POST QUANTUM CRYPTOGRAPHY FOR HARDWARE EFFICIENT RISC-V ACCELERATORS

Project Reference No.: *49S_BE_4068*

College : Alliance University, Bengaluru
Branch : Department of Electronics and Communication Engineering
Guide(s) : Dr. Srikanth Itapu
Student(s) : Ms. G. Rashmitha
Ms. K. Praneetha
Mr. G. Vamsi Ram
Mr. V. Amarnath

Keywords:

Hardware Accelerator, Kyber Algorithm, NTT, Post Quantum Cryptography, RISC-V

Introduction:

The rapid advancement of quantum computing poses a serious threat to traditional cryptographic systems used in modern digital communication. Conventional public key encryption methods rely on mathematical problems such as integer factorization and discrete logarithms, which can be efficiently solved using quantum algorithms like **Shor's algorithm** and **Grover's algorithm**. This creates a need for new cryptographic techniques that are secure against quantum attacks.

Post-Quantum Cryptography (PQC) focuses on developing such secure algorithms. Among these, the **CRYSTALS-Kyber** algorithm is a lattice-based cryptographic scheme that has been selected by NIST for standardization due to its strong security and efficiency.

However, implementing Kyber efficiently requires handling computationally intensive operations such as polynomial multiplication and modular arithmetic. To address this, hardware acceleration techniques are used to improve performance and reduce latency.

This project focuses on the design and development of a hardware-efficient system for Kyber using a **RISC-V** based architecture. The system integrates a processor with a dedicated accelerator and utilizes optimized techniques such as the **Number Theoretic Transform** to enhance computational efficiency. The implementation is carried out on FPGA to evaluate performance improvements in terms of speed, resource utilization, and scalability.

The overall goal is to develop a secure and efficient post-quantum cryptographic system suitable for future applications in areas such as secure communication, defense systems, and embedded platforms.

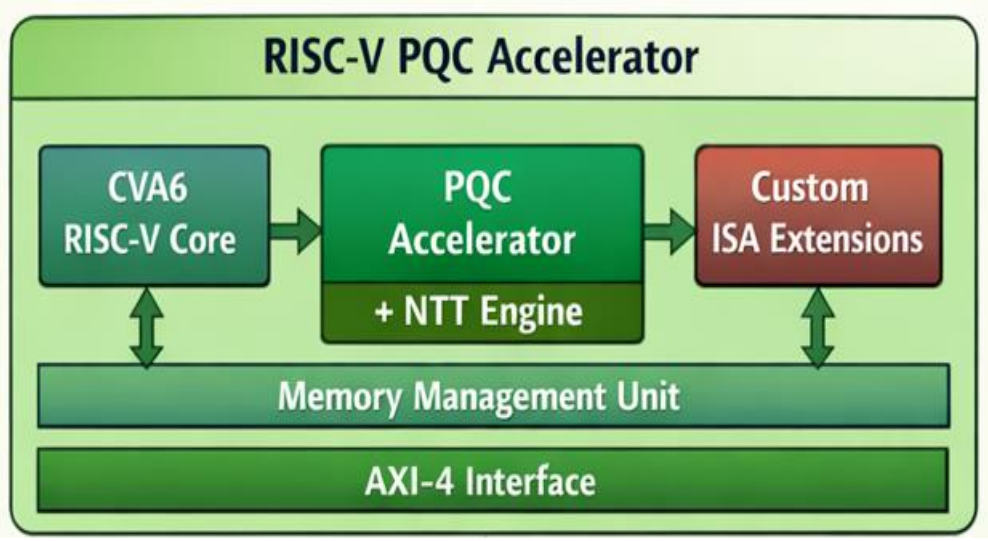

Figure 1: Proces flow in RISC-V PQC Accelerator.

Objectives:

1. To study and understand the CRYSTALS-Kyber algorithm
2. To implement Number Theoretic Transform (NTT) and Inverse NTT (INTT)
3. To design hardware modules using Verilog for modular arithmetic operations
4. To verify the design using Vivado simulation

Methodology:

1. The proposed system focuses on the hardware implementation of the Number Theoretic Transform (NTT), which is a key computational component of the CRYSTALS-Kyber algorithm. Instead of implementing the complete cryptosystem, the work concentrates on designing an efficient NTT module using Verilog.
2. The design is developed using a modular approach. Basic arithmetic units such as modular addition, subtraction, and multiplication are first implemented. These modules are then combined to form the butterfly unit (CTBF), which is the fundamental building block of the NTT.
3. A 4-point NTT architecture is constructed using multiple butterfly units. Similarly, an inverse NTT (INTT) module is designed to reconstruct the original input from the transformed values.
4. The entire design is implemented in Verilog and simulated using Vivado tools. The correctness of the system is verified by comparing the input values with the output obtained after performing NTT followed by INTT.
5. This approach demonstrates how NTT can be efficiently implemented in hardware and used as a core component in post-quantum cryptographic accelerators.

Result and Conclusion:

1. The NTT and INTT modules were successfully implemented using Verilog and simulated in Vivado. The results show that the INTT output is close to the original input after applying NTT followed by INTT, confirming the correctness of the design.

2. The modular arithmetic blocks and butterfly structure function properly within the system. This work demonstrates that the Number Theoretic Transform can be efficiently implemented in hardware and used as a core component in post-quantum cryptographic systems.

References:

1. National Institute of Standards and Technology, *"CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation,"* 2023.
2. Joppe Bos et al., *"CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM,"* IEEE European Symposium on Security and Privacy, 2018.
3. Leo Ducas et al., *"CRYSTALS-Kyber: Algorithm Specifications and Design Rationale,"* NIST PQC Submission, 2021.
4. Xilinx, *"Vivado Design Suite User Guide,"* 2022.
5. RISC-V Foundation, *"The RISC-V Instruction Set Manual,"* 2019.

Future Scope:

The future scope of this project includes:

1. To extend the current work to higher-point NTT implementations (8-point, 16-point)
2. To optimize the NTT architecture for better speed and area efficiency
3. To integrate the NTT module with RISC-V based systems for real-time applications
4. To implement the design on FPGA/ASIC platforms for improved performance