NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Computer Science and Engineering
College of Engineering

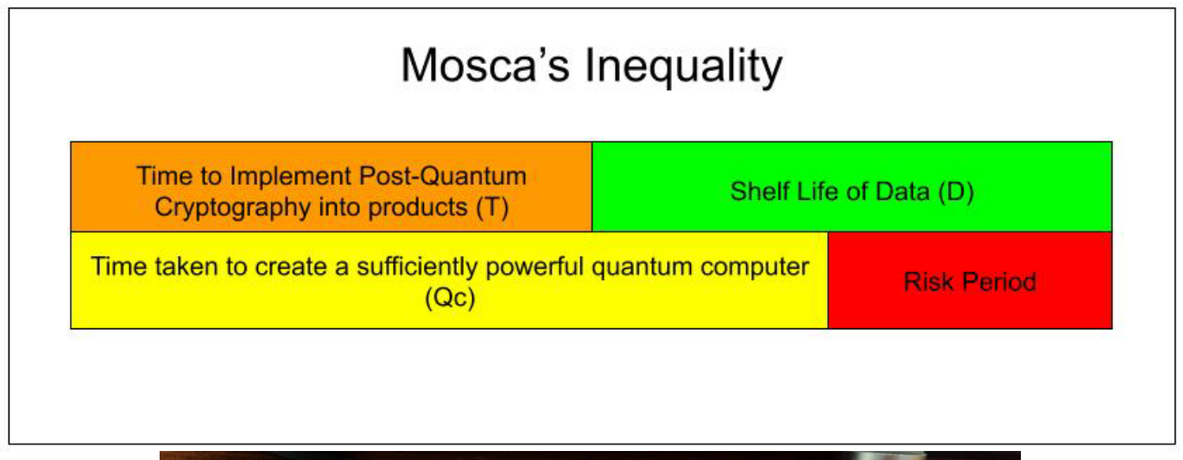
Developing Secure, Ultra-low Power RISC Processor

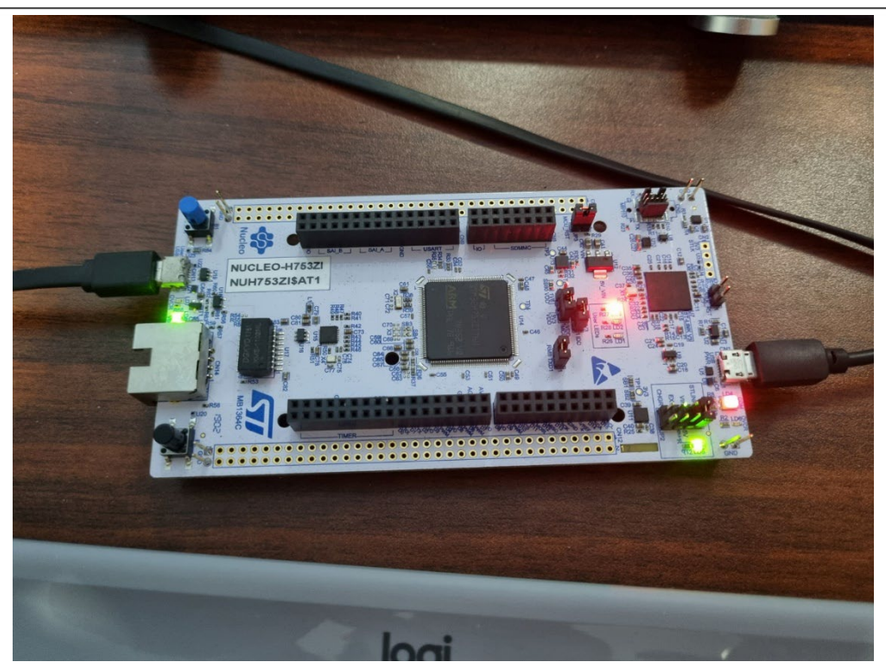
Student: Ang Kai Jun

Supervisor: Assoc. Prof. Anupam Chattopadhyay

Importance of Post Quantum Cryptography:

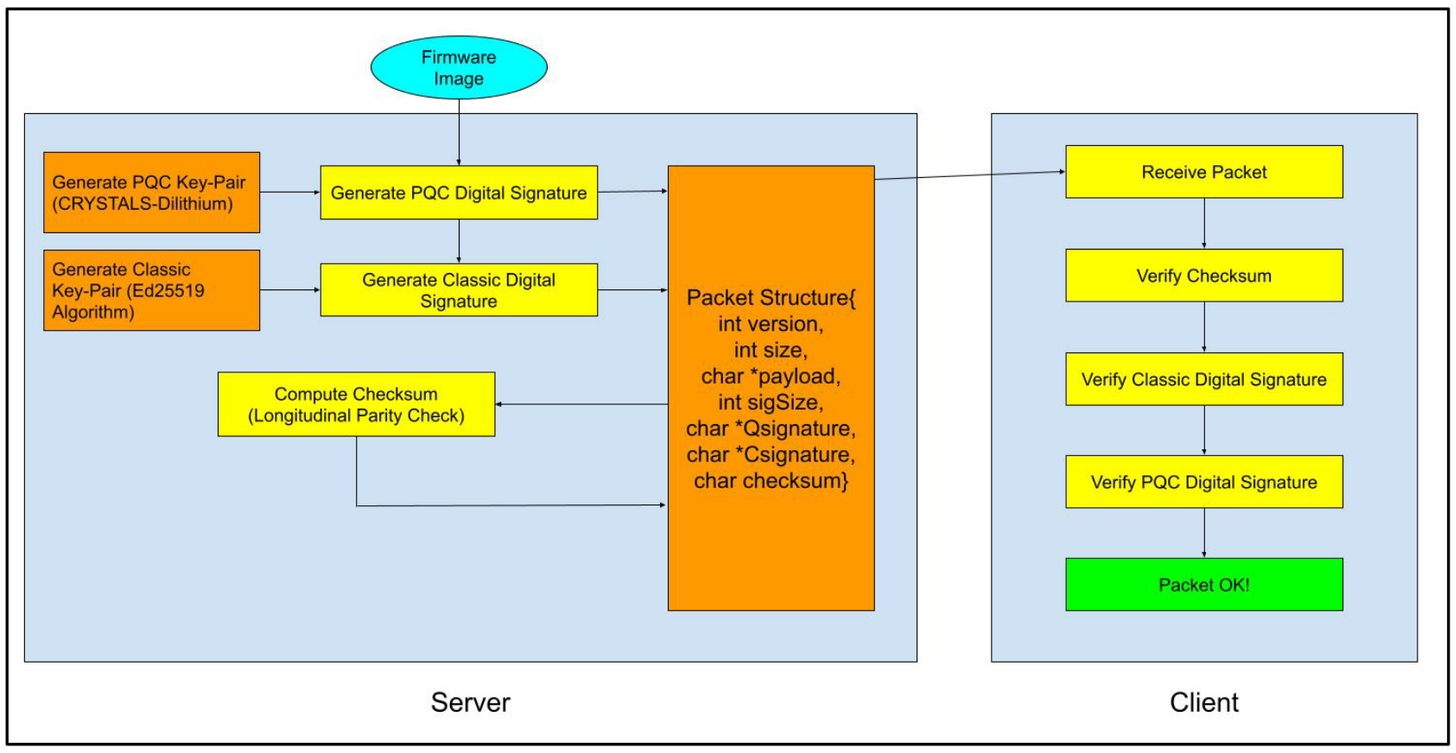
Quantum computers can perform simultaneous manipulation and enormous quantum parallelism. It has been proven that a sufficiently powerful quantum computer can break numerous public key cryptography encryption schemes, putting multiple systems at risk [1]. Mosca's Inequality [2] describes the point of time where the world must be quantum resistant.



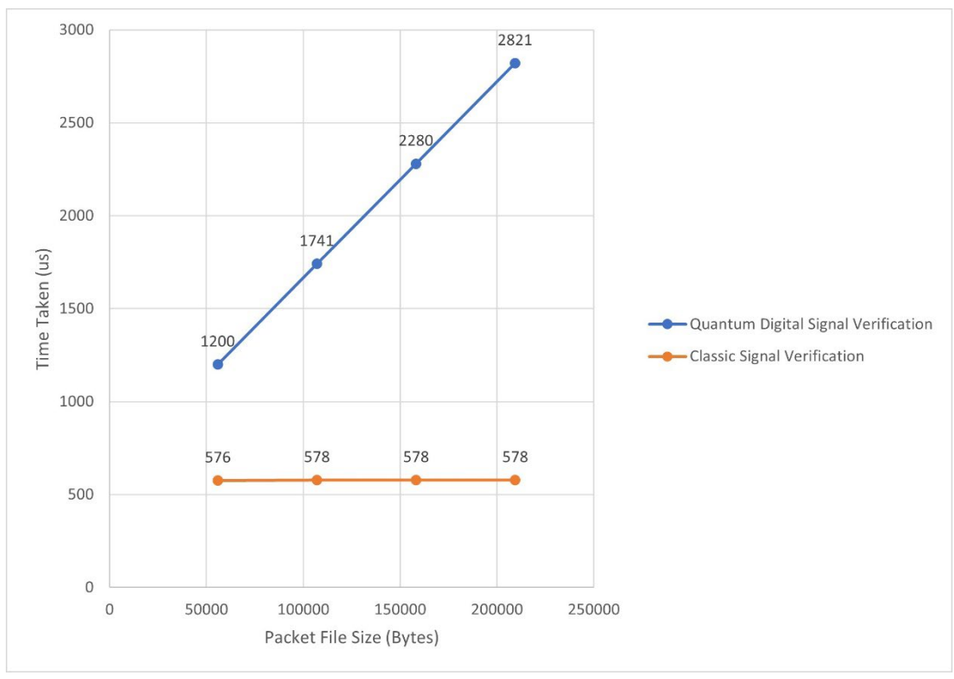


Project Objectives:

This project aims to develop a hybrid implementation of the firmware over-the-air update process, incorporating both classical and post-quantum cryptography. Firmware over-the-air updates are an important feature in Internet of Things devices as it allows developers to incorporate new functionality as well as patch existing bugs. Emergence of quantum computing threatens the security of such updates and measures must be taken to ensure security.



Relationship between Payload Size and Time Taken



References:

[1] C. H. Ugwuishiwu, U. E. Orji, C. I. Ugwu, and C. N. Asogwa, 'An overview of quantum cryptography and shor's algorithm', *Int. J. Adv. Trends Comput. Sci. Eng*, vol. 9, no. 5, 2020.

[2] M. Mosca, 'Cybersecurity in an era with quantum computers: Will we be ready?' IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018. doi: 10.1109/MSP. 2018.3761723.