# EGCI491: Assignment II

Enter your name here

February 2, 2025

# Chapter 2
# Literature Review

This chapter provides a comprehensive review of the literature on FPGA-based implementations of Post-Quantum Cryptography (PQC). It highlights the growing need for quantum-resistant cryptographic solutions due to the vulnerabilities of traditional cryptographic systems like RSA and ECC in the face of quantum computing advancements. The chapter focuses on two major works in this area, exploring their contributions, techniques, data, key findings, and research gaps

## 2.1 FPGA Accelerated Post-Quantum Cryptography [2]

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.

## 2.2 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. Meanwhile, 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.

# Reference

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

[2] 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.