Performance Evaluation of Classical, Post-Quantum, and Hybrid Cryptographic Mechanisms

Student:Muhammad Bilal Zahid | Email: C00315721@setu.ie | Supervisor: Mark Cummins | April 2026

Introduction

- Quantum computing poses a significant threat to many widely used classical cryptographic systems.
- To address this challenge, researchers are developing Post-Quantum Cryptography (PQC) algorithms that are resistant to quantum attacks.
- This research investigates the performance implications of transitioning from classical cryptography to PQC.
- The study compares classical, post-quantum, and hybrid cryptographic schemes through experimental evaluation.

Methodology

- Implement cryptographic algorithms using Python, OpenSSL, and Post-Quantum Cryptography (PQC) libraries.
- Design and build experimental scenarios to evaluate different cryptographic mechanisms.
- Execute each cryptographic operation across 2000 iterations to ensure reliable performance measurements.
- Measure and record execution time for each algorithm.
- Evaluate performance across four scenarios: Key Exchange: ECDH P-256, RSA-2048, and Kyber512,Hash Functions: SHA-256, SHA3-256, and SHAKE256v, AES Encryption: Compare AES key sizes (128, 192, 256).Hybrid Cryptography: Implement ECDH-Kyber hybrid key exchange with AES encryption

Literature Review

- Early literature indicates that most PQC research focuses on hardware implementation and performance optimisation.
- Existing research highlights that quantum computing poses a serious threat to classical cryptographic algorithms such as RSA and Elliptic Curve Cryptography.
- To address this risk, the NIST Post-Quantum Cryptography project has introduced quantum-resistant algorithms, including lattice-based schemes such as Kyber.
- Studies also show that post-quantum algorithms may introduce higher computational costs and larger key sizes compared to classical methods.

Finding & Results

- Post-Quantum Cryptography (PQC) algorithms, particularly Kyber512, introduce higher computational overhead compared to classical schemes such as ECDH P-256 and RSA-2048, especially during key exchange operations.
- Hybrid cryptographic schemes (ECDH + Kyber512 with AES) demonstrate a balanced trade-off, maintaining improved security while reducing the performance impact of standalone PQC
- Hash functions show negligible performance differences.
- AES remains fast and scalable across key sizes.
- PQC exhibits greater variability and scalability challenges.

Research Questions

- How does the performance of post-quantum key exchange (Kyber512) compare to classical mechanisms such as ECDH P-256 and RSA-2048?
- How do sponge-based hash functions (SHA-3 / SHAKE) perform compared to classical SHA-256?
- What is the performance impact of different AES key sizes (128, 192, 256)?
- Does a hybrid ECDH-Kyber key exchange significantly impact encryption performance?

Conclusion

- This research investigates the performance differences between classical, post-quantum, and hybrid cryptographic mechanisms.
- The study focuses on experimental benchmarking and statistical analysis to evaluate execution time and performance variability.
- The results aim to provide insights into the practical impact of adopting post-quantum cryptography in real-world systems.