Advance SOC
Final Project Proposal

Group 3

Project Title:
Implementation of the Falcon Algorithm: Applying High-Level Synthesis to Post-Quantum Cryptography

Content of Final Project Proposal

- Team: Leader + Members
- Problem statement
- Project scope
- Project plan
- Reference

Team

- Leader: 陳冠晰
- Members: 王彥智、陳柏翰

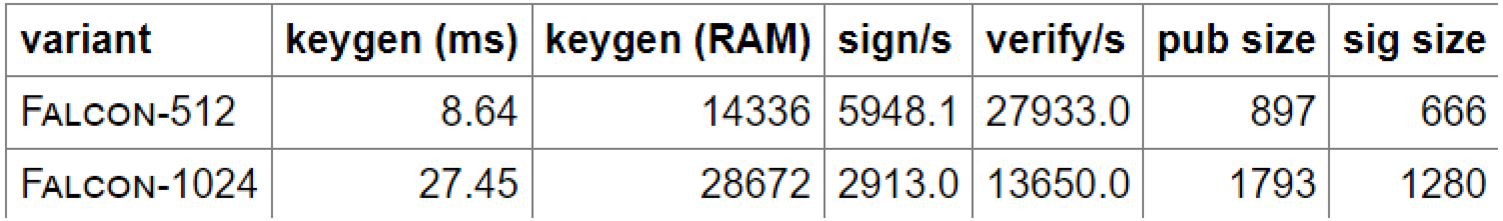
Problem Statement

- Context: PQC algorithm - Falcon

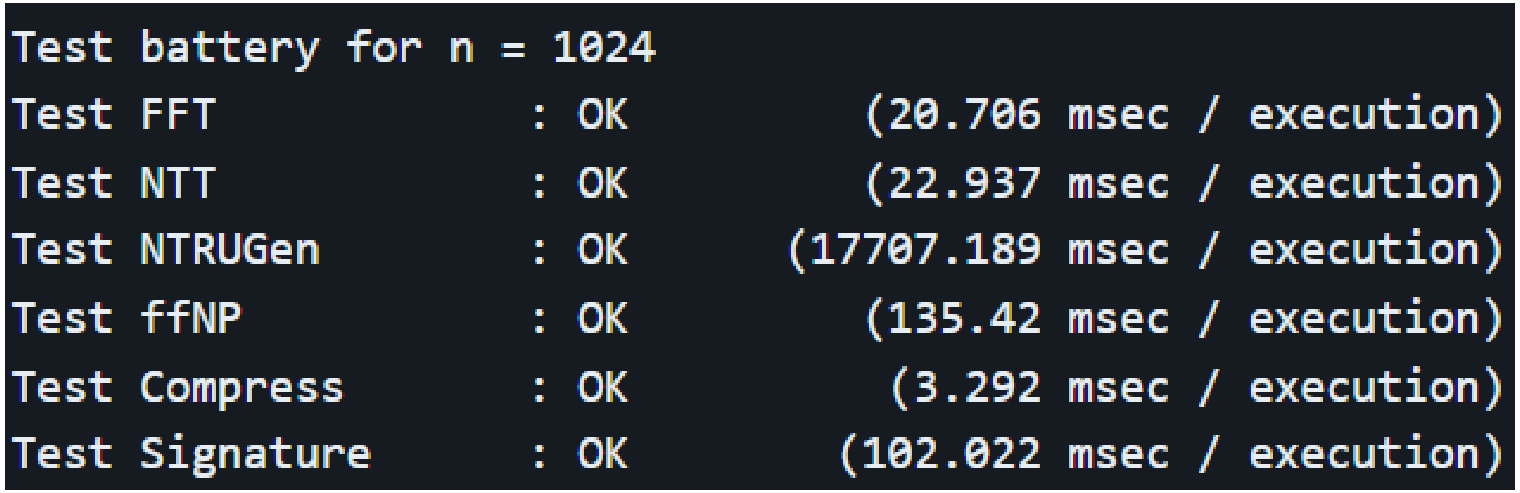
Fast-Fourier Lattice-based
Compact Signatures over NTRU

Problem Statement

- Issue: Takes long time looping with some critical functions



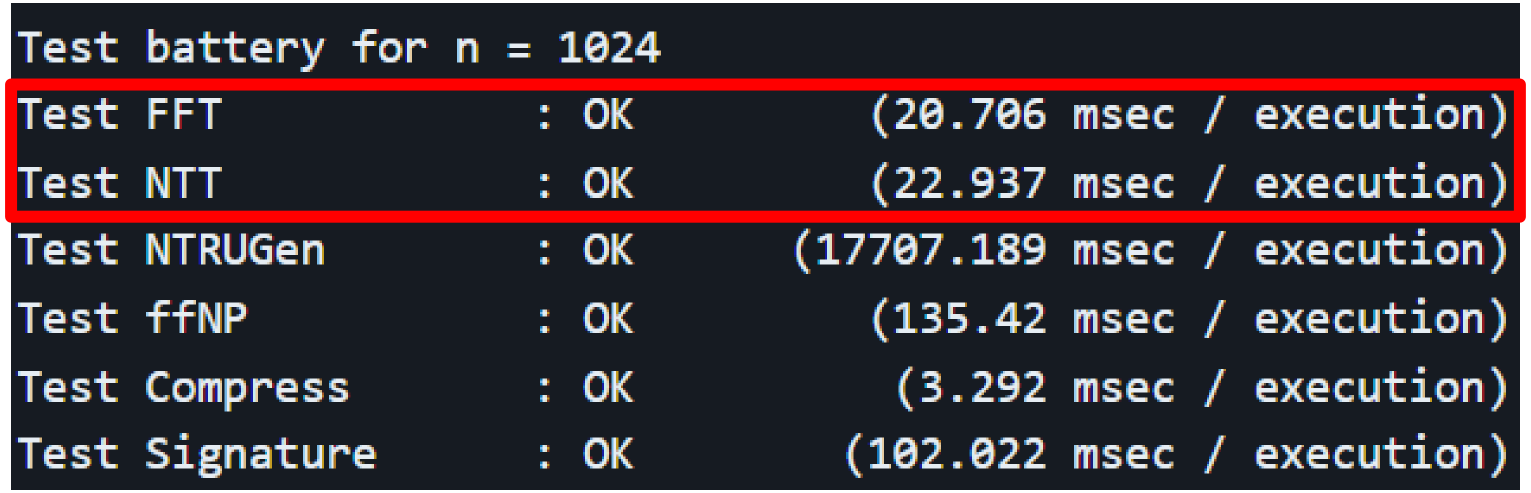
variant	keygen (ms)	keygen (RAM)	sign/s	verify/s	pub size	sig size
Falcon-512	8.64	14336	5948.1	27933.0	897	666
Falcon-1024	27.45	28672	2913.0	13650.0	1793	1280



```
Test battery for n = 1024
Test FFT                : OK          (20.706 msec / execution)
Test NTT                : OK          (22.937 msec / execution)
Test NTRUGen            : OK       (17707.189 msec / execution)
Test ffNP               : OK          (135.42 msec / execution)
Test Compress           : OK           (3.292 msec / execution)
Test Signature          : OK         (102.022 msec / execution)
```

Problem Statement

- Objective: Replace those critical functions with hardware accelerators
  - Ex: FFT / iFFT / NTT / iNTT



```
Test battery for n = 1024
Test FFT             : OK         (20.706 msec / execution)
Test NTT             : OK         (22.937 msec / execution)
Test NTRUGen         : OK      (17707.189 msec / execution)
Test ffNP            : OK         (135.42 msec / execution)
Test Compress        : OK          (3.292 msec / execution)
Test Signature       : OK        (102.022 msec / execution)
```

Which execute many times while looping in Falcon

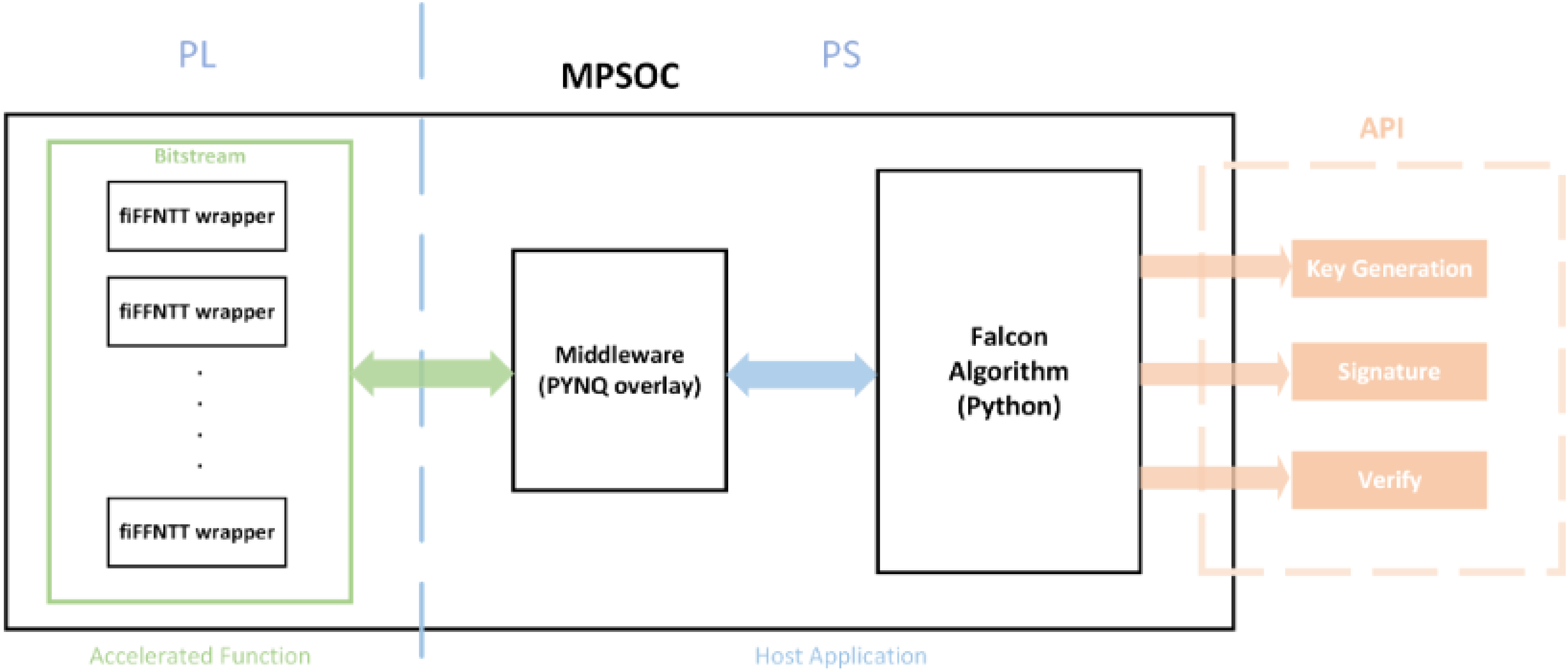
Project Scope

- Background Introduction
- System block diagram, and its operation flow
- Implement on KV260

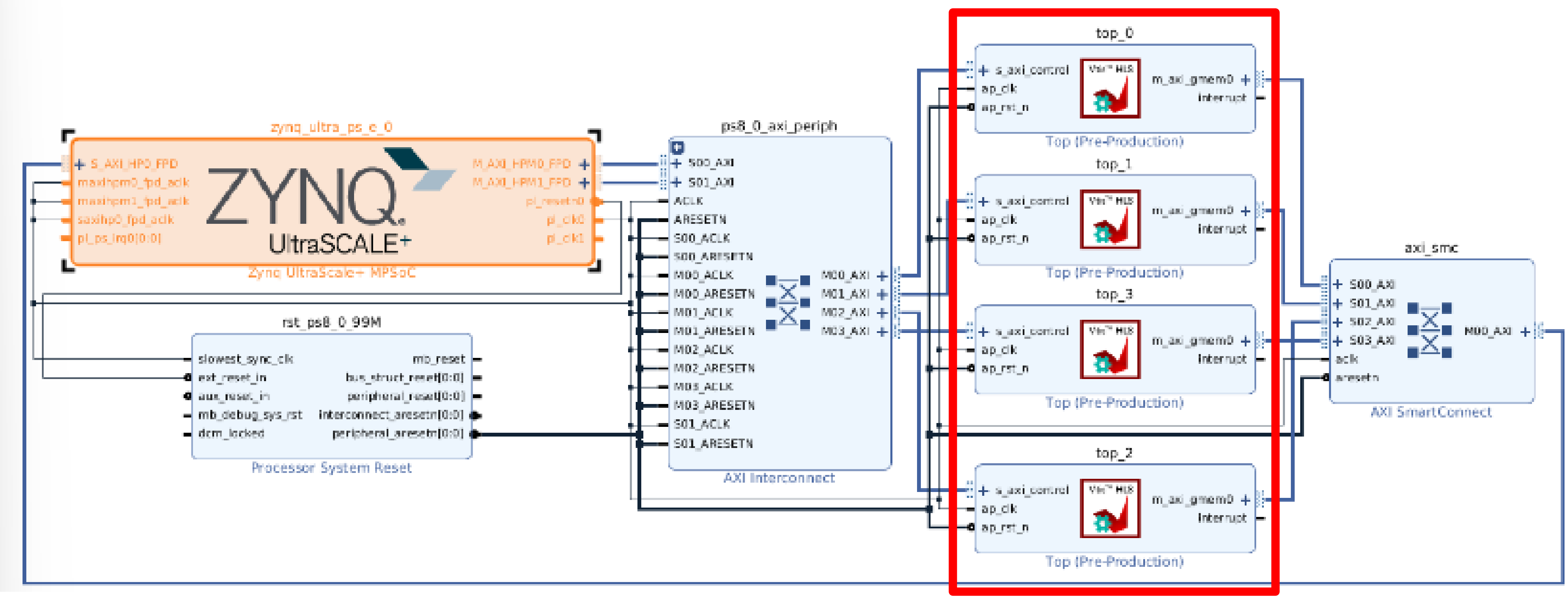
Background Introduction

- In response to the emergence of quantum computers, which pose a significant threat to existing cryptographic standards due to their potential to easily break them, post-quantum cryptography (PQC) has emerged as a critical area of research.
- Falcon stands for Fast Fourier Lattice-based Compact Signatures over NTRU. This scheme is not only a candidate in NIST’s post-quantum cryptography standardization process but also one of the frontrunners, aiming to set new benchmarks for efficiency and security in the era of quantum computing.

A Brief System Block Diagram



Implement on KV260



Our hardware accelerators

Project Plan

- Identify algorithm C-source code - Done
  - self-contained, no library function call
  - Identify test dataset
  - Partition host + kernel
- Run C-sim in Vitis environment Partition - Done
  - run through dataset -> check correctness
- Kernel HLS implementation, Host implementation – 2w
  - Develop MCU, MSI(Message Signal Interrupt), Middleware
- Individual Kernel FPGA validation/integration test – 1w
  - Integrate into Caravel FSIC
- Kernel and Host Optimization - 1w

Reference

- List of Papers for reference
- Identify open-source to use