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

專題組員：黃子洵、曾立呈、陳彥定、蔡丞昕　　指導教授：陳培殷

研究動機與目的

1.研究動機

- 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**。因此，NIST 頒布新標準 FIPS-205 (SLH-DSA) 以抵抗量子攻擊
- 邊緣運算的效能瓶頸

  (1) SLH-DSA 安全性極高，但極度依賴 Hash 函數運算

  (2) 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

2.研究目的

針對 IoT 在執行 SLH-DSA 後量子數位簽章時面臨的效能瓶頸，重現並實作論文《RVSLH: Acceleration of Postquantum Standard SLH-DSA With Customized RISC-V Processor》中的軟硬體協同設計，於 **RISC-V 架構上進行深度優化**

實作技術與環境

1.核心處理器 IP：OpenHW CV32E40P
- 320-bit 寬資料路徑：**新增 SIMD 暫存器與 ALU**，專為 Keccak 矩陣運算設計。
- 擴充專屬指令集：**實作平行運算指令**（如 xor3v, lv, sv），將冗長的軟體邏輯高度硬體化。
- 零開銷矩陣轉置：利用暫存器定址映射瞬間完成轉置，省去 23 回合的中間記憶體存取。

2.硬體驗證平台：Xilinx PYNQ-Z2
- 以ARM為主控端、客製化RISC-V為運算端，透過Dual-Port BRAM共享簽章資料，並由Python腳本動態驅動驗證

3.開發與編譯工具
- 硬體模擬與驗證：Synopsys VCS(修改後 RISC-V RTL之功能驗證與波形分析)
- 硬體合成：Xilinx Vivado(RTL合成繞線與Bitstream生成)
- 軟體交叉編譯：riscv32-unknown-elf-gcc 裸機交叉編譯

優化成果展示

（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
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
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**

（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**

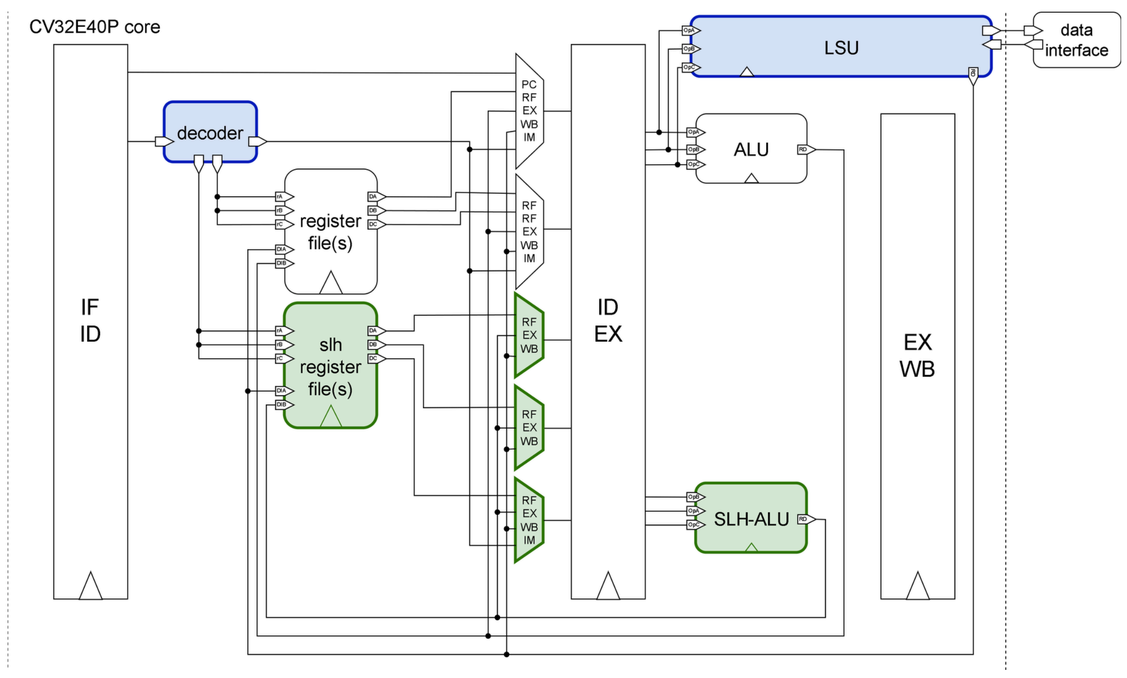
結論與未來展望

1.結論：
- 底層架構最佳化：擴充 320-bit SIMD 暫存器與自定義指令集，將 SHAKE256 **核心排列運算高度硬體化**。
- 軟體記憶體重構：利用就地更新 (In-place update) 消除 memcpy 呼叫，**打通軟硬體高速資料通道**。
- 端到端系統實體化：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。

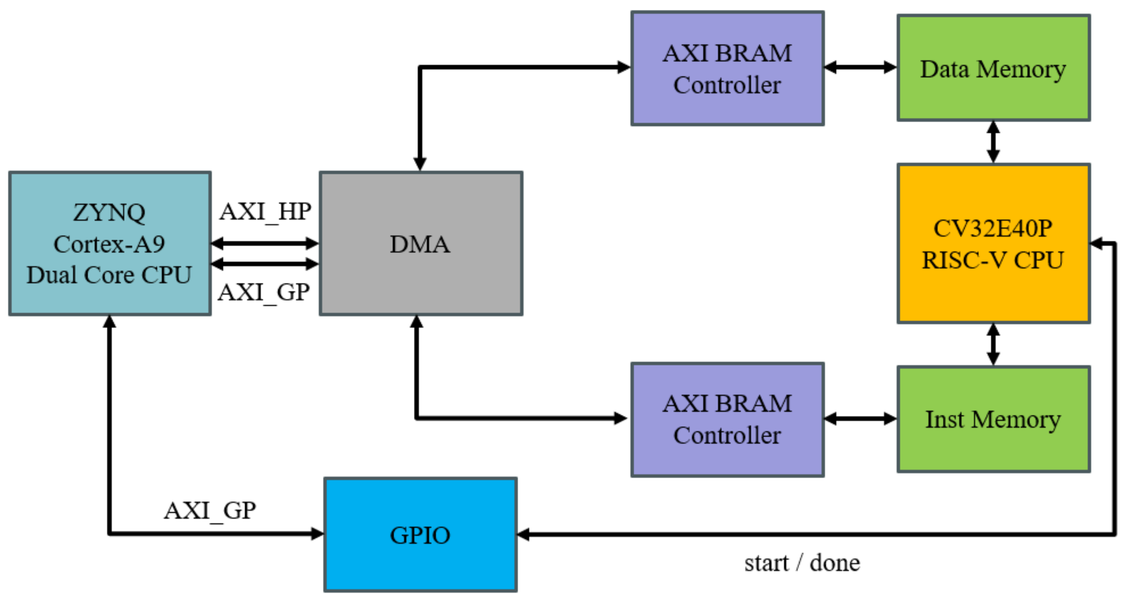
2.未來展望：

基於此穩固的硬體加速 SoC 平台，未來可朝以下方向深化
- FIDO2 安全金鑰：將硬體整合CTAP2協定與USB介面，**開發支援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加速架構延伸至 ML-KEM 等高度依賴Keccak的標準，以極致化Performance

系統架構圖



(圖一) 更動後 CPU 局部架構，綠色為新增部分，藍色為修改部分



(圖二) FPGA 板上 Demo 系統示意圖

上板Demo影片