D-9組

針對 SLH-DSA 後量子簽章之 RISC-V SHACK-256 指令集擴充設計與實現

Design and Implementation of RISC-V SHACK-256 Instruction Set Extension for SLH-DSA Post-Quantum Signature

專題成員：黃子洵、曾立呈、陳彥定、蔡丞昕
指導教授：陳培殷

Outline

一、研究動機與背景

二、後量子密碼學 (PQC) 的崛起

三、軟硬體協作架構

四、硬體層面優化：客製化SIMD加速引擎與指令集

五、軟體層面優化：記憶體最佳化

六、系統整合與硬體驗證

七、實驗結果與效能展現

八、FPGA版上Demo方式

九、結論與展望

Outline

一、研究動機與背景
二、後量子密碼學 (PQC) 的崛起
三、軟硬體協作架構
四、硬體層面優化：客製化SIMD加速引擎與指令集
五、軟體層面優化：記憶體最佳化
六、系統整合與硬體驗證
七、實驗結果與效能展現
八、FPGA版上Demo方式
九、結論與展望

研究背景：後量子密碼學 (PQC) 的崛起

- 傳統數位簽章（RSA、ECC）依賴數學難題，將面臨量子電腦 (Shor's 演算法) 的破解威脅
- NIST 頒布數位簽章新標準 FIPS-205 (SLH-DSA) 以抵抗量子攻擊

研究動機： 邊緣運算的效能瓶頸

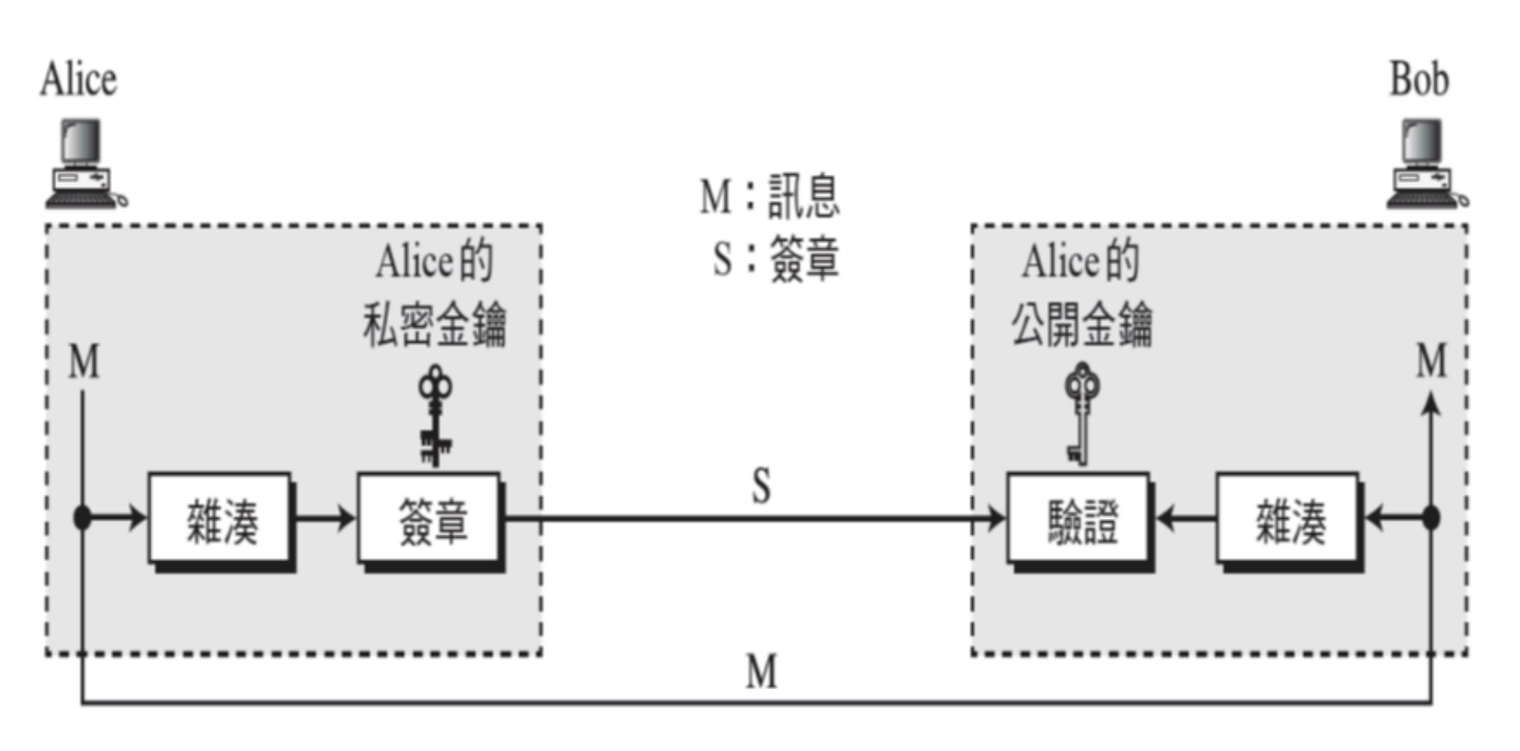
- SLH-DSA 安全性極高，但極度依賴 Hash 函數運算
- 軟體執行代價高，在一般 CPU 上執行，單次簽章最高需耗時 1000~2000 秒

專題目標：軟硬體協同設計

- 藉由客製化 RISC-V 指令集與 SIMD 架構，以較單純的架構，從底層硬體突破 SLH-DSA 的效能瓶頸

後量子密碼學 (PQC) 的崛起

使用傳送者的私密金鑰簽章, 接收端則用公開金鑰解開。



保證訊息M的完整性

後量子密碼學 Post-Quantum Cryptography (PQC)

- 量子密碼學泛指利用量子力學(電腦)的特性，來執行加密的科學與技術(於量子電腦上實現)。

- 後量子密碼技術則是一種新興的加密技術，旨在提供更高的安全性，使得**傳統電腦也能抵禦未來量子電腦的攻擊**(在一般電腦上執行之抗量子電腦攻擊的特殊演算法) 。

- 因為近幾年量子電腦技術急速發展，故後量子加密演算法相關之研究也逐漸受到關注。**後量子密碼學演算法之 VLSI 電路實現**也愈來愈重要。

NIST(美國國家標準局)PQC 標準進展時程

- 2015年4月：NIST 舉辦「後量子世界網路安全研討會」
- 2016年4月：Report on PQC
- 2016年12月：NIST 正式向全球徵求 PQC 演算法提案
- 2017年11月：提交截止，收到來自 25 個國家 82 份提案
- 2017年12月：公布第一輪預選演算法(69 個)
- 2018年4月：第一屆 PQC 標準化會議，提交者演講發表
- 2019年1月：公布第二輪預選演算法(26 個)
- 2020年7月：公布第三輪候選算法(7 個正式和 8 個替代)
- 2022年7月：NIST 確定四種優勝算法：**Kyber**、**Dilithium**、**FALCON** 和 **SPHINCS+**
- 2023年8月：NIST 發布三份標準草案 RFC
- 2024年8月13日：NIST 正式發布首批三項 PQC 標準

NISTPQC 三大標準現況(2024)

- FIPS-203 (ML-KEM) (based on Kyber)
  通用加密的主要標準

純硬體方式加速

- FIPS-204 (ML-DSA) (based on Dilithium)
  數位簽章的主要標準

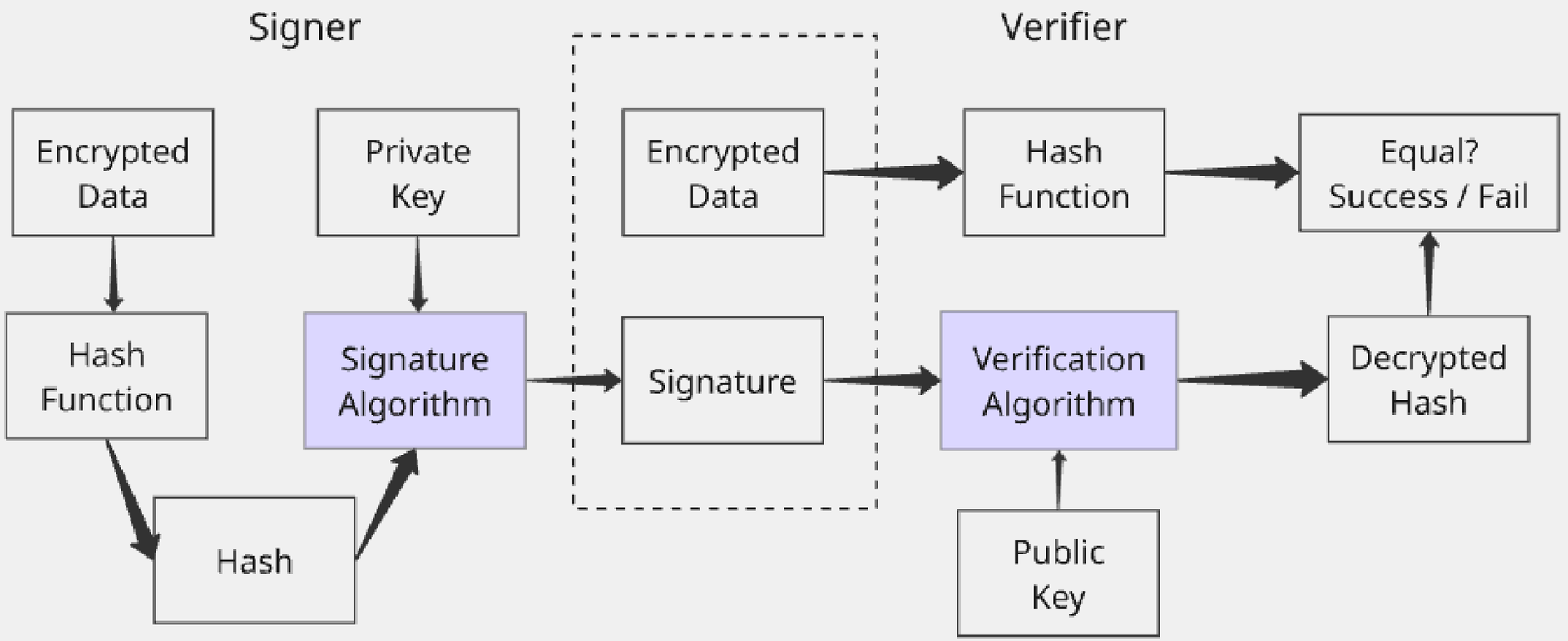
純硬體方式加速

- **FIPS-205 (SLH-DSA) (based on SPHINCS+)**
  Stateless Hash-Based的數位簽章演算法

較適合以軟硬體協同加速

軟硬體協作架構

數位簽章流程圖



*紫色方框為硬體加速部分

Outline

一、研究動機與背景
二、後量子密碼學 (PQC) 的崛起
三、軟硬體協作架構
四、硬體層面優化：客製化SIMD加速引擎與指令集
五、軟體層面優化：記憶體最佳化
六、系統整合與硬體驗證
七、實驗結果與效能展現
八、FPGA版上Demo方式
九、結論與展望

硬體層面優化：客製化SIMD加速引擎與指令集

320-bit 寬資料路徑與暫存器：

- 引入能一次容納大資料量的 SIMD Register Files 以及 SIMD ALU，解決 Keccak 演算法複雜的資料依賴問題

自定義指令集擴充：

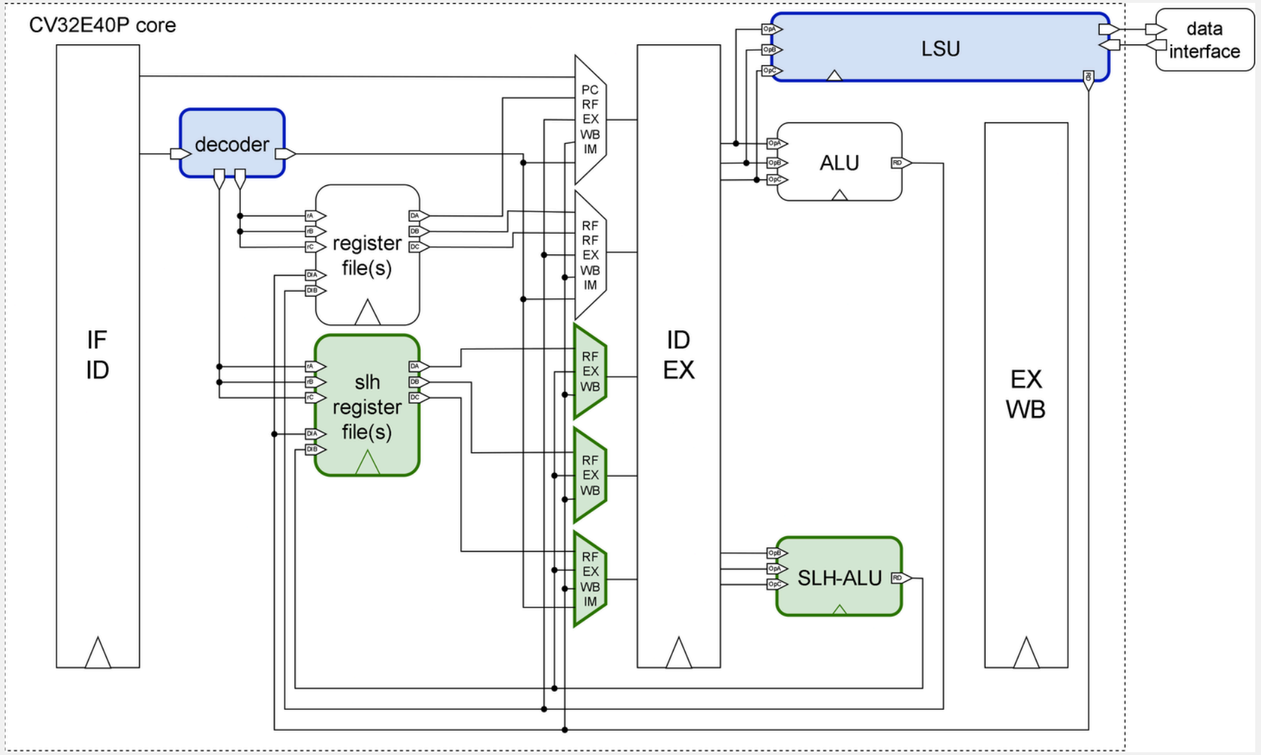
- 實作專屬的平行運算指令（如 xor3v, xorrv, rxorv, xornav, lv, sv），將冗長的軟體邏輯運算高度平行化

擴充 Load/Store 單元：

- 設計了專屬 lv 與 sv 指令，可連續執行記憶體與 SIMD 暫存器之間的區塊資料傳輸

快速轉置暫存器與零向量暫存器：

- 利用虛擬暫存器定址映射至實體暫存器的轉置，同時實現將5x5矩陣快速轉置與更精細的暫存器存取



*更動後 CPU 局部架構，綠色為新增部分，藍色為修改部分

軟體層面優化：記憶體最佳化

我們發現 NIST 官方的 C 語言實作呼叫雜湊函數時，使用大量的 memcpy 來動態拼接 pub_seed、address 與 data 。

- **消除資料搬移瓶頸**

我們在演算法高層預先配置連續的結構體，透過直接就地更新(In-place Update)位址與指標傳遞，拔除軟體層面的 memcpy 呼叫。

- **減少記憶體存取**

受益於SIMD Register Files，Keccak-f[1600]、SHAKE256皆可以將大量內部狀態存於其中，因而降低記憶體存取次數。

系統整合與硬體驗證

為了驗證硬體加速器在真實世界中的可行性，本專題運用FPGA SoC 架構，將客製化的 RISC-V 處理器實際部署於 Xilinx PYNQ FPGA 平台上，完成軟硬體介接 。

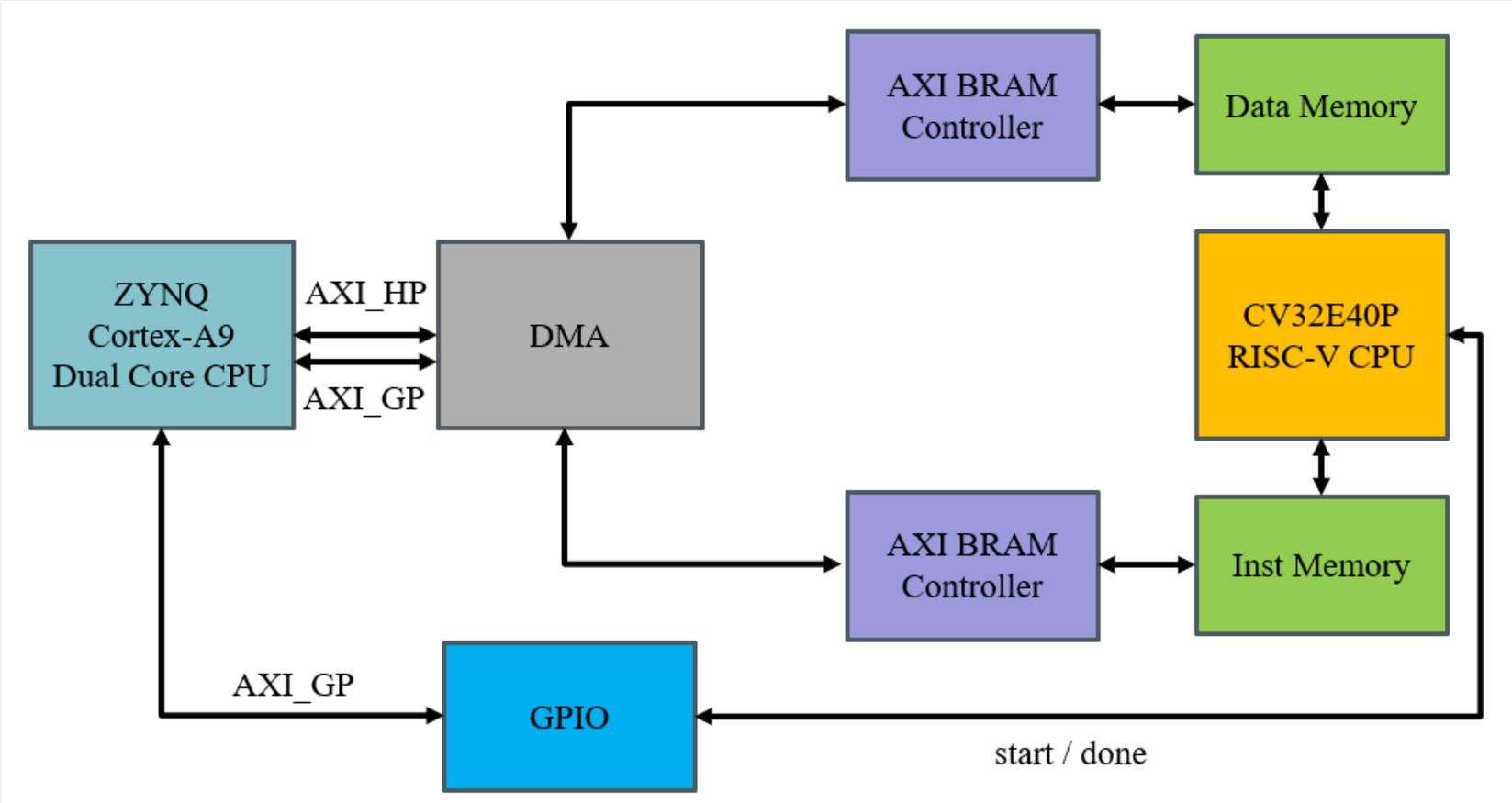
- **主從式 SoC 記憶體通訊架構**

PYNQ 開發板上 ARM 作為主控端，客製化 RISC-V 作為協同運算端。雙方透過 Dual-Port BRAM 建立共享記憶體機制。

- **裸機交叉編譯與記憶體映射**

針對無作業系統的 RISC-V 環境，我們重新撰寫了啟動組合語言(boot.S)與連結器腳本 (link.ld)，將 SLH-DSA C語言演算法交叉編譯為純二進位機器碼，並映射至 FPGA 內部的獨立指令與資料記憶體 (IMEM/DMEM)。

系統整合與硬體驗證



上圖為FPGA板上Demo系統示意圖

Outline

一、研究動機與背景
二、後量子密碼學 (PQC) 的崛起
三、軟硬體協作架構
四、硬體層面優化：客製化SIMD加速引擎與指令集
五、軟體層面優化：記憶體最佳化
六、系統整合與硬體驗證
七、實驗結果與效能展現
八、FPGA版上Demo方式
九、結論與展望

實驗結果與效能展現

本專題成功針對後量子密碼演算法 SLH-DSA (基於 SPHINCS+) 進行優化與硬體加速：

- **整體系統加速**：SLH-DSA 的三大參數集（128f、192f、256f）之總週期數與執行時間顯著降低

（表一）SLH-DSA 於原始 CPU 上的執行效能

Parameter Set	Keygen Kilo Cycle	Sign Kilo Cycle	Verify Kilo Cycle	Total Kilo Cycle	Execution Time(s)	Speedup Relative to Baseline
SLH-DSA-SHAKE-128f	103,788	2,429,352	141,574	2,674,714	56.1	x1.0
SLH-DSA-SHAKE-192f	152,101	3,932,052	211,608	4,295,762	88.2	x1.0
SLH-DSA-SHAKE-256f	402,075	8,082,375	210,582	8,695,033	176.3	x1.0

（表二）SLH-DSA 於加入 SIMD 指令之 CPU 上的執行效能

Parameter Set	Keygen Kilo Cycle	Sign Kilo Cycle	Verify Kilo Cycle	Total Kilo Cycle	Execution Time(s)	Speedup Relative to Baseline
SLH-DSA-SHAKE-128f	7,395	174,093	10,300	191,789	6.0	**x13.95**
SLH-DSA-SHAKE-192f	11,049	289,984	15,672	316,707	10.0	**x13.56**
SLH-DSA-SHAKE-256f	29,701	607,253	15,904	652,859	16.1	**x13.32**

***Compiled with riscv64-unknown-elf-gcc 15.1.0, -O3.**

實驗結果與效能展現

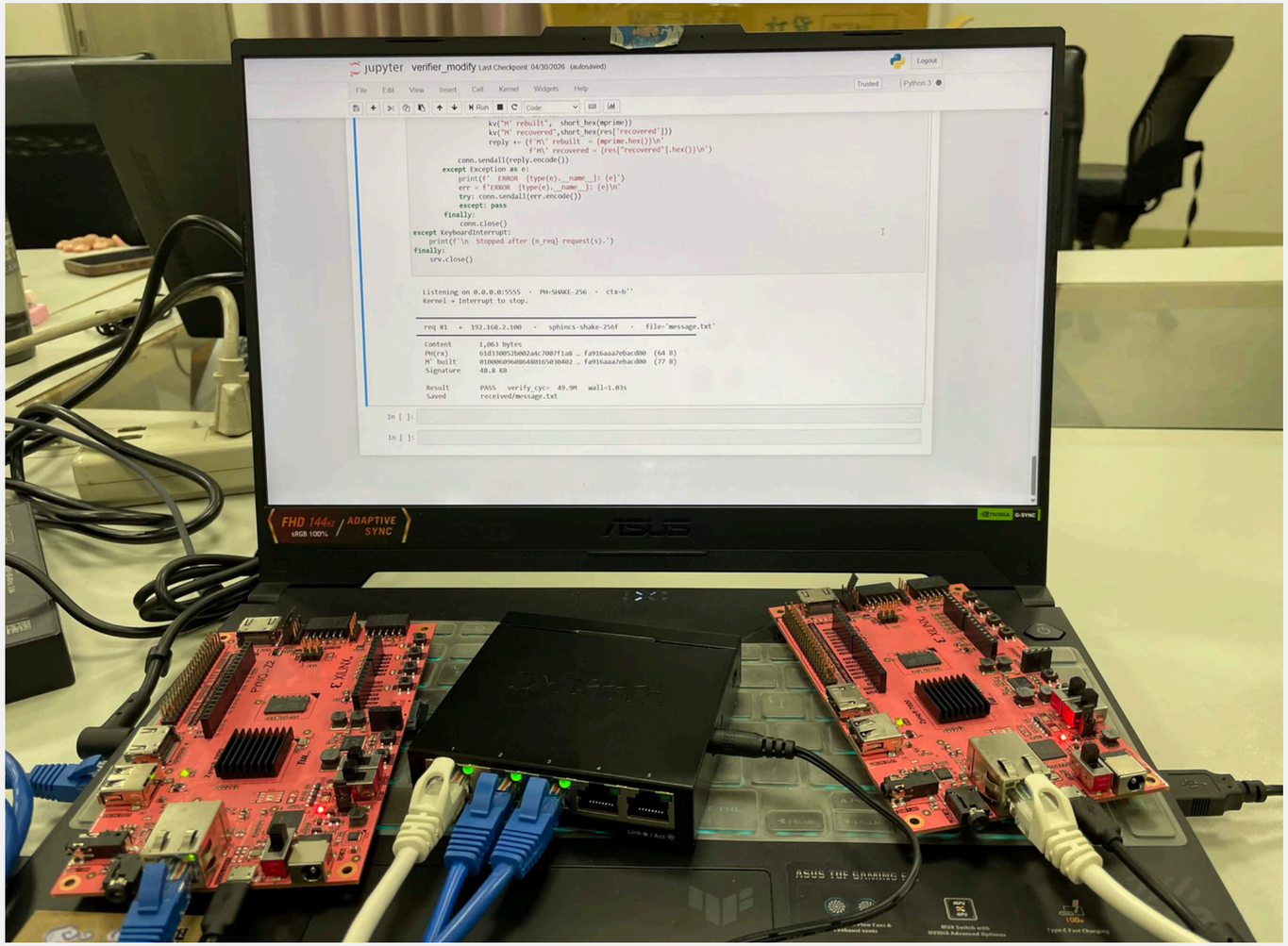
- **核心演算法優化**：針對 Keccak 與 SHAKE256 實作 SIMD 指令優化（表三）

（表三）Keccak、SHAKE256 優化後於加入 SIMD 指令之 CPU 上的執行效能

Algorithm	Baseline Cycle	Ours Cycle	Speedup
Keccak-f[1600]	42,793	1,231	**x34.76**
SHAKE256	220,357	9,200	**x23.95**

FPGA版上Demo方式

- 一個FPGA板負責簽章，在檔案簽章完成後，透過Socket傳送到另一塊板子
- 另一個FPGA板在接收到簽章後，透過解密成功驗證初始檔案



結論

本專題針對 NIST 發布之 SLH-DSA 後量子數位簽章標準，成功提出並實現了一套基於 RISC-V 架構的高效能軟硬體協同設計。最終透過以下創新突破了效能瓶頸：

1. **底層架構最佳化**：擴充 320-bit SIMD 暫存器與自定義指令集，將 SHAKE-256 核心排列運算高度硬體化。

2. **軟體記憶體重構**：利用就地更新(In-place update)拔除memcpy呼叫，打通軟硬體高速資料通道。

3. **顯著的效能躍升**：在 Xilinx PYNQ FPGA 上建構裸機編譯環境與主從式 SoC 架構，並開發 Python 自動化腳本完成硬體驗證。

測試結果證明，本系統在三大參數集中的運算週期與執行時間皆獲得大幅縮減，證實了此架構的極高實用性。

未來展望

基於此穩固的硬體加速SoC平台，未來可朝以下方向深化：

- **實作FIDO2安全金鑰**：將硬體整合 CTAP2 協定與 USB 介面，升級為支援WebAuthn無密碼登入的「後量子實體安全金鑰」。

- **擴展至完整PQC套件**：將SIMD加速架構無縫移植至ML-KEM等高度依賴Keccak函數的標準。