Performance Evaluation and Analysis of Post-Quantum Cryptographic Algorithms on Modern Architectures

John A. O'Dowd, C00304254@setu.ie
Supervisor: Dr. Martin Harrigan

Introduction

The consistent advances in quantum technologies are imposing one of the greatest challenges upon cryptography in recent times: the **transition to post-quantum cryptography.**

NIST's Post-Quantum Cryptography Standardization competition introduced new **quantum-resistant digital signature algorithms** including CRYSTALS-Dilithium, SPHINCS+, and FALCON that have been standardised as Federal Information Processing Standards.

Preliminary findings suggest that some of these post-quantum algorithms exhibit **high computational overheads**; such as larger key sizes, increased memory and bandwidth requirements.

This study will attempt to evaluate the **performance of these post-quantum** digital signature algorithms, providing insights into real-world feasibility.

Literature Review

The literature review has highlighted a fundamental trade-off between security strength and computational performance among various post-quantum cryptographic algorithms. This balance often dictates the suitability of a given algorithm for specific use cases. For instance, **CRYSTALS-Dilithium** demonstrates notable efficiency and lower resource consumption, making it particularly well-suited for **embedded systems and low-power devices**, where computational overhead and energy efficiency are critical.

Conversely, **Falcon** offers exceptionally fast verification speeds, which presents a significant advantage in high-frequency transaction environments, such as **payment processing systems** or **blockchain technologies**, where minimizing latency is essential.

To accurately assess the performance characteristics, the **SuperCop** benchmarking suite is utilised. SuperCop is recognised as an industry-leading tool for delivering **comprehensive**, **state-of-the-art** performance evaluations of cryptographic algorithms.

Moreover, the field of post-quantum cryptography is undergoing **rapid evolution**. New developments continuously reshape the landscape, presenting both **opportunities** and **challenges** in the quest for cryptographic solutions that balance security, performance, and practicality

Early Indicators

Early performance assessments of post-quantum cryptographic algorithms reveal a trade-off between **security**, **speed**, and **resource efficiency.**

Some algorithms demand **larger key sizes or higher computational resources**, posing challenges for integration into existing infrastructure.

Overall, early indicators suggest that while post-quantum algorithms provide robust security against quantum threats, their performance **varies significantly** based on algorithm design and intended use case.

Research Questions

1. What is the **current state-of-play** for Post-Quantum cryptographic algorithms in terms of performance on modern computer architectures using currently available optimised implementations?

2. Can we provide a **data analysis tool** that complements benchmarking tools such as SuperCop, to identify the best performing algorithms for a given system/architecture?

3. Can we **crowd-source the analyses** from RQ2 to identify trends and issues across a range of architectures?

Methodology

To ensure a comprehensive and representative dataset, data will be gathered from **multiple hardware architectures**, including x86 and ARM.

The benchmarking process will leverage **SuperCop**, a widely recognised state-of-the-art benchmarking suite specifically designed for evaluating cryptographic primitives. SuperCop ensures **consistency and reliability** in measurements, capturing key performance metrics such as execution time, memory usage, and throughput under controlled conditions.

The raw benchmarking data will be parsed and cleaned for analysis using a **custom-developed Python tool**. This tool leverages powerful libraries such as Pandas for data manipulation and structuring, and NumPy for performing numerical operations and statistical calculations.

Insights derived from the analysis will be translated into clear and informative **visual representations** using Matplotlib, a widely used Python library.

These visualizations will aid in **intuitively communicating** the findings, facilitating easier comparison and interpretation for both technical and non-technical audiences.

Sample of Data Analysis