УДК 621.391:519.2 **DOI:10.30837/rt.2025.4.223.13**

Y. KOTUKH

TOWARDS THE UNIFIED CRYPTOGRAPHIC COPROCESSOR ARCHITECTURE FOR POST-QUANTUM CRYPTOGRAPHY IN 6G NETWORK SETUP

Introduction

The rapid advancement of quantum computing technology presents unprecedented challenges to the security foundations of modern telecommunications infrastructure. Shor's algorithm, when executed on a sufficiently powerful quantum computer, can efficiently solve the mathematical problems underlying RSA and Elliptic Curve Cryptography (ECC) – the cryptographic primitives currently securing 5G networks and forming the basis for emerging 6G specifications [1]. The "harvest now, decrypt later" threat model, where adversaries collect encrypted data today for future decryption, makes the transition to quantum-resistant cryptography an urgent priority for telecommunications infrastructure [2].

In response to this threat, NIST completed its Post-Quantum Cryptography Standardization process in August 2024, publishing three initial standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [3]. Both ML-KEM and ML-DSA are based on the Module Learning with Errors (M-LWE) problem over lattices, sharing significant mathematical structure that can be exploited for efficient unified hardware implementations.

The 6G networks, expected to be deployed commercially around 2030, will require quantum-safe security from inception. The 3GPP and GSMA have initiated work on quantum-safe network specifications, with particular emphasis on the Authentication and Key Agreement (AKA) protocols that form the foundation of mobile network security [4]. These protocols require both key encapsulation mechanisms (for establishing shared secrets) and digital signatures (for authentication), making the efficient implementation of both ML-KEM and ML-DSA essential for 6G equipment.

This paper presents the following contributions: first, a novel unified architecture supporting all operations of ML-KEM-768 and ML-DSA-65 with runtime-configurable security levels; second, an optimized NTT engine with shared butterfly units supporting both q=3329 (ML-KEM) and q=8380417 (ML-DSA); third, a conflict-free memory management strategy enabling parallel polynomial operations; and finally, FPGA implementation results demonstrating suitability for 6G URLLC requirements.

Background and Related Work

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is specified in FIPS 203 and derived from the CRYSTALS-Kyber algorithm [5]. It provides three security levels: ML-KEM-512 (NIST Level 1), ML-KEM-768 (Level 3, recommended), and ML-KEM-1024 (Level 5). The algorithm operates on polynomials in the ring $R_q = Z_q[X]/(X^{256}+1)$ with q=3329, using 256-coefficient polynomials with 12-bit coefficients.

ML-DSA (Module-Lattice-Based Digital Signature Algorithm), specified in FIPS 204 and derived from CRYSTALS-Dilithium [6], similarly offers three security levels: ML-DSA-44, ML-DSA-65, and ML-DSA-87. It operates in the same polynomial ring structure but with q=8380417, requiring 23-bit coefficient representation. Both algorithms rely heavily on the Number Theoretic Transform (NTT) for efficient polynomial multiplication.

Number Theoretic Transform

The NTT is a finite-field analog of the Fast Fourier Transform (FFT) that enables polynomial multiplication in $O(n \log n)$ complexity instead of $O(n^2)$. For a polynomial a(x) of degree n-1, the forward NTT computes coefficients in the frequency domain using a primitive n-th root of unity modulo q. The Cooley-Tukey (CT) butterfly for forward NTT and Gentleman-Sande (GS) butterfly for inverse NTT form the computational core of these transforms [7].

Related Work

Several hardware implementations of individual PQC algorithms have been proposed. Kundi et al. [8] presented a high-performance NTT accelerator using Multi-path Delay Commutator (MDC) architecture achieving 322 MHz on Zynq UltraScale+. Mandal and Roy [9] introduced the KiD framework targeting unified NTT for Kyber and Dilithium. The TU Graz team developed the KaLi coprocessor [10] supporting both algorithms with side-channel attack countermeasures. However, existing unified designs either focus solely on the NTT engine or lack optimization for the specific requirements of 6G network equipment, particularly the stringent latency constraints of URLLC applications.

Proposed Unified Architecture

The proposed architecture, termed UniPQC (Unified Post-Quantum Cryptographic coprocessor), integrates all components necessary for complete ML-KEM and ML-DSA operations within a single hardware module. The architecture consists of the following sub-modules: (1) Unified Polynomial Arithmetic Module (UniPAM); (2) Hash and Sampling Unit (HSU); (3) Memory Management Unit (MMU); (4) Control and Configuration Logic (CCL).

This architecture supports runtime switching between ML-KEM and ML-DSA operations through configuration registers, enabling flexible deployment in network equipment that may require different cryptographic operations at different times. The CCL implements a finite state machine that coordinates the execution of all standard crypto operations for both algorithms.

Unified NTT Engine Design

The core innovation of our architecture lies in the unified NTT engine that efficiently supports both ML-KEM (q=3329, 12-bit coefficients) and ML-DSA (q=8380417, 23-bit coefficients) transforms. We employ a radix-2 decimation-in-frequency (DIF) architecture for forward NTT and decimation-in-time (DIT) for inverse NTT. The butterfly unit (BU) performs the Cooley-Tukey/Gentleman-Sande operations.

To achieve efficient modular reduction for both moduli, we implement a configurable Barrett reduction unit. For ML-KEM with q=3329, we utilize the special form $q = 13 \cdot 2^8 + 1$, enabling simplified reduction. For ML-DSA with $q = 2^{23} - 2^{13} + 1$, we exploit the sparse binary representation for efficient reduction using shift-and-add operations.

Our design employs four parallel butterfly units (4-BU configuration) enabling processing of 8 coefficients per clock cycle. The twiddle factors for both algorithms are pre-computed and stored in dedicated ROM blocks, with address generation logic selecting the appropriate factors based on the current operation mode.

Memory Architecture and Conflict Resolution

A key challenge in unified NTT design is the different memory requirements of ML-KEM and ML-DSA. We propose a banked memory architecture with 8 memory banks, each implemented as dual-port BRAM. For ML-KEM, coefficients are packed with 8 12-bit values per 96-bit memory word. For ML-DSA, 4 23-bit coefficients are stored per memory word with appropriate padding.

To eliminate memory access conflicts during NTT computation, we implement a conflict-free addressing scheme based on bit-reversal permutation combined with linear congruential mapping. The address generation unit computes bank indices and intra-bank addresses in parallel with butterfly operations, hiding memory access latency through pipelining.

Hash and Sampling Unit

Both ML-KEM and ML-DSA extensively use SHA-3 family functions (SHA3-256, SHA3-512, SHAKE128, SHAKE256). Our HSU implements a unified Keccak-f[1600] permutation core with configurable output modes. The sampling operations for matrix A generation (rejection sam-

pling) and error polynomial generation (centered binomial distribution for ML-KEM, uniform distribution for ML-DSA) are integrated with the SHAKE output processing.

The HSU achieves 2.5 Gbps throughput for SHAKE operations, sufficient for the sampling requirements of both algorithms. On-the-fly sampling eliminates the need to store intermediate SHAKE output, reducing memory requirements significantly.

Implementation and Results

The proposed UniPQC architecture was implemented in Verilog HDL and synthesized for Xilinx Zynq UltraScale+ ZCU102 FPGA using Vivado 2023.2. The design was verified through extensive simulation using test vectors from the NIST reference implementations of ML-KEM and ML-DSA. Hardware-software co-simulation was performed with the ARM Cortex-A53 processor acting as the host CPU.

Table 1

FPGA Resource Utilization

Module	LUTs	FFs	DSPs	BRAMs
UniPAM (NTT)	2,156	1,523	20	5
HSU (SHA-3)	1,645	1,287	0	0
MMU	456	312	0	3
CCL	255	123	4	0
Total UniPQC	**4,512**	**3,245**	**24**	**8**

Performance Analysis

Table 2 presents the cycle counts and latency for complete cryptographic operations at the recommended security levels (ML-KEM-768 and ML-DSA-65). The design achieves a maximum operating frequency of 285 MHz after place-and-route optimization.

Table 2

Operation Latency at 285 MHz

Operation	Cycles	Latency (μs)	Throughput
ML-KEM-768 KeyGen	8,542	29.97	33.4 kop/s
ML-KEM-768 Encaps	10,124	35.52	28.2 kop/s
ML-KEM-768 Decaps	11,856	41.60	24.0 kop/s
ML-DSA-65 KeyGen	15,234	53.45	18.7 kop/s
ML-DSA-65 Sign	42,567	149.36	6.7 kop/s
ML-DSA-65 Verify	18,923	66.40	15.1 kop/s

Comparison with Prior Work

The Area-Time Product (ATP) metric is computed using Equivalent Number of Slices (ENS) where 1 DSP = 100 Slices and 1 BRAM = 200 Slices. Our design achieves 34 % reduction in ATP compared to the sum of the best separate ML-KEM and ML-DSA implementations, while providing the flexibility of runtime algorithm selection.

Compared to the KaLi coprocessor [10], our design offers 15 % higher throughput for ML-KEM operations while using 12 % fewer resources. The improvement stems from our optimized memory architecture and conflict-free addressing scheme that enables better parallelization of NTT butterfly operations.

Suitability for 6G Network Equipment

The 6G URLLC requirements specify end-to-end latency targets of 100 μs to 1 ms for critical applications [11–15]. Our implementation achieves complete TLS 1.3 handshake (2×ML-KEM + 1×ML-DSA) in under 300 μs, leaving sufficient margin for network transmission and processing overhead.

The compact resource footprint enables integration into small-cell base stations and edge computing nodes where silicon area is constrained. Power consumption measurements on the ZCU102 platform indicate 245 mW during ML-KEM operations and 312 mW during ML-DSA signing, making the design suitable for power-constrained IoT gateway applications in 6G massive IoT deployments.

Conclusion

This paper presented UniPQC, a unified cryptographic coprocessor architecture supporting both NIST-standardized ML-KEM and ML-DSA post-quantum algorithms. By exploiting the shared mathematical structure of lattice-based cryptography, the proposed architecture achieves significant resource optimization compared to separate implementations while meeting the stringent performance requirements of emerging 6G network equipment.

The key innovations include a configurable NTT engine with dual-moduli support, conflict-free memory management, and efficient SHA-3 integration for sampling operations. FPGA implementation results demonstrate the viability of the approach for practical deployment, with latency figures compatible with 6G URLLC requirements.

Future work will extend the architecture to support additional PQC algorithms (HQC, FN-DSA) for crypto-agility and investigate side-channel attack countermeasures suitable for high-throughput operation. ASIC implementation targeting 28nm technology node is also planned to further reduce power consumption for battery-powered devices.

References

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Proc. 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134. https://doi.org/10.1109/SFCS.1994.365700

2. Mosca M. Cybersecurity in an era with quantum computers: Will we be ready? // IEEE Security & Privacy. 2018. Vol.16(5). P. 38–41. https://doi.org/10.1109/MSP.2018.3761723

3. NIST. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203. https://csrc.nist.gov/pubs/fips/203/final

4. GSMA. (2024). Post Quantum Telco Network Impact Assessment. White Paper. https://www.gsma.com/security/pqtn/

5. Avanzi R. et al. (2022). CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation. NIST PQC Submission.

6. Ducas L. et al. (2022). CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation. NIST PQC Submission.

7. Longa P., & Naehrig M. Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography // CANS 2016, LNCS. Vol. 10052. P. 124–139. https://doi.org/10.1007/978-3-319-48965-0_8

8. Kundi D. E. S., Mera J. M. B., Strub P.-Y., & Hutter M. (2024). High-Performance NTT Hardware Accelerator to Support ML-KEM and ML-DSA // Proc. ASHES '24. 2024. P. 100–105. https://doi.org/10.1145/3689936.3694706

9. Mandal S., & Roy D. B. KiD: A Hardware Design Framework Targeting Unified NTT Multiplication for CRYSTALS-Kyber and CRYSTALS-Dilithium on FPGA // Proc. VLSID. 2024. P. 455–460. https://doi.org/10.1109/VLSID60093.2024.00089

10. Aikata S. et al. KaLi: A crypto coprocessor for Kyber and Dilithium with side-channel protection // IACR TCHES. 2024. Vol. 1. P. 291–325. https://doi.org/10.46586/tches.v2024.i1.291-325

11. ITU-R. (2023). Framework and overall objectives of the future development of IMT for 2030 and beyond. Recommendation ITU-R M.2160.

12. NIST. (2024). Module-Lattice-Based Digital Signature Standard. FIPS 204. https://csrc.nist.gov/pubs/fips/204/final

13. Truong H. T. et al. High-performance Unified Hardware Architecture for ML-DSA and ML-KEM PQC Standards // IEEE Access. 2025.https://doi.org/10.1109/ACCESS.2025.3628733

14. 3GPP. (2024). Study on quantum-safe security in the 5G System (5GS). TR 33.848, Release 19.

15. Di Matteo S., Sarno I., & Saponara S. CRYPHTOR: A Memory-Unified NTT-Based Hardware Accelerator for Post-Quantum CRYSTALS Algorithms // IEEE Access. 2024. Vol. 12, P. 25501–25511. https://doi.org/10.1109/ACCESS.2024.3367230

16. Khalimov G., Kotukh Y., Kolisnyk M., & Khalimova S., Sievierinov O. LINE: Cryptosystem based on linear equations for logarithmic signatures // Cryptology ePrint Archive: Report 2024/697. 2024. https://ia.cr/2024/697

17. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., Sievierinov O., & Korobchynskyi M. Digital signature scheme based on linear equations // K. Arai (Ed.). Advances in Information and Communication. FICC 2025. Lecture Notes in Networks and Systems. 2025. Vol. 1285. Springer. https://doi.org/10.1007/978-3-031-84460-7_46

18. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., Sievierinov O., & Volkov O. SIGNLINE: Digital signature scheme based on linear equations cryptosystem // 2024 4th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). 2024. P. 1–9. IEEE. https://doi.org/10.1109/ICECCME62383.2024.10796704

19. Kotukh Y., Severinov E., Vlasov O., Tenytska A., & Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Radiotekhnika. 2021. №204. P. 66–72.

20. Kotukh Y., & Khalimov G. Hard problems for non-abelian group cryptography // Fifth International Scientific and Technical Conference "Computer and Information Systems and Technologies". 2021. https://doi.org/10.30837/csitic52021232176

21. Kotukh Y., Khalimov G., Dzhura I., & Hivrenko H. (2025). Application of the LINE encryption scheme in the key encapsulation mechanism for the authentication protocol in 5G networks // Radiotekhnika. 2025. № 219. P. 36–45. https://doi.org/10.30837/rt.2024.4.219.04

22. Kotukh Y., Khalimov G., Korobchynskyi M., Rudenko M., Liubchak V., Matsyuk S., & Chashchyn M. Research horizons in group cryptography in the context of post-quantum cryptosystems development // Radiotekhnika. 2024. №216. P. 62–72. https://doi.org/10.30837/rt.2024.1.216.05

23. Kotukh Y., & Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: Problems and prospects. 2022. P. 55–60.

24. Khalimov, G., & Kotukh, Y. (2025). MST3 encryption improvement with three-parameter group of Hermitian function field // arXiv preprint arXiv:2504.15391. https://arxiv.org/abs/2504.15391

25. Khalimov G., & Kotukh Y. (2025). Advanced MST3 encryption scheme based on generalized Suzuki 2-groups // arXiv preprint arXiv:2504.11804. https://arxiv.org/abs/2504.11804

Надійшла до редколегії 11.10.2025

Відомості про автора:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X