EGCI491: Assignment II

Pakin Panawattanakul 6580043

February 2, 2025

Chapter 2
Literature Review

Provide a brief description of what this chapter covers. It is typically an outline of a comprehensive literature review for the whole project. All related papers and previous works should be reviewed. You should summarize the main contributions, techniques used, data, key findings, and research gaps of each paper.

2.1 NIST Post-Quantum Cryptography – A Hardware Evaluation Study [1]

This paper provides an in-depth evaluation of the hardware performance of NIST's Post-Quantum Cryptography (PQC) candidates, focusing on both FPGA and ASIC implementations. With the rapid advancements in quantum computing, conventional cryptographic algorithms such as RSA and ECC are becoming increasingly vulnerable, necessitating the development of efficient and secure quantum-resistant alternatives. The National Institute of Standards and Technology (NIST) has been leading the PQC standardization process, and this study critically examines the feasibility of implementing these algorithms in hardware.

The paper evaluates multiple PQC algorithms shortlisted by NIST, including lattice-based, hash-based, code-based, and multivariate cryptosystems. Key performance metrics such as resource utilization, power consumption, latency, and computational throughput are analyzed across different hardware platforms. FPGA implementations are shown to offer significant flexibility, parallel processing capabilities, and adaptability for PQC acceleration, while ASIC-based solutions provide better power efficiency and lower area overhead, making them suitable for energy-constrained environments.

Experimental results indicate that lattice-based cryptographic schemes, particularly Kyber and Dilithium, achieve a good balance between security and efficiency, with FPGA implementations leveraging optimized arithmetic units and pipelined architectures for enhanced performance. Mean-

while, hash-based and code-based schemes exhibit higher memory and computational demands, posing challenges for real-world deployment. Security concerns, such as potential side-channel attack vulnerabilities, are also discussed, emphasizing the need for additional countermeasures.

In conclusion, this study provides a comprehensive comparison of hardware-based PQC implementations, highlighting both strengths and limitations. Future research should focus on optimizing FPGA architectures, improving resource utilization, and integrating countermeasures against physical attacks. This work serves as a reference for researchers and engineers designing secure and efficient cryptographic hardware solutions for the post-quantum era.

2.2 FPGA Accelerated Post-Quantum Cryptography [4]

This paper presents a comprehensive survey on FPGA-based implementations of Post-Quantum Cryptography (PQC), highlighting key advancements, methodologies, and security considerations. With the emergence of quantum computing, traditional cryptographic systems such as RSA and ECC face vulnerabilities, necessitating quantum-resistant alternatives. The National Institute of Standards and Technology (NIST) has progressed into the fourth round of PQC standardization, emphasizing the importance of efficient hardware implementations.

FPGA technology has emerged as a promising platform for accelerating PQC algorithms due to its reconfigurability, parallel processing capabilities, and hardware-software co-optimization. This paper surveys state-of-the-art FPGA implementations, focusing on fast arithmetic techniques, architectural optimizations, and open-source PQC hardware projects. Additionally, it discusses algorithm-hardware codesign strategies, which enhance computational efficiency and adaptability.

Experimental evaluations of FPGA-based PQC implementations demonstrate significant improvements in performance and resource utilization compared to general-purpose hardware. Optimized modular arithmetic units, deep pipeline architectures, and memory-efficient designs contribute to lower latency and improved power efficiency. However, challenges such as scalability, security vulnerabilities, and standardization gaps remain key areas for future research.

In conclusion, this survey provides a detailed analysis of current FPGA-based PQC implementations, emphasizing both performance optimization and security challenges. The paper aims to inform future research on designing efficient and secure FPGA accelerators for PQC, paving the way for widespread adoption of quantum-resistant cryptographic solutions.

2.3 Post-quantum cryptography Algorithm's standardization and performance analysis [3]

This paper proposed an analysis on the feasiblity of various quantum-safe cryptography alogirthms.

The performance analysis of the algorithm is done using the Open Quantum Safe (OQS) Project. It is a project , developing and prototyping quantum-resistanct cryptography algorithms.It provides bechmarking data such as the algorithm's runtime behavior and memory consumption. these are collected based on the execution on Amazon Web Service (AWS) with CPU Model Intel(R) Xeon (R) Platinum 8259CL CPU @ 2.50 GHz.

The data is from the NIST(National Institute of Standards and Technology) process to solicit, evaluate, and standardize the quantum-resistant cryptographic algorithms is published. The paper gives a comparative analysis of 7 finalist and 8 alternate quantum-resistant algorithms during the 3rd round in the year 2020.

The analysis shows that Lattice-based cryptography seem to be the most promising and quantum-safe. The algorithm is relatively efficient in implementation and has a very strong security proofs based on worst-case hardness. The maximum number of algorithms announced by NIST in 3rd round belongs to the lattice-based cryptography family.

The future work is to further evaluate the result of the 4th round evaluation of the process of Post Quantum Cryptography standardization. With early preparation and thorough planning, migration to post-quantum cryptographic alogrithms should be implement at the earlist due to the exponential growth in quantum computer's development.

2.4 Efficient and Scalable FPGA-Oriented Design of QC-LDPC Bit-Flipping Decoders for Post-Quantum Cryptography [6]

2.5 Low latency FPGA implementation of NTT for Kyber [5]

2.6 High-performance area-efficient polynomial ring processor for CRYSTALS-Kyber on FPGAs [2]

Reference

[1] Kanad Basu, Deepraj Soni, Mohammed Nabeel, and Ramesh Karri. NIST post-quantum cryptography- a hardware evaluation study. Cryptology ePrint Archive, Paper 2019/047, 2019. URL `https://eprint.iacr.org/2019/047`.

[2] Zhaohui Chen, Yuan Ma, Tianyu Chen, Jingqiang Lin, and Jiwu Jing. High-performance area-efficient polynomial ring processor for crystals-kyber on fpgas. *Integration Volume 78*, 2021. doi: 10.1016/j.vlsi.2020.12.005.

[3] Manish Kumar. Post-quantum cryptography algorithm's standardization and performance analysis. *Array Volume 15*, 2022. doi: 10.1016/j.array.2022.100242.

[4] He Li, Yongming Tang, Zhiqiang Que, and Jiliang Zhang. Fpga accelerated post-quantum cryptography. *IEEE Transactions on Nanotechnology (Volume: 21)*, pages 685 – 691, 2022. doi: 10.1109/TNANO.2022.3217802.

[5] Mohamed Saoudi, Akram Kermiche, Omar Hocine Benhaddad, Nadir Guetmi, and Boufeldja Allailou. Low latency fpga implementation of ntt for kyber. *Microprocessors and Microsystems Volume 107*, 2024. doi: 10.1016/j.micropro.2024.105059.

[6] David Zoni, Andre Gamlimberti, and William Fornaciari. Efficient and scalable fpga-oriented design of qc-ldpc bit-flipping decoders for post-quantum cryptography. *IEEE Access, vol. 8, pp. 163419-163433*, 2020. doi: 10.1109/ACCESS.2020.3020262.