CRYPTOGRAPHY BEYOND QUANTUM

A STUDY COMPARING THE EFFICIENCES OF POST QUANTUM AND CLASSICAL CRYPTOGRAPHIES

By Fatima Patel
Supervisor Adrian Turcanu

INTRODUCTION

As the quantum computing era dawns, classical cryptography becomes vulnerable due to quantum algorithms like Grover's and Shor's [1]. This study aims to evaluate existing cryptography against post-quantum algorithms in round 4 of NIST's evaluation or those standardized by NIST [2].

OBJECTIVES

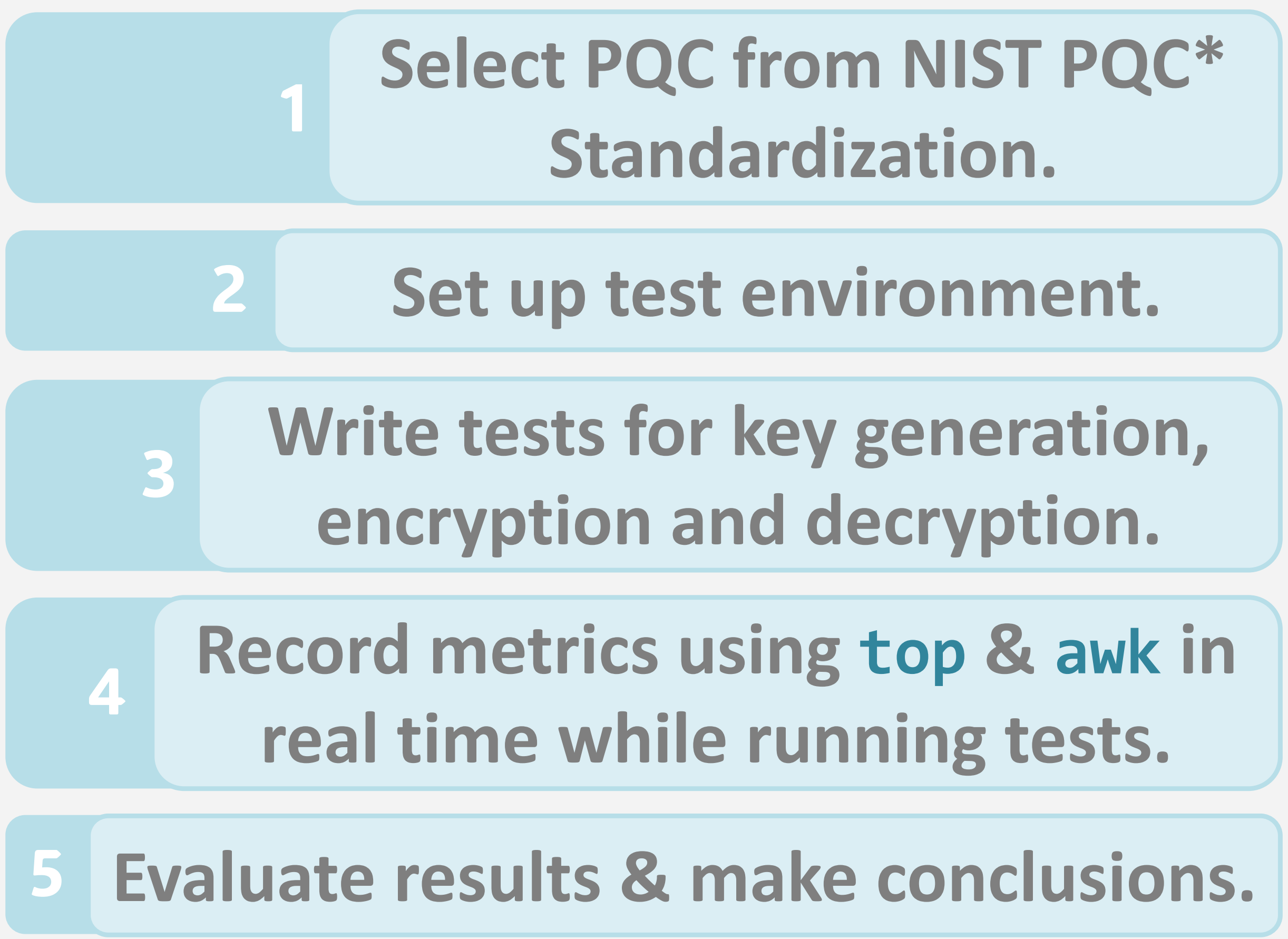
Compare the efficiencies of PQC & classical cryptographies using the following criteria:

1- Time Taken for Operations.
2- Time Complexity.
3- Memory Required.
4- Energy Consumption.
5- Hard/Software Compatibility.

METHODOLOGY

The algorithms are sourced, and tests are created then run while collecting metrics. The results are analyzed, and conclusions drawn.

Figure 1: Project Workflow



1 Select PQC from NIST PQC* Standardization.
2 Set up test environment.
3 Write tests for key generation, encryption and decryption.
4 Record metrics using top & awk in real time while running tests.
5 Evaluate results & make conclusions.

Acknowledgements I would like to thank my family, friends and Professor Adrian who encouraged and supported me whilst I worked on this research.

RESULTS

The total time taken by each algorithm to carry out the operations was calculated then graphed below:

Figure 2: Graph for Time Taken for 1000 Operations by Key Encapsulation Mechanisms

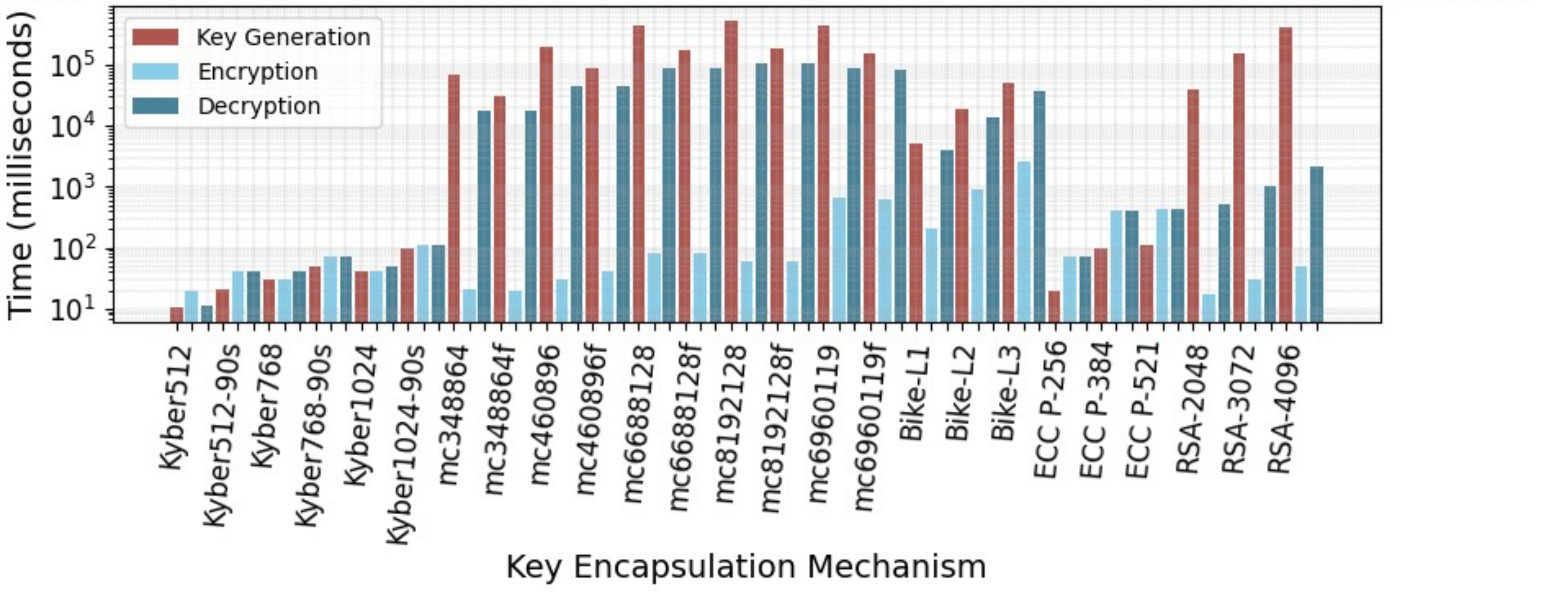
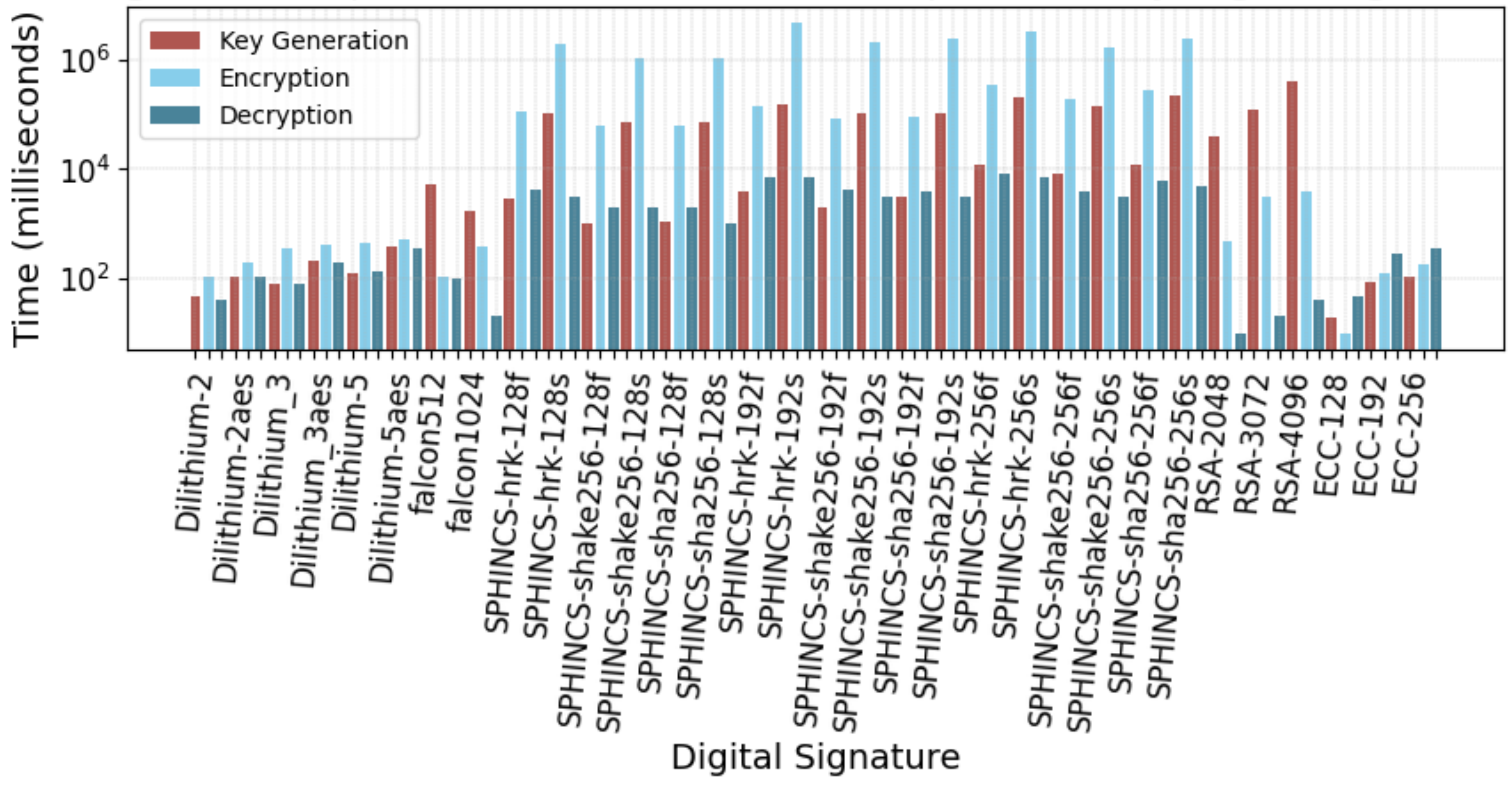


Figure 3: Graph for Time Taken for 1000 Operations by Digital Signatures



Total power used was calculated and found to be directly proportional to time taken. Lattice families were usually the fastest and therefore least power consuming. The size of the keys and cipher text was used to determine the memory required. ECC required the least memory whilst McEliece had the largest key sizes. Kyber had the least time complexity of O (log n).

CONCLUSION

Evaluating PQC and classical algorithms is complex and multifaceted. While lattice PQC like Kyber are often faster, ECC and RSA take less memory. This study evaluated multiple algorithms across many metrics and offers insights into the advancement of PQC and their direct comparison with classical algorithms.

References [1] A. S. Course, et al, Quantum Computation: A Grand Mathematical Challenge for Twenty-first Century and Millennium, January 17-18, 2000, Washington.
[2] I. T. L. Computer Security Division, "Selected Algorithms 2022 - PQC | CSRC | CSRC," CSRC | NIST, Jan. 03, 2017.

**PQC Full Form: Post Quantum Cryptography.*

HERIOT WATT UNIVERSITY