

Máster en Electrónica y Tecnología Digital Aplicada

Análisis, diseño y desarrollo de sistemas de verificación avanzada para implementaciones de criptografía postcuántica en FPGA

René Rodríguez Paredes rene.rodriguez102@alu.ulpgc.es

Dr. Pedro Pérez Carballo carballo@iuma.ulpgc.es

Agoney Jesús Moreno Rodríguez amoreno@arquimea.com

Agosto 2026

Resumen:

Los avances en computación cuántica presentan una amenaza para los sistemas criptográficos actuales, lo que ha impulsado el desarrollo de la criptografía postcuántica, es decir, algoritmos y primitivas resistentes tanto al modelo de computación actual como a computación cuántica. Los esfuerzos de estandarización de algoritmos postcuánticos han dado lugar a tres estándares hasta la fecha: FIPS 203, FIPS 204 y FIPS 205. No obstante, su adopción requiere de su correcta implementación, mediante una reducción del impacto de los errores que puedan surgir durante el desarrollo. Este Trabajo de Fin de Máster propone un pipeline de verificación avanzada para sistemas de criptografía postcuántica implementados en FPGA, tomando como caso de estudio un acelerador de la operación Number-Theoretic Transform (NTT), de alta relevancia para el algoritmo de encapsulado de claves postcuántico ML-KEM. El pipeline integra diferentes enfoques de verificación complementarios en un entorno que permite su ejecución durante el desarrollo o como parte de un flujo de CI/CD.

La figura A resume el flujo resultante en tres etapas: (1) análisis de la jerarquía del diseño, (2) asignación a cada área del diseño el framework de verificación más apto según sus fortalezas y (3) la ejecución de todos los frameworks de verificación para obtener los productos de verificación de forma centralizada.

B

```

RUN NTT
KYBER REG0 = 0x00000000
DMA transfers started
TX DMA done
RX DMA done
RESULT NTT 238 961 525 2698 3146 1001 849 1843 2238...
DONE

READY format: NTT|INTT c0 c1 ... c255
PASS NTT vector=999
case 2000/2000: INTT pattern=random seed=1 vector=999

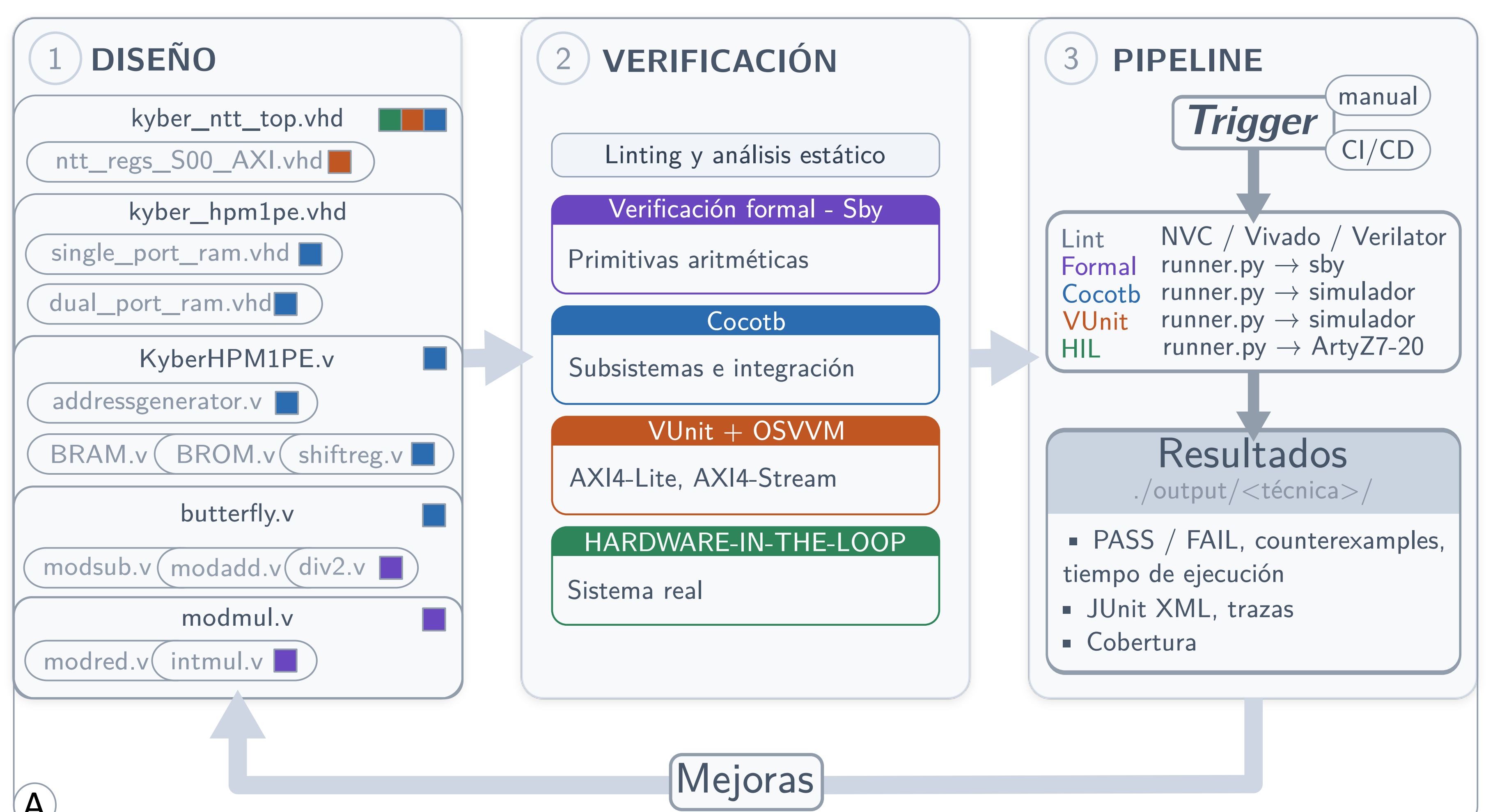
RUN INTT
KYBER REG0 = 0x00000001
DMA transfers started
TX DMA done
RX DMA done
RESULT INTT 2494 916 2616 2144 1778 2014 1842 912...
DONE

READY format: NTT|INTT c0 c1 ... c255
PASS INTT vector=999
PASS 2000/2000 cases
    
```

C

Design Units Coverage Summary (92.75%)

Instance Coverage Summary (80.71%)



La asignación por áreas aprovecha las fortalezas de cada técnica: verificación formal con Sby sobre la aritmética modular, Cocotb con modelos de referencia en Python para bloques y subsistemas, y VUnit con los componentes de verificación de OSVVM para las interfaces AXI4-Lite y AXI4-Stream. El último nivel es la verificación hardware-in-the-loop, cuya ejecución se recoge en la figura B: el proyecto implementado en una Arty Z7-20 incluye una aplicación bare-metal que permite utilizar el Processing System junto a un bloque AXI DMA para recibir los vectores por el puerto serie, transmitirlos al acelerador y retornar el resultado de la computación de las operaciones NTT/INTT, que se contrasta con el mismo modelo de referencia empleado en simulación. Las 2000 operaciones de NTT e INTT se completan de forma correcta.

Se ha diseñado e implementado con éxito un pipeline unificado de verificación avanzada para sistemas de criptografía postcuántica sobre FPGA, aplicado a un acelerador NTT del estándar ML-KEM. La combinación de los frameworks ha permitido aprovechar las fortalezas de cada uno dentro de un flujo centralizado, configurable y apto para entornos de desarrollo locales y CI/CD. Los resultados finales dan lugar a una cobertura del 92.75 % por unidad de diseño y 80.71 % por instancia (Figura C), la ejecución satisfactoria de los tests y la validación sobre la implementación del diseño en la plataforma de desarrollo Arty Z7-20. Además, la combinación de los frameworks ha revelado limitaciones no documentadas en el módulo de reducción modular, código sin uso y un incumplimiento del protocolo AXI4-Stream relacionado con la generación de TLAST, pese a tratarse de un diseño ampliamente probado y utilizado en entornos cercanos a producción. Estos resultados demuestran que la aplicación selectiva de técnicas distintas aporta garantías complementarias y constituye una base reproducible para verificar futuras implementaciones de criptografía postcuántica.