NED University of Engineering & Technology

Department of Electronics

Proposal for ME Electronics Eng. Specialization

in Integrated Circuit Design

Thesis (EL-5002)

“Hardware Design and Verification of Dilithium – Post Quantum Digital Signature Algorithm”

Student Name	Muhammad Abdul Ahad S/o Muhammad Azeem
Roll No/Batch	EL-25B5008
Program	ME Electronics Eng. Specialization in Integrated Circuit Design (Evening)
Name of Supervisor	Dr. Fahim Ul Haq (Assistant Professor Telecommunication Department NEDUET)
Duration	Spring 2026 to Fall 2026

Hardware Design and Verification of Dilithium – Post Quantum Digital Signature Algorithm

Table of Contents

Abstract

Post quantum cryptographic algorithms are required to ensure long term security in digital and embedded systems as classical public key schemes become vulnerable to emerging quantum computing attacks. CRYSTALS Dilithium is a lattice based digital signature algorithm standardized by the National Institute of Standards and Technology for its strong security guarantees and practical efficiency. However, the algorithm involves computationally intensive polynomial arithmetic and Number Theoretic Transform operations that limit the performance of software based implementations.

This thesis presents a hardware based implementation of the CRYSTALS Dilithium digital signature algorithm at the register transfer level. The proposed work focuses on designing and verifying an efficient hardware architecture that accelerates key operations including polynomial arithmetic, Number Theoretic Transform, and hashing. The design is developed in Verilog by analyzing and mapping the reference C implementation to dedicated hardware modules. Functional verification is performed through simulation to validate correctness. The results demonstrate the feasibility of hardware accelerated Dilithium for deployment in security critical and long lifetime embedded systems.

1. Introduction and Motivation

The increasing reliance on digital systems in communication, embedded devices, and critical infrastructure has made cryptographic security a fundamental requirement in modern technology. Digital signature algorithms are widely used to ensure authentication, integrity, and trust in applications including secure boot mechanisms, firmware authentication, digital certificates, and secure communication protocols. Most current systems rely on classical public key cryptographic schemes including RSA and Elliptic Curve Cryptography, which derive security from mathematical problems assumed to be computationally infeasible for classical computers.

Recent advances in quantum computing have introduced a significant threat to these cryptographic foundations. Quantum algorithms have demonstrated the ability to efficiently solve the mathematical problems underlying RSA and Elliptic Curve Cryptography, making these schemes vulnerable in a future quantum computing environment. This challenge has motivated global research efforts toward post quantum cryptography, which focuses on developing cryptographic algorithms resistant to both classical and quantum attacks.

CRYSTALS Dilithium is a lattice based digital signature algorithm standardized by the National Institute of Standards and Technology due to its strong security guarantees and practical performance. Despite these advantages, Dilithium relies on computationally intensive polynomial arithmetic and Number Theoretic Transform operations that impose performance limitations in software based implementations. This research explores the hardware implementation of Dilithium to improve performance, reduce power consumption, and enable secure deployment in long lifetime embedded systems. The work also opens opportunities for further exploration in hardware acceleration, power optimization, and side channel resistant cryptographic architectures.

2. Literature Review

Post quantum cryptography has emerged as a critical research area due to the vulnerability of classical public key cryptographic schemes to quantum computing attacks. Shor’s algorithm demonstrated that large scale quantum computers could efficiently factor integers and solve discrete logarithm problems, directly threatening widely deployed public key algorithms. This realization motivated extensive research into alternative cryptographic constructions that rely on mathematical problems believed to be resistant to both classical and quantum attacks [3].

Among the proposed post quantum cryptographic approaches, lattice based cryptography has gained significant attention due to its strong theoretical foundations and efficient implementation characteristics. Bernstein et al. provided a comprehensive overview of post quantum cryptographic techniques and identified lattice based schemes as promising candidates for long term security [3]. These constructions rely on the hardness of problems including the Learning With Errors problem, for which no efficient classical or quantum solving algorithms are currently known.

The National Institute of Standards and Technology initiated a multi year Post Quantum Cryptography standardization process to evaluate and select secure and practical cryptographic algorithms [1]. After multiple rounds of cryptanalysis and performance evaluation, CRYSTALS Dilithium was selected as a standardized post quantum digital signature algorithm. The selection was based on its strong security proofs, relatively simple design, and competitive performance among lattice based signature schemes.

The original design and security analysis of Dilithium were presented by Ducas et al., who demonstrated that the scheme achieves strong unforgeability guarantees while maintaining practical key sizes and signature lengths [2]. The algorithm relies heavily on polynomial arithmetic and Number Theoretic Transform operations to enable efficient multiplication of large polynomial vectors. While the reference implementation is optimized for software execution, the computational cost remains significant for resource constrained embedded platforms.

Several studies have investigated software implementations of Dilithium on microcontrollers and embedded processors. These works highlight challenges related to execution latency, memory footprint, and energy consumption, particularly in low power environments. The findings indicate that software only implementations are often unsuitable for time critical or energy constrained security applications.

To overcome these limitations, recent research has focused on hardware acceleration of lattice based cryptographic algorithms. Roy et al. presented a high performance FPGA implementation of CRYSTALS Dilithium, demonstrating substantial improvements in throughput and latency compared to software implementations [4]. Their work emphasized accelerating Number Theoretic Transform operations, which dominate the computational workload. Banerjee et al. explored optimized NTT architectures for lattice based cryptography and showed that pipelined and parallel designs significantly improve performance efficiency [5].

Other hardware oriented studies have examined architectural trade offs between area, power, and performance for lattice based cryptographic accelerators. These studies consistently show that dedicated hardware implementations outperform general purpose processors and enable practical deployment of post quantum digital signatures in embedded systems.

Despite these advancements, many existing works focus on platform specific optimizations or side channel protected designs, which increase design complexity. There remains a need for modular, resource efficient, and clearly structured hardware implementations that emphasize functional correctness, architectural clarity, and verification. This research addresses this gap by developing a hardware level implementation of CRYSTALS Dilithium that serves as a baseline architecture for future optimization and security enhancement.

3. Proposed Research Work

Research Problem

Software based implementations of CRYSTALS Dilithium suffer from high computational complexity, increased latency, and elevated power consumption, limiting their suitability for embedded and real time security applications.

Objectives

The objectives of this research are to design an efficient hardware architecture for Dilithium, implement key cryptographic modules including polynomial arithmetic and Number Theoretic Transform, verify functional correctness through simulation, and evaluate performance in terms of latency, area, and power consumption.

Scope

This research focuses on hardware implementation of Dilithium signing and verification modules using Verilog. The study includes architectural optimization and performance evaluation but excludes physical chip fabrication.

Limitations

The work is limited to a selected parameter set of Dilithium and does not address advanced countermeasures related to comprehensive side channel attack protection.

4. Research plan

a) Proposed Research Methodology

The research will follow a structured methodology consisting of algorithm analysis, architectural decomposition, module level RTL design, integration of cryptographic blocks, and functional verification using simulation tools. The study will begin with analysis of the reference C implementation to identify computational bottlenecks. Key modules including polynomial multiplication, Number Theoretic Transform, hashing, and control logic will be mapped to dedicated hardware blocks.

The design will be implemented using Verilog and verified through testbench driven simulation. Performance metrics including execution latency, resource utilization, and power estimation will be collected using FPGA synthesis tools. The research hypothesis is that hardware acceleration significantly improves Dilithium performance compared to software implementations on embedded processors.

b) Activity Timeline (Gantt Chart)

Project Activities	Month											
	Thesis 1						Thesis 2					
	1	2	3	4	5	6	7	8	9	10	11	12
Literature study and algorithm understanding	■	■	■	■	■	■	■	■	■	■	■	■
Requirement analysis and architecture design		■	■	■								
RTL design of polynomial arithmetic module			■	■	■							
RTL design of Number Theoretic Transform module					■	■	■					
Integration of cryptographic modules						■	■	■	■			
Testbench development and verification							■	■	■	■		
Performance evaluation and optimization								■	■	■	■	■
Documentation and thesis writing			■	■	■	■	■	■	■	■	■	■

5. References

1. National Institute of Standards and Technology, *Post Quantum Cryptography Standardization Project*, NIST, 2022.
2. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehlé, D., *CRYSTALS Dilithium: Algorithm Specifications and Supporting Documentation*, NIST PQC Round 3, 2020.
3. Bernstein, D. J., Buchmann, J., and Dahmen, E., *Post Quantum Cryptography*, Springer, Berlin, 2009.
4. Roy, S., Vercauteren, F., Verbauwhede, I., and Mentens, N., "High Performance Hardware Implementation of CRYSTALS Dilithium," *IEEE Transactions on Computers*, vol. 70, no. 9, pp. 1459–1473, 2021.
5. Banerjee, U., Pöppelmann, T., and Gaj, K., "Efficient Number Theoretic Transform Architectures for Lattice Based Cryptography," *IEEE International Symposium on Hardware Oriented Security and Trust*, 2020.

I certify that the above MS thesis proposal is prepared by me under the guidance of my supervisor and/or co-supervisor. I will carry out this research project with academic integrity, research ethics and punctuality. If my performance is found unsatisfactory in the mid-year evaluation or any time during this research project, my enrollment in MS thesis may be cancelled.

Signature of Student with date

For Office Use Only

Recommendations / Comments

1) Supervisor and/or Co-Supervisor:

I / We agree to supervise the above-mentioned student. I / We verify that the MS thesis proposal was prepared by the student with my / our consultation and the similarity index of this proposal is less than 20%.

Supervisor Signature with date **Co-Supervisor Signature with date**

2) Post Graduate Coordinator (PGC):

I certify that the above student has / has not achieved the minimum requirement /eligibility to enroll in MS thesis (MT-5002) as defined in the postgraduate regulations of NED University of Engineering & Technology.

The above student may / may not be recommended to enrolled in MS thesis.

PGC Signature with date

3) Chairperson:

This proposal is / is not recommended to be discussed in BoS.

Chairman Signature with date

4) BoS Recommendation:

This proposal is discussed in the BoS held, ____.

This proposal is recommended to be Approved / Approved with correction / Rejected.

Chairman Signature with date