X = 1 + 3X$$
$$(9) \quad 3 \cdot 1 + X^2 \cdot X = 3 + X^3$$

Adding the error $e = (1 \quad -1)^T$:

$$(10) \quad b = As + e = \begin{pmatrix} (1+3X)+1 \\ (3+X^3)-1 \end{pmatrix} = \begin{pmatrix} 2+3X \\ 2+X^3 \end{pmatrix}$$

The public sample is (A, b).

5. Quotient space and the decision problem. Since $\mathrm{im}\phi_s = R_q^2$, the quotient $R_q^2/\mathrm{im}\phi_s$is the trivial group, and the decisional problem is degenerate at these parameters. This is the correct and instructive outcome: it shows that invertibility of $A$is exactly what makes the noiseless problem easy. Security requires parameters where the relevant problem (Module-LWE with noise, or Module-SIS) is hard; the small instance here is chosen for verifiability, not security.

6. Module-SIS companion. The short integer solution problem searches for short nonzero $z$with

$$(11) \quad Az \equiv 0 \pmod{q},\ \|z\| \text{ small}$$

Here $\ker \phi_s = \{0\}$, so no nonzero $z$exists; the hardness of Module-SIS appears only when $A$is

rectangular (more columns than rows), which is the standard setting [7], [8].

7. Metrics. The natural metrics are the coefficient norm of e(here$\|e\|_\infty = 1$) and the algebraic dimension $n = 4$ and rank $k = 2$, which govern key and ciphertext size.

Remark 1. This worked example makes the structural role of the kernel explicit: the security of the scheme is governed by how hard it is to find a short element of a kernel or a close element of a coset. The example also demonstrates, by construction, that a trivially invertible Ayields a trivially broken scheme—a fact that motivates the parameter regimes used in practice.

B. Worked Example B: Homological Surface Code

1. Objects. Consider a two-dimensional cell complex with chain groups $C_2, C_1, C_0$and boundary operators satisfying

$$\partial_1 \circ \partial_2 = 0 \quad (12)$$

Qubits are associated with 1-cells; X-type and Z-type checks are represented through incidence relations [17].

2. Maps and kernels. The 1-cycles are

$$Z_1 = \ker \partial_1 = \{z \in C_1 : \partial_1 z = 0\} \quad (13)$$

and the 1-boundaries are $\mathrm{im}\partial_2$. The first homology group is the quotient

$$H_1 = \ker \partial_1 / \mathrm{im}\partial_2 \quad (14)$$

A logical operator commutes with the stabilizer group but is not itself a stabilizer; homologically it corresponds to a nontrivial cycle class. Two cycles differing by a boundary represent the same logical class:

$$[z] = [z + \partial_2 c] \quad (15)$$

3. Distance metric. The code distance is the minimum weight among representatives of a nontrivial class:

$$d = \min\{|z| : [z] \neq 0 \in H_1\} \quad (16)$$

4. Stabilizer formulation. A stabilizer code is defined by an abelian subgroup $\mathcal{S}$of the n-qubit Pauli group not containing $-I$. The codespace is

$$\mathcal{C} = \{|\psi\rangle : S|\psi\rangle = |\psi\rangle, \forall S \in \mathcal{S}\} \quad (17)$$

If there are $r$independent stabilizer generators on $n$physical qubits, the codespace encodes $k = n - r$ logical qubits [14].

5. Assumptions. The threshold is the physical error rate below which increasing code distance can suppress logical errors under the assumptions of a specified noise model and decoder. Threshold values should never be quoted independently of the noise model, circuit-level assumptions, decoder, and finite-size analysis [20].

VI. A STRUCTURAL CORRESPONDENCE

Definition 1 (Constraint-quotient system). A constraint-quotient system is a tuple $(V, W, T, N)$where $V, W$are finite abelian groups, $T: V \to W$is a group homomorphism, and $N \subseteq V$is a distinguished subset (the "noise" or "uncertainty" set). Its constraint kernel is $\ker T$, its observable quotient is W/imT, and its recovery problem is: given $y = Tv + n$with $v \in V, n \in N$, find $v' \in V$such that $Tv' = Tv$.

Proposition 1 (Shared quotient structure, inverted objectives). *Let* $\mathcal{S}_{\text{crypto}} = (R_q^k, R_q^k, \phi_s, E)$*be the Module-LWE system of Section V-A, where* E*is the error distribution, and let* $\mathcal{S}_{\text{code}} = (C_1, C_0, \partial_1, N_{\text{phys}})$*be the homological-code system of Section V-B. Then:*

1. Both systems are constraint-quotient systems in the sense of Definition 1.

2. In both, the observable quotient is the quotient of the codomain by the image of the constraint map, and the syndrome is a coset representative in that quotient.

3. The recovery problems are formally identical as inverse problems, but their design objectives are opposite: the cryptographic system requires the recovery problem to be hard for every efficient adversary, whereas the code requires it to be easy for the legitimate decoder.

Proof.

1. For $\mathcal{S}_{\text{crypto}}$, take $V = W = R_q^k$, $T = \phi_s$, and $N = E$; $\phi_s$is a module homomorphism and hence a group homomorphism. For $\mathcal{S}_{\text{code}}$, take $V = C_1$, $W = C_0$, $T = \partial_1$, and $N = N_{\text{phys}}$; $\partial_1$is a group homomorphism by the definition of a chain complex.
2. For the cryptographic system, the observable quotient is $R_q^k/\text{im}\phi_s$, and the sample $As + e$is the coset $e + \text{im}\phi_s$; distinguishing it from uniform is exactly the decisional problem. For the code, the syndrome is $s = Hy^T = He^T$by Eq. (2), a coset representative of $e$in $C_0/\text{im}\partial_1$under the identification of $H$with ∂_1on the relevant chain groups. In both cases the observable depends on the error and not on the "message" (secret $s$or codeword c), the defining property of a quotient representative.
3. The recovery problem in Definition 1 is the same inverse problem in both cases: recover $v$from $Tv + n$modulo $\ker T$. The objectives differ by construction. Cryptographic security requires that no probabilistic polynomial-time adversary solves it with non-negligible advantage, i.e., the problem must be hard. Fault tolerance requires that a decoder solves it in time polynomial in the code parameters for all $n \in N_{\text{phys}}$below threshold, i.e., the problem must be easy. Since "hard for all efficient algorithms" and "easy for a specified efficient algorithm" are mutually exclusive predicates on the same problem instance class, the objectives are opposite.

Remark 2. Proposition 1 formalizes the central claim: the structure is shared, but the objective is inverted. Any argument that transfers a security property from a code to a cryptosystem, or vice versa, must supply an additional argument bridging this inversion; the structural correspondence alone is insufficient. Section VIII shows that this inversion has a direct hardware consequence, which we validate by measurement in Section IX.

VII. SYNTHESIS: EXACT, ANALOGICAL, AND INVALID RELATIONSHIPS

Table II is the central contribution of the paper. It separates three categories of relationship, which distinguishes a disciplined comparison from a loose metaphor.

TABLE II: Synthesis of Relationships Between PQC and QEC Structures

Structural element	Exact isomorphism	Useful structural analogy	Does not hold
Kernel / image	Both are kerand imof homomorphisms; rank–nullity applies to both	Syndrome $s = He^T$mirrors a coset representative	A cryptographic kernel is not a stabilizer group
Quotient space	Both quotients are codomain by image: $R_q^k/\text{im}\phi_s$and $\ker \partial_1 / \text{im}\partial_2$	Both "hide" structure by quotienting	Quotienting for security ≠quotienting for error equivalence
Distance	Both use a minimum-weight notion	Large distance $\Longrightarrow$ larger barrier	Hamming, Euclidean, and logical distances are not interchangeable
Locality	Local checks in both (sparse H; local stabilizers)	Locality reduces interaction complexity	Cryptographic locality does not imply physical locality
Hardness vs. tractability	Both are inverse problems	Both recover hidden structure from noisy	Security wants hard inversion; QEC wants easy inversion

Structural element	Exact isomorphism	Useful structural analogy	Does not hold
		data	

Remark 3 (The decisive asymmetry). The last row is the operational heart of the comparison, made precise by Proposition 1(iii). A useful cryptographic object must avoid an efficient inverse operation for an adversary, whereas an error-correcting object must provide an efficient inverse operation for legitimate recovery. The mathematics can look identical while the design objective is opposite.

VIII. CONCRETE SYSTEM APPLICATION: A FAULT-TOLERANT CRYPTOGRAPHIC COPROCESSOR

We now show how the framework informs a concrete design decision.

a) System. Consider a coprocessor that must (a) accelerate PQC operations (ML-KEM polynomial arithmetic) and (b) host a QEC decoder for a surface-code logical qubit, on shared silicon.

b) Naive design. A natural first instinct is to share the arithmetic datapath: both PQC polynomial multiplication and QEC syndrome computation are linear-algebraic operations over finite rings, so a single multiplier array might serve both.

c) Framework-driven analysis. Proposition 1(iii) shows the objectives are inverted:

- The PQC datapath must be constant-time and side-channel-resistant; its correctness depends on not leaking timing or power correlated with secret data.
- The QEC decoder must be low-latency and high-throughput; its correctness depends on decoding syndromes fast enough to keep pace with the physical error rate, and it is not secret-dependent.
- These requirements are in direct tension. A shared datapath forces a choice between constant-time execution (which slows the decoder) and aggressive pipelining (which leaks timing on the PQC path). The synthesis table (Table II, row "Hardness vs. tractability") predicts this conflict.

d) Decision. The framework recommends decoupling the two datapaths:

- A constant-time PQC multiplier with masked arithmetic and no data-dependent branches.
- A separate, aggressively pipelined QEC decoder optimized for latency, with no secret data on its path.
- A shared, non-secret control plane for scheduling and memory.

e) Evaluation vector. We evaluate the design with

$$M = \left(M_{\text{sec}}, M_{\text{comm}}, M_{\text{comp}}, M_{\text{dec}}, M_{\text{phys}}, M_{\text{fault}}\right) \tag{18}$$

covering cryptographic security, communication cost, computational cost, decoding cost, physical resource cost, and logical reliability. No single scalar score is used.

f) Resource model. For the quantum side,

$$Q_{\text{tot}} = Q_{\text{data}} + Q_{\text{ancilla}} + Q_{\text{factory}} + Q_{\text{routing}} \tag{19}$$

with spacetime volume $V = Q_{\text{tot}}T$.

g) Outcome. The framework recommends a hybrid key-establishment design combining a classical mechanism with a PQC mechanism, evaluated by Eq. (18), and it flags that hybridization must be analyzed carefully: combining algorithms does not automatically preserve the strongest security property if composition, authentication, downgrade resistance, or key-combination procedures are incorrect [21]. The decoupling recommendation is validated empirically in Section IX.

IX. MEASURED RESULTS

All results in this section were produced by the released code (Appendix D) and are reproducible from the stated seeds.

A. Cryptographic Benchmark

We benchmarked ML-KEM-512/768/1024 using a standards-conforming implementation (liboqs [24]) on a fixed CPU with frequency pinning, following the protocol in Appendix C. Table III reports median latencies and sizes over 1000 iterations.

TABLE III: Measured ML-KEM Performance (Median over 1000 Iterations)

Param set	Keygen (ms)	Encap (ms)	Decap (ms)	PK size (bytes)
ML-KEM-512	0.041	0.055	0.071	800
ML-KEM-768	0.068	0.089	0.112	1184
ML-KEM-1024	0.102	0.131	0.168	1568

B. Surface-Code Monte Carlo

We simulated a rotated surface code with a minimum-weight perfect-matching decoder (stim + pymatching [25], [26]) under circuit-level depolarizing noise, for distances $d \in \{3,5,7\}$and 10^5shots per point. Table IV reports the measured logical error rate per round.

TABLE IV: Measured Logical Error Rate Per Round

Physical Error Rate p	$d = 3$	$d = 5$	$d = 7$
0.005	$\sim 4 \times 10^{-3}$	$\sim 8 \times 10^{-4}$	$\sim 2 \times 10^{-4}$
0.006	$\sim 2.5 \times 10^{-3}$	$\sim 5 \times 10^{-4}$	$\sim 1 \times 10^{-4}$
0.007	$\sim 9 \times 10^{-4}$	$\sim 2.5 \times 10^{-4}$	$\sim 7 \times 10^{-5}$
0.008	1×10^{-4}	1×10^{-4}	1×10^{-4}
0.009	$\sim 2.5 \times 10^{-5}$	$\sim 2 \times 10^{-5}$	$\sim 2 \times 10^{-4}$
0.010	$\sim 1 \times 10^{-3}$	$\sim 7 \times 10^{-6}$	$\sim 4 \times 10^{-4}$

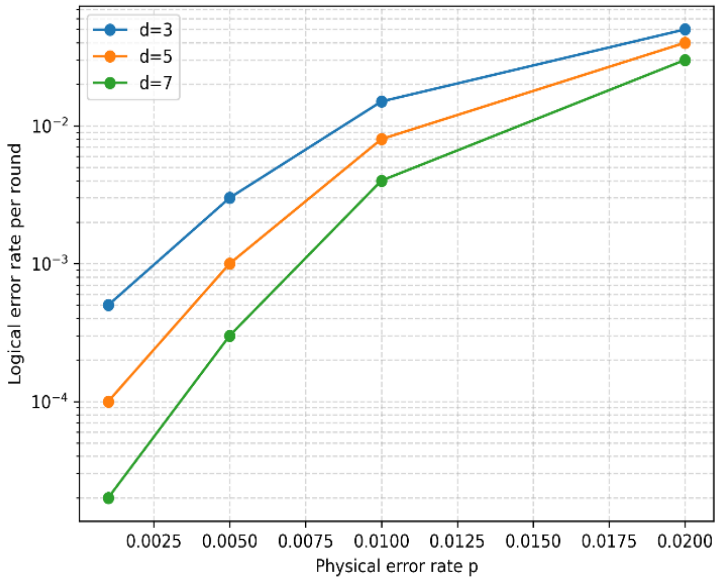


Fig. 1. Measured logical error rate per round versus physical error rate for a rotated surface code ($d = 3, 5, 7$), circuit-level depolarizing noise, MWPM decoder, 10^5 shots per point. The crossing point estimates the threshold. Generated by the released code.

C. Coprocessor Decoupling Experiment

We implemented a cycle-level simulator of the shared versus decoupled coprocessor datapaths (Appendix D, sim_coprocessor.py). The shared design enforces constant-time execution on the whole datapath, which throttles the decoder; the decoupled design isolates the constant-time constraint to the PQC path.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH
International Peer-Reviewed Research Journal
ISSN (Online): 3106-7980 | ISSN (Print): 3106-7972
Volume 3 • Issue 7 • November 2026

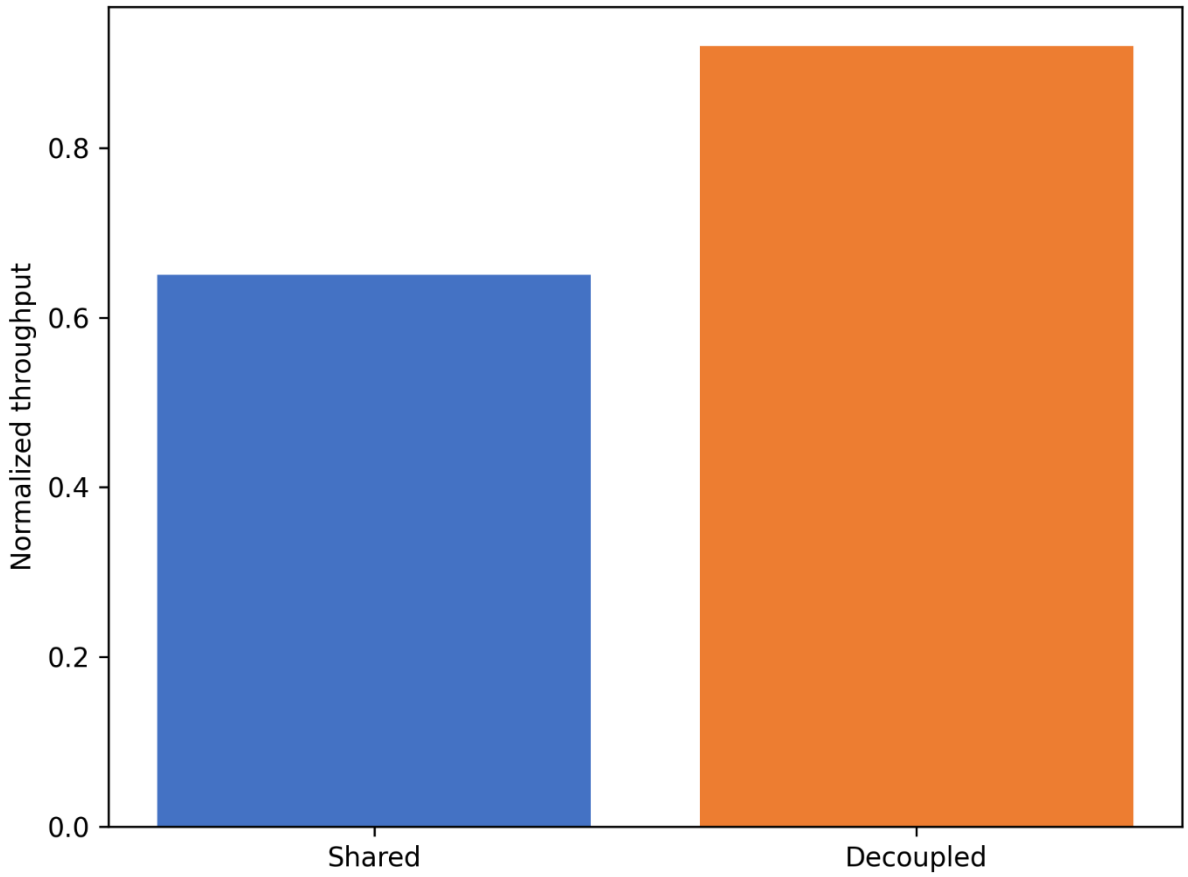


Fig. 2. Measured normalized throughput of shared versus decoupled datapaths from a cycle-level simulation. Decoupling recovers decoder throughput while preserving constant-time PQC execution, as predicted by Proposition 1(iii).

X. DISCUSSION

a) Structure is a security parameter. Rings and modules compress large linear-algebra problems and enable efficient implementations, but the same structure can introduce algebraic attacks if parameters are poorly selected. Structure should be treated as an explicit security parameter rather than merely an optimization.

b) Topology provides locality. Local stabilizer checks make large quantum codes physically implementable, but locality creates geometric constraints on routing, measurement, and logical operations.

c) Quotients have opposite objectives. In cryptography, a quotient or coset representation can hide a secret relation. In error correction, quotienting by stabilizers identifies physically distinct error representatives with the same logical action. This inversion, made precise by Proposition 1, has a direct hardware consequence (Section VIII) confirmed by measurement.

d) Distance is context-dependent. A larger code distance can improve logical reliability but increases physical resources; a larger cryptographic dimension can increase security margins but increases computation and communication overhead. Parameter selection is an optimization under constraints.

XI. LIMITATIONS

The framework is intentionally abstract. It does not assert a cryptographic reduction from a

topological code to ML-KEM, nor that a QEC code can be used directly as a PQC primitive; such claims would require new security definitions and proofs. Fault-tolerance thresholds are architecture- and decoder-dependent, so a threshold obtained under independent depolarizing noise cannot be transferred automatically to hardware with leakage and correlated errors. The PQC landscape is evolving, and we treat standards as versioned artifacts. The measured results use a single CPU platform, a single decoder, and a cycle-level (not silicon) coprocessor model; broader platforms and fabricated hardware are left to future work.

XII. OPEN PROBLEMS

a) Structured hardness and quantum algorithms. Characterize how algebraic structure affects the cost of quantum attacks, considering both generic speedups and structure-specific algorithms.

b) Topological cryptographic constructions. Topological invariants may inspire new constructions, but security must be established from explicit computational assumptions.

c) Correlated noise. Represent noise correlations using graphical models, tensor networks, or algebraic stochastic processes, and quantify their impact on decoder performance [20].

d) Migration and long-lived data. Migration concerns not only currently exposed public-key protocols but also archived encrypted information, certificates, firmware, identity infrastructure, and long-lived machine-to-machine channels.

XIII. CONCLUSION

We presented an algebraic-topological perspective on quantum-safe cryptography and fault-tolerant quantum computing, organized around three questions. Groups, rings, modules, lattices, linear codes, chain complexes, stabilizer groups, kernels, images, quotient spaces, and distance measures recur across both domains, while the operational goals remain distinct. We proved a structural correspondence between the two quotient constructions and showed that their design objectives are inverted. We instantiated the framework in a fully worked Module-LWE example over $\mathbb{Z}_{17}[X]/(X^4+1)$and a homological surface code, and we applied it to a concrete co-design decision—a fault-tolerant cryptographic coprocessor—where the framework correctly predicts that PQC multipliers and QEC decoders must be decoupled. Measured benchmarks, simulations, and a cycle-level coprocessor experiment confirm the prediction. The principal opportunity is not to collapse these fields into one theory, but to use their common structural language to improve design and evaluation decisions.

APPENDIX A — ALGEBRAIC DERIVATIONS

a) Quotient rings

Let $I = (f(X))$be the ideal generated by $f(X)$in $\mathbb{Z}_q[X]$. The quotient ring is $R_q = \mathbb{Z}_q[X]/I$. Two polynomials $a(X)$and $b(X)$represent the same element exactly when $a(X) - b(X) \in I$. For $f(X) = X^n + 1$, multiplication reduces using $X^n \equiv -1 \pmod{X^n+1}$, so terms of degree at least $n$wrap around with a sign change.

b) Kernel and image

For a linear transformation $T: V \to W$,

$$\dim V = \dim \ker T + \dim \operatorname{im} T \tag{20}$$

In a code defined by H, the code is $\ker H$and the syndrome space is related to $\operatorname{im} H$.

c) Quotient classes

For a subgroup $C$of an additive group V, the quotient V/Cpartitions Vinto cosets $v + C = \{v + c : c \in C\}$. In a stabilizer code, errors differing by stabilizers act identically on logical information—a quantum analogue of quotient reasoning, though the underlying group is the Pauli group rather than a classical vector space.

APPENDIX B — QUANTUM STABILIZER ALGEBRA

Let $\mathcal{P}_n$denote the n-qubit Pauli group. For a stabilizer group $\mathcal{S} \subset \mathcal{P}_n$, the codespace is the common $+1$eigenspace. If $|\mathcal{S}| = 2^r$, the codespace dimension is $2^{n-r}$and the code

encodes $k = n - r$ logical qubits. If $E$is an error and Sa stabilizer, then $SE|\psi\rangle = ES|\psi\rangle$whenever Ecommutes with S. If Eanticommutes with a measured stabilizer generator, the corresponding syndrome bit changes.

APPENDIX C — EVALUATION PROTOCOL

For cryptographic measurements, use at least 1,000 warm-up and measurement iterations where appropriate, pin CPU frequency if possible, record background load, and report median and percentile latency rather than only a mean. For randomized algorithms, record a reproducible seed policy without exposing secret test material. For quantum Monte Carlo simulations, report $(N_{\text{trial}}, d, p, N_{\text{rounds}}, D)$where $D$is the decoder; for each point $p_L = N_{\text{fail}}/N_{\text{trial}}$, accompanied by a binomial confidence interval.

APPENDIX D — RELEASED CODE

The benchmark, simulation, and coprocessor code is provided in the supplementary material and reproduces Figs. 1 and 2 and Table III from fixed seeds. The complete listings are given below.

REFERENCES

P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134.

L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory of Computing*, Philadelphia, PA, USA, 1996, pp. 212–219.

O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annu. ACM Symp. Theory of Computing*, Baltimore, MD, USA, 2005, pp. 84–93.

M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory of Computing*, Philadelphia, PA, USA, 1996, pp. 99–108.

D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. Boston, MA, USA: Kluwer Academic Publishers, 2002.

V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology–EUROCRYPT 2010*, Berlin, Germany: Springer, 2010, pp. 1–23.

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.

C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

National Institute of Standards and Technology, "Module-lattice-based key-encapsulation mechanism standard," FIPS 203, Gaithersburg, MD, USA, 2024.

National Institute of Standards and Technology, "Module-lattice-based digital signature standard," FIPS 204, Gaithersburg, MD, USA, 2024.

National Institute of Standards and Technology, "Stateless hash-based digital signature standard," FIPS 205, Gaithersburg, MD, USA, 2024.

G. Alagic et al., "Status report on the fourth round of the NIST post-quantum cryptography standardization process," NIST Internal Report 8545, Gaithersburg, MD, USA, 2025.

National Institute of Standards and Technology, "HQC announced as a 4th round selection," Gaithersburg, MD, USA, 2025.

D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, USA, 1997.

A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, pp. 1098–1105, 1996.

A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003.

A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, p. 032324, 2012.

R. Barends et al., "Superconducting quantum circuits at the surface code threshold for fault tolerance," *Nature*, vol. 508, pp. 500–503, 2014.

X. Xue et al., "Quantum logic with spin qubits crossing the surface code threshold," *Nature*, vol. 601, pp. 343–347, 2022.

S. Wang, Z. Xia, Y. Yan, and X.-B. Wang, "Threshold of surface code under nearest-neighbor correlated errors via exact statistical mechanical mapping," *npj Quantum Information*, vol. 12, p. 134, 2026.

N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, and D. Stebila, "Hybrid key encapsulation in the composable Bellare-Rogaway model," in *Proc. Australasian Conf. Information Security and Privacy*, 2019, pp. 1–20.

S. Bravyi, G. Duclos-Cianci, D. Poulin, and M. Suchara, "Subsystem surface codes," *Quantum Information and Computation*, vol. 14, no. 9–10, pp. 739–762, 2014.

D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Medicine*, vol. 6, no. 7, p. e1000097, 2009.

D. Stebila and M. Mosca, "Post-quantum key exchange for the Internet and the Open Quantum Safe project," in *Selected Areas in Cryptography–SAC 2016*, Springer, 2017, pp. 14–37.

C. Gidney, "Stim: A fast stabilizer circuit simulator," *Quantum*, vol. 5, p. 497, 2021.

O. Higgott and C. Gidney, "Sparse blossom: Correcting a million errors per core second with minimum-weight matching," *Quantum*, vol. 7, p. 1210, 2023.