УДК 004

ANALYSIS AND DEVELOPMENT OF A DATA TRANSMISSION SYSTEM USING LOW-LEVEL PROGRAMMING LANGUAGES: CONCEPTUAL AND EXPERIMENTAL FOUNDATIONS

M. R. Satanov

Joint Stock Company «Kazakh National Research Technical University named after K. I. Satbayev», Almaty, Republic of Kazakhstan

The development of secure data transmission systems is a crucial task in the modern digital infrastructure, especially under the threat of quantum computing. Conventional algorithms such as RSA and ECC are expected to be vulnerable to quantum attacks. Kyber, a lattice-based post-quantum cryptographic algorithm standardized by NIST [1], provides an efficient and secure foundation for encryption key exchange in next-generation networks. To improve the performance of Kyber's mathematical operations, this work introduces polyhedral optimization – a formal method that analyzes and transforms loop-based computations to exploit parallelism and reduce execution time.

The goal of the research is to develop and evaluate a low-level implementation of a secure data transmission system that integrates Kyber for quantum-resistant key exchange and polyhedral optimization for computational efficiency.

Data exchange within the system is organized as a series of asynchronous message transmissions, each securely encapsulated to guarantee integrity and confidentiality. The logical connections between components, including data flow directions and integration points, are illustrated in Figure 1, which presents the overall conceptual architecture of the implemented solution.

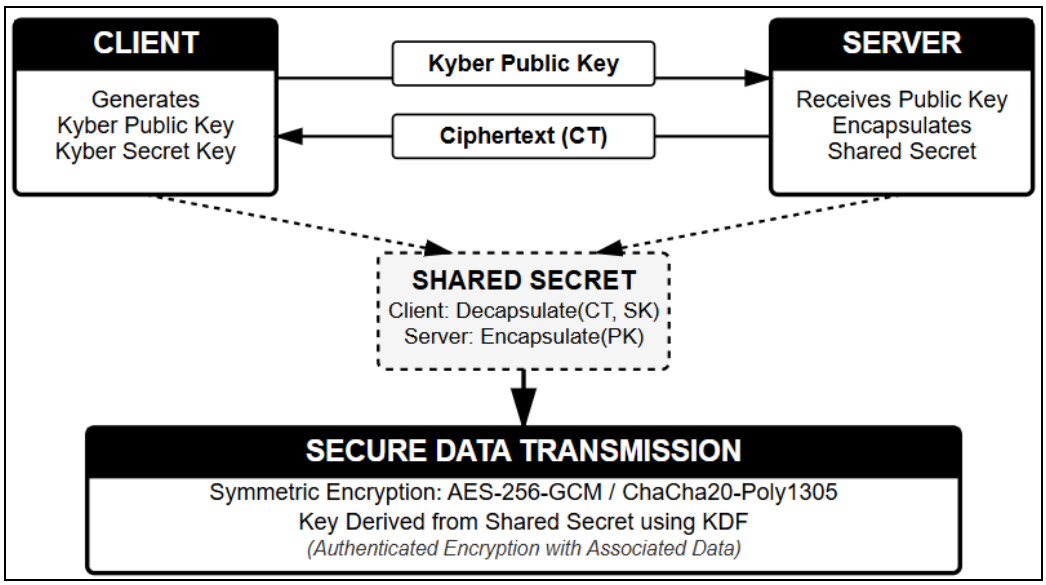

Figure 1 – System Architecture Overview

System concept and implementation approach.

The system is divided into three functional layers:

1. low-level layer. Implemented in Rust for direct access to hardware and memory-level control. This enables efficient handling of network I/O and precise optimization of the Kyber algorithm's arithmetic routines [2];

2. cryptographic layer. Utilizes Kyber for key encapsulation, providing a secure exchange of symmetric session keys [3]. After key exchange, data is encrypted with AES-256 for performance efficiency during continuous communication;

3. optimization layer. The polyhedral model is applied to Kyber's computationally intensive parts, specifically the Number Theoretic Transform (NTT) used in polynomial multiplications [4].

This approach restructures NTT loops to execute concurrently without violating data dependencies, improving throughput and cache efficiency.

To enhance performance and demonstrate computational optimization, a polyhedral representation of the encryption process is used. This approach allows the parallelization of independent computations by mapping them into geometric regions where dependencies can be analyzed and optimized. The model provides a structured visualization of how multiple encryption tasks can be executed concurrently without violating data consistency or synchronization constraints.

A schematic view of this polyhedral model is shown in Figure 2, where each node corresponds to a computational block, and the edges represent dependency relationships. This representation highlights how parallel execution paths are formed within the process, improving both efficiency and resource utilization.

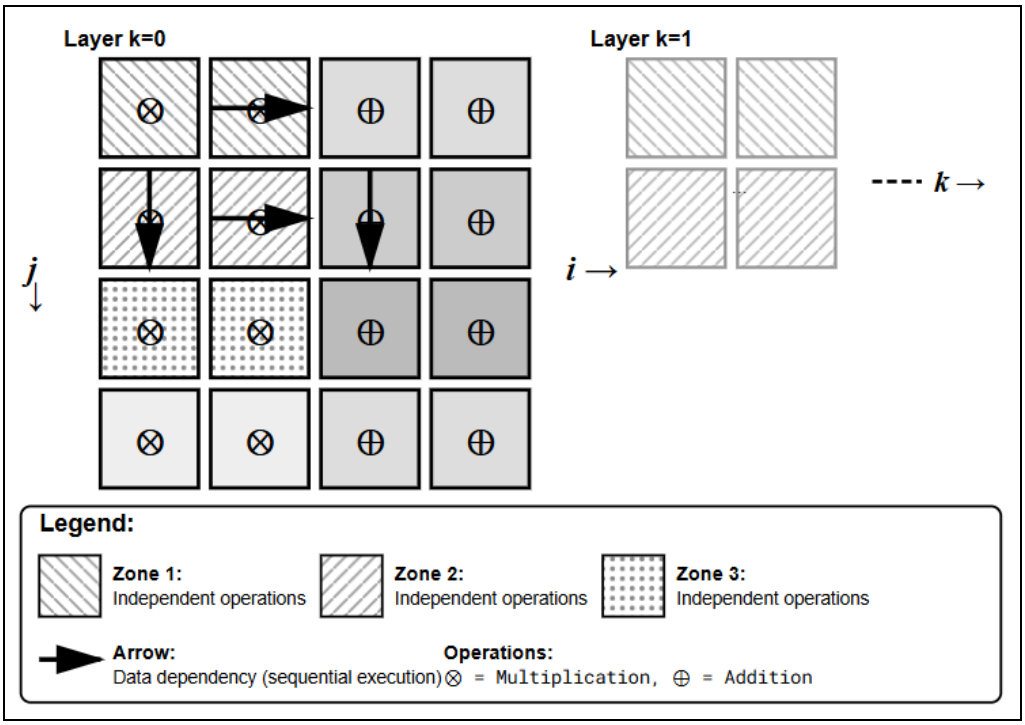

Figure 2 – Polyhedral Representation of NTT

In the polyhedral model, each operation is represented as a point in a multidimensional space (a «polyhedron»), where dependencies between iterations are analyzed geometrically [5].

This allows the compiler or the developer to automatically derive an optimized iteration schedule – in this case, minimizing redundant modular multiplications and improving cache coherence.

As a result, cryptographic transformations such as NTT can achieve significant acceleration, particularly when executed on multicore or GPU architectures.

Experimental and research perspective.

The developed system serves primarily as an experimental platform for testing optimization methods in post-quantum cryptography.

It provides:

– tools for measuring the performance of Kyber operations with and without polyhedral optimization;

– profiling at the instruction level;

– and comparison of different compiler-based transformation techniques (such as loop interchange, skewing, or tiling).

This experimental design allows researchers to visualize how algorithmic parallelism translates into practical performance gains on real hardware.

Conclusion.

The presented system demonstrates the feasibility of combining low-level programming, post-quantum cryptography, and polyhedral optimization techniques into a unified data transmission framework.

While the current stage of the research is primarily experimental, the results can be extended toward practical implementations in embedded systems, secure IoT devices, or distributed computation networks.

Scientific novelty of this work lies in the application of the polyhedral optimization method to accelerate key cryptographic operations within a post-quantum algorithm, while maintaining the low-level control required for system-level security implementations.

Practical significance lies in the creation of a flexible experimental environment for further research and teaching purposes in the domain of secure data transmission and computational cryptography.

References:

1. A. Abdulrahman, V. Hwang, M. J. Kannwischer, and A. Sprenkels, «Faster Kyber and Dilithium on the Cortex-M4,» in Proc. Applied Cryptography and Network Security (ACNS 2022), Rome, Italy, June 2022, pp. 853-871.

2. T. Kamucheka, A. Nelson, D. Andrews, and M. Huang, «A Masked Pure-Hardware Implementation of Kyber Cryptographic Algorithm,» in Fourth PQC Standardization Conference, NIST, Nov. 2022, pp. 1-1.
3. M. Kumar, «Post-quantum cryptography algorithm's standardization and performance analysis,» Array, vol. 15, Art. 100242, Sep. 2022. URL: https://doi.org/10.1016/j.array.2022.100242 (accessed: Nov. 01, 2025).
4. K. Kreuzer, «Verification of the (1–δ)-Correctness Proof of CRYSTALS-KYBER with Number Theoretic Transform,» in Proc. FAVPQC 2022: International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols, Madrid, Spain, Oct. 2022. URL: https://eprint.iacr.org/2023/027 (accessed: Oct. 20, 2025).
5. W. Tan, Y. Lao, and K. K. Parhi, «KyberMat: Efficient Accelerator for Matrix-Vector Polynomial Multiplication in CRYSTALS-Kyber Scheme via NTT and Polyphase Decomposition,» arXiv preprint arXiv:2310.04618, Oct. 2023. URL: https://arxiv.org/abs/2310.04618 (accessed: Sep. 21, 2025).