CHAPTER 1
LITERATURE REVIEW

The literature review provides a brief overview of FPGA-based implementations of Post-Quantum Cryptography (PQC). It summarizes key contributions, techniques, and findings from previous research, focusing on advancements in hardware acceleration, security considerations, and performance optimizations. Additionally, it identifies research gaps and areas for future exploration, establishing a foundation for further study.

1.1 Post-quantum cryptography Algorithm's standardization and performance analysis [1]

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 study provides insights into 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 algorithms should be implement at the earlist due to the exponential growth in quantum computer's development.

1.2 FPGA Accelerated Post-Quantum Cryptography [2]

While the previous study focused on the efficiency of Post-Quantum cryptographic algorithms on traditional hardware, this paper shifts the focus to FPGA-based implementations of PQC. Given the vulnerabilities of RSA and ECC in the quantum era, FPGA technology has emerged as a powerful platform for accelerating PQC algorithms due to its parallel processing capabilities, and hardware-software co-optimization.

This paper presents a comprehensive survey on FPGA-based implementations of Post-Quantum Cryptography (PQC), highlighting key advancements, methodologies, and security considerations. Additionally, it explores algorithm-hardware design strategies that enhance computational efficiency and adaptability. Experimental evaluations show that FPGA implementations achieve significant improvements in performance and resource utilization compared to general-purpose hardware.

However, despite these advancements, challenges remain. Scalability issues, security vulnerabilities, and gaps in standardization pose key obstacles to widespread adoption. This paper emphasizes that addressing these concerns through optimized modular arithmetic units, deep pipeline architectures, and memory-efficient designs can lead to lower latency and improved power efficiency.

1.3 Quantum-Resistant Cryptography in FPGA [3]

Building upon the findings of FPGA acceleration research, this study introduces an FPGA-based implementation of CRYSTALS-Kyber, a quantum-resistant key encapsulation mechanism selected by NIST for post-quantum cryptography standardization. The research presents a reconfigurable CRYSTALS-Kyber accelerator designed using High-Level Synthesis (HLS) technology to enhance performance and efficiency on FPGA hardware.

The accelerator requires approximately 2200 LUTs, 3001 FFs, and 28 DSPs on a low-cost Zynq FPGA (XC7Z020-1CLG400C), operating at 100 MHz. Experimental results indicate that the key exchange process is completed in approximately 0.84 ms, with an estimated power consumption of 1.695W. The study highlights the advantages of FPGA-based cryptographic implementations, such as improved execution speed, reconfigurability, and efficient hardware utilization.

Further discussions focus on integrating the Number Theoretic Transform (NTT) to enhance the efficiency of polynomial multiplication, which is a key component of lattice-based cryptography. The paper concludes that leveraging HLS tools enables efficient post-quantum cryptographic hardware designs, providing flexibility while maintaining competitive performance. Future work aims to optimize the polynomial multiplication function and implement additional cryptographic operations on FPGA to further enhance security and efficiency.

REFERENCES

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

[2] H. Li, Y. Tang, Z. Que, and J. Zhang. Fpga accelerated post-quantum cryptography. *IEEE Transactions on Nanotechnology (Volume: 21)*, pages 685 -- 691, 2022. doi: 10.1109/TNANO.2022.3217802.

[3] R. C. Policarpo, A. S. Nery, and R. de O. Albuquerque. Quantum-resistant cryptography in fpga. *7th Workshop on Communication Networks and Power Systems (WCNPS 2022)*, 2022. doi: 10.1109/WCNPS56355.2022.9969738.