POST-QUANTUM BASED KEY EXCHANGE AND AUTHENTICATION IN TLS 1.3: A PURE POST-QUANTUM CRYPTOGRAPHY APPROACH

A PROJECT REPORT

Submitted by

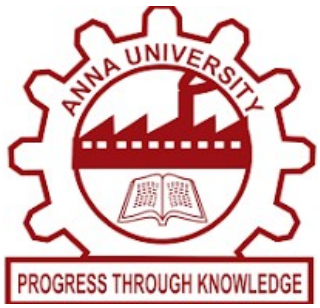
TEJESSHREE S (2022503524)

JANANI A (2022503502)

KATHIRVEL M (2022503060)

COURSE CODE: CS6611

COURSE TITLE: CREATIVE AND INNOVATIVE PROJECT



DEPARTMENT OF COMPUTER TECHNOLOGY

ANNA UNIVERSITY, MIT CAMPUS

CHENNAI – 600044

MAY 2025

DEPARTMENT OF COMPUTER TECHNOLOGY
ANNA UNIVERSITY, MIT CAMPUS
CHROMPET, CHENNAI – 600044

BONAFIDE CERTIFICATE

Certified that this project report "**Post-Quantum based Key Exchange and Authentication in TLS 1.3: A Pure Post-Quantum Cryptographic Approach**" is the work of **Ms. Tejesshree S (2022503524), Ms. Janani A (2022503502), Mr. Kathirvel M (2022503060)** in the Creative and Innovative Project Laboratory subject code CS6611 during the period January to May 2025.

SIGNATURE

Dr. GUNASEKARAN R
SUPERVISOR
Professor
Department of Computer Technology
Anna University, MIT Campus
Chromepet – 600044

SIGNATURE

Dr. JAYASHREE P
HEAD OF THE DEPARTMENT
Professor and Head
Department of Computer Technology
Anna University, MIT Campus
Chromepet – 600044

ABSTRACT

Classical cryptographic algorithms such as Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), and Elliptic Curve Diffie–Hellman (ECDH) currently secure critical network protocols like TLS and SSH. However, with the advent of quantum computing, algorithms like Shor's and Grover's threaten these classical methods by exploiting their mathematical weaknesses, creating an urgent need for cryptographic algorithms resilient to quantum attacks.

This project implements pure Post-Quantum Cryptography (PQC) within TLS 1.3, replacing classical mechanisms with quantum-resistant alternatives for key exchange and authentication, specifically integrating ML-KEM and ML-DSA, lattice-based algorithms designed to resist quantum threats.

To evaluate the practical deployment of these algorithms, a custom test environment is developed, utilizing a PQC-signed Root Certificate Authority (CA). This setup enables comprehensive benchmarking of PQC-enabled TLS performance, assessing metrics such as handshake time, certificate size, and communication delays.

In addition to performance analysis, the project investigates the security benefits, computational overhead, and compatibility challenges associated with adopting pure PQC in TLS. These insights are essential for understanding the trade-offs and feasibility of transitioning to quantum-secure communication protocols in future internet infrastructures.

ACKNOWLEDGEMENT

We take this humble opportunity to thank the Dean, MIT Campus, Anna University, Dr. Ravichandran K, and Dr. Jayashree P, Professor & Head, Department of Computer Technology, MIT Campus, Anna University for providing all the lab facilities in pursuit of this project.

Undertaking this project has helped us learn a lot, and we would like to express our gratitude towards our supervisor Dr. Gunasekaran R, Professor, Department of Computer Technology, MIT, Anna University, whose guidance, and directions helped shape this project perfectly. The feedback from the supervisor was very instrumental in the successful completion of the project.

We acknowledge the efforts and feedback of the panel members Dr. Ponsy R K Sathia Bhama, Associate Professor, Department of Computer Technology, MIT, Anna University, Dr. P. Pabitha, Associate Professor, Department of Computer Technology, MIT, Anna University, Dr. S. Muthurajkumar, Associate Professor, Department of Computer Technology, MIT, Anna University, Dr. R. Kathiroli, Assistant Professor (Sr. Gr.), Department of Computer Technology, MIT, Anna University, and Dr. T. Sudhakar, Associate Professor, Department of Computer Technology, MIT, Anna University, in reviewing our work, providing constant valuable comments and encouraging us to view the different aspects of the project in successful implementation of the project.

We thank NGN Lab, and all the teaching and non-teaching members of the Department of Computer Technology, MIT, Anna University for their support during our project. We extent our sincere gratitude to the almighty, parents, family and friends for boosting us with moral support during this project.

Tejesshree S (2022503524)

Janani A (2022503502)

Kathirvel M (2022503060)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

PQC	-	Post Quantum Cryptography
TLS	-	Transport Layer Security
ML-KEM	-	Module-Lattice Key Encapsulation Mechanism
ML-DSA	-	Module-Lattice Digital Signature Algorithm
RSA	-	Rivest-Shamir-Adleman
ECC	-	Elliptic Curve Cryptography
AES	-	Advanced Encryption Standard
ECDH	-	Elliptic-curve Diffie-Hellman
CSR	-	Certificate Signing Request
CA	-	Certificate Authority
RTT	-	Round Trip Time
OpenSSL	-	Open Secure Sockets Layer
libOQS	-	Open Quantum Safe Library
OQS-Provider	-	Open Quantum Safe Provider
NGINX	-	Engine X (High performance HTTP Server)
cURL	-	Client URL
NIST	-	National Institute of Standards and Technology
HTTP	-	Hypertext Transfer Protocol
SSH	-	Secure Shell
ECDLP	-	Elliptic Curve Discreate Logarithm Problem
KDF	-	Key Derivation Function
SVP	-	Shortest Vector Problem
CVP	-	Closest Vector Problem
LWE	-	Learning with Errors

SIS	-	Shortest Integer Solutions
FIPS	-	Federal Information Processing Standards