國立臺北大學資訊工程學系114學年度專題

A Hardware-Accelerated Post-Quantum Signature System on FPGA

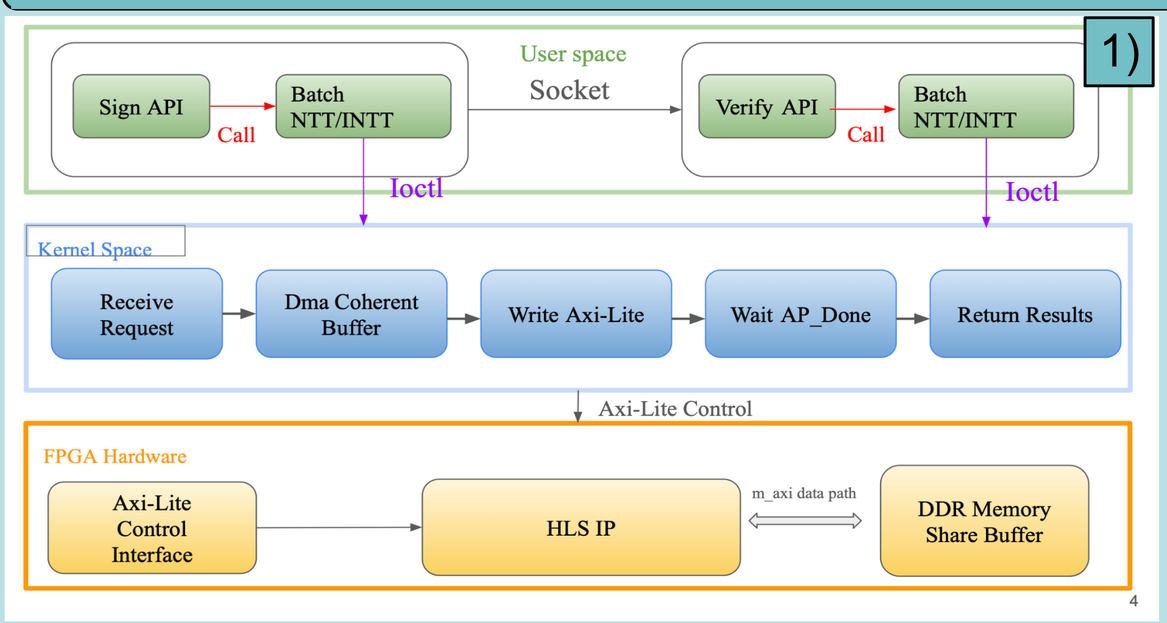
組員：曾責晏、張皓宇

摘要

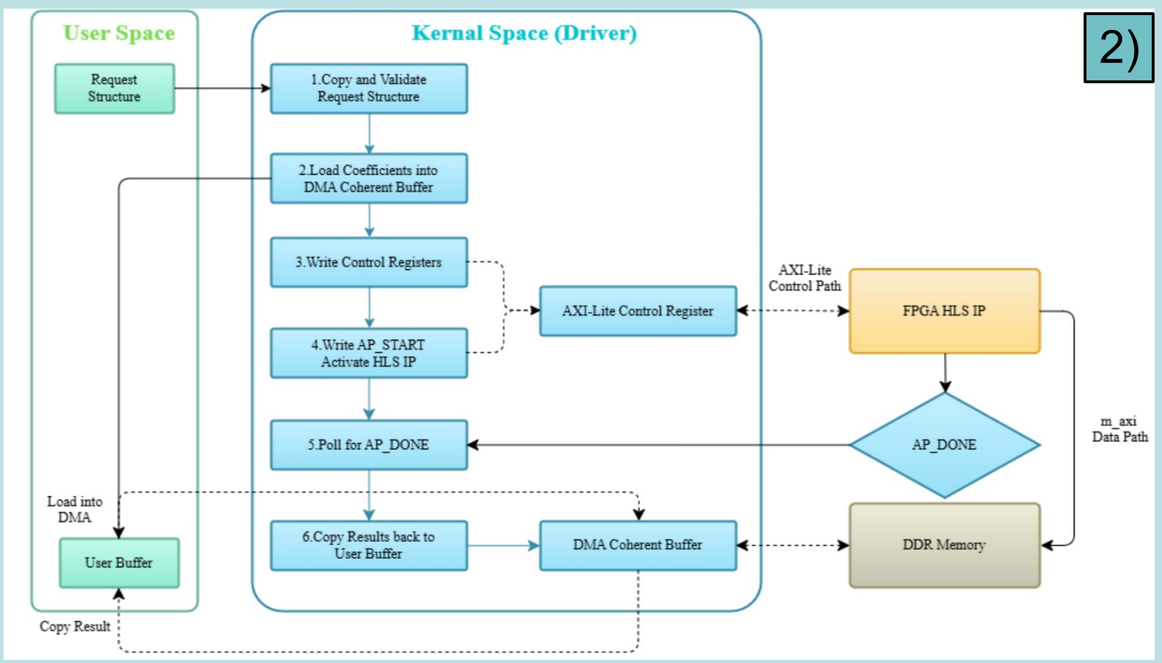
本專題旨在製作一個應用ML-DSA 的 FPGA NTT / INTT 硬體加速系統，並將加速器整合至 PQC library 中。系統透過 Linux kernel driver 與 ioctl() 介面，使 Library 內部能在不改變原本 API 的情況下呼叫 FPGA 執行核心運算。使用者仍可依照原本流程進行金鑰產生、簽章與驗章，而底層 NTT / INTT計算則由硬體加速器負責完成。本專題完成 HLS 硬體設計、FPGA 實作、Driver 控制與 PQC library 整合，展示後量子密碼演算法於軟硬體協同設計中的應用可行性。

系統架構

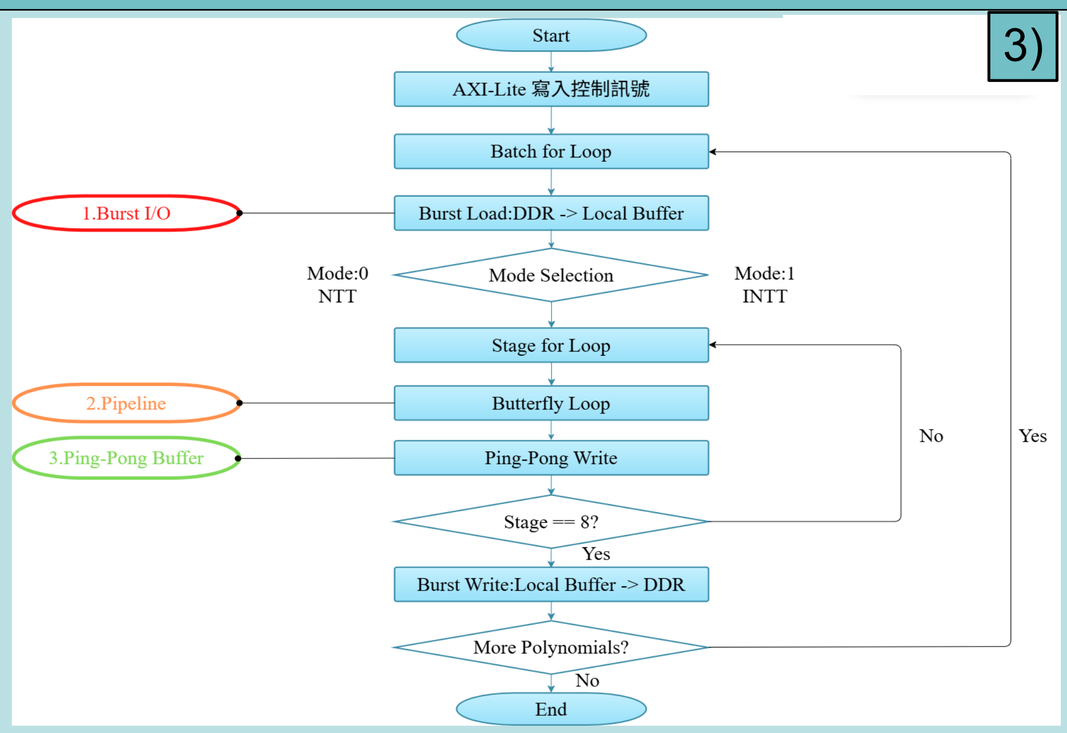
1)



2)



3)



1)系統整體架構分為三個層次：User Space、Kernel Space 與 FPGA Hardware

2)Driver 把 User Space 的 Request轉換為硬體控制訊號，透過DMA coherent buffer 作為 CPU 和 FPGA 之間共享資料的區域。

3)硬體電路

任務:硬體接收控制訊號進行NTT / INTT 運算

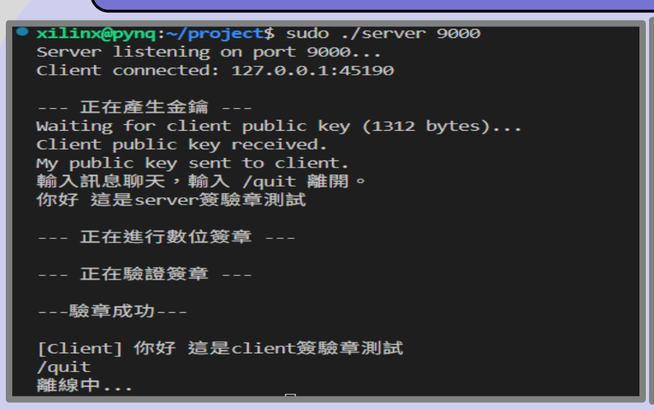
優化方式:

1.Pipeline平行處理。

2.DDR Burst減少資料搬移時間。

3.Ping-Pong buffer解決Memory Dependency。

成果展示



Server 簽驗章

Client 簽驗章

	Clock Rate	NTT Clock Cycle	INTT Clock Cycle	Time Cost
CPU	625 MHz	21666	25266	35 ± 3 us
FPGA (Without Driver)	125 MHz	1984	2046	15 ± 3 us

結語

本專題完成了從演算法分析、HLS 硬體設計、FPGA 系統整合、Linux driver 控制，到 PQC library 修改與端對端簽驗章測試的完整流程。此成果展示了 FPGA 應用於後量子密碼系統運算卸載的可行性，也提供了一個軟硬體協同設計應用於實際密碼函式庫的實作案例。

未來若能進一步降低系統Overhead、提升硬體使用率，並支援更高安全層級與更多核心運算，將能使此系統更接近實際應用需求，也可作為後續發展後量子密碼硬體加速平台的基礎。

國立臺北大學
資訊工程學系
Department of Computer Science and Information Engineering, NTPU