

Septiembre 2026

Resumen:

- Los avances en la computación cuántica representan una amenaza para los sistemas criptográficos clásicos en los que se basa la seguridad informática actualmente: **Criptografía post-cuántica (PQC)**.
- **Estándares NIST ML-KEM, ML-DSA y SH-DSA** lideran la **transición a sistemas más seguros basados en PQC**.
 - Reto para **sistemas empotrados con recursos limitados** debido a la **alta complejidad** de los algoritmos PQC.
 - Soluciones *hardware* con **aceleración de operaciones críticas**.
- Este TFM propone una **extensión del juego de instrucciones en una arquitectura RISC-V** para la **aceleración de estándar ML-DSA**.

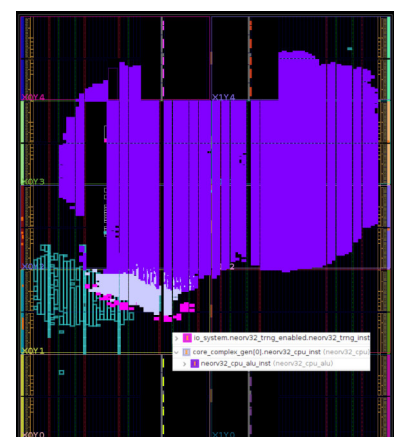
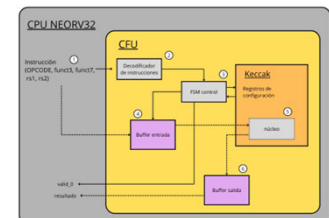
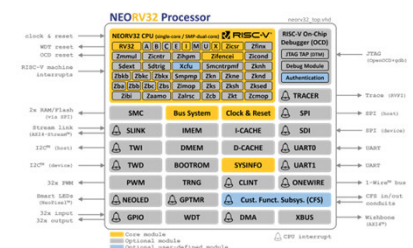
Solución basada en RISC-V + FPGA

- Elección de arquitectura RISC-V: **NEORV32**
 - **Extensión del juego de instrucciones dedicadas a PQC**
 - **Custom Funtions Unit** (CFU) + librería PQC.
 - Extensión del juego de instrucciones para ejecutar en *hardware* la función **hash SHAKE**.
 - Inclusión de un **True Random Number Generator** (TRNG) para asegurar que el algoritmo dispone de una semilla realmente aleatoria.

- Se definen **cinco nuevas instrucciones** tipo R dentro del espacio reservado que proporciona RISC-V en la ISA para extensiones personalizadas:
 - keccak_hw_init(func7, rs1, rs2)** : Operación de configuración
 - keccak_hw_data(rs1, rs2)** : Operación de envío del mensaje.
 - keccak_hw_data_last(rs1, rs2)**: Operación de envío del último bloque.
 - keccak_hw_read()** : Operación de lectura del resultado *hash*.
 - keccak_hw_reset()**: Operación de *reset*.

- **Secuencia de operación de la CFU:**
 1. La CPU **identifica una instrucción de la CFU**, activando su funcionamiento.
 2. La CPU **decodifica la instrucción** y extrae la información necesaria.
 3. La **unidad de control** desencadena la **ejecución** de la acción correspondiente.
 4. Los **datos se almacenan en un buffer de entrada** hasta que llega el último dato.
 5. El módulo Keccak **realiza la operación configurada** con los datos que ha recibido .
 6. El **resultado se almacena en un buffer de salida** hasta que es leído mediante instrucciones.

- **Implementación en FPGA Artix-7 de Xilinx (Nexys Video).**
 - El núcleo **CPU NEORV32**, que incluye el **TRNG** y el **wrapper** de depuración, utiliza **3.232 LUT**, **2.248 registros** y **34 BRAM**.
 - **CPU+CFU** para **Ceccak**, el uso de recursos aumentó hasta alcanzar las **37.089 LUT** y los **39769 registros**.
 - Este incremento se debe principalmente a las estructuras utilizadas para el **almacenamiento en buffer de datos de entrada y salida** dentro de la CFU, que se sintetizaron en lógica distribuida en lugar de en bloques de memoria dedicados.



Resultados y trabajos futuros

- Los **resultados de la extensión del juego de instrucciones** muestran que se reduce en **x60 veces** el número de ciclos necesario para la ejecución de SHAKE en el proceso de generación de claves de ML-DSA.
 - El **impacto de esta mejora** en la ejecución completa usando la Ley de Amdahl es moderada.
- Los **trabajos futuros** se centrarán en **optimizar el área lógica de la CFU**, la **mejora de los mecanismos de transferencia de datos entre la CPU y la CFU** y la **aceleración hardware** para otras funciones críticas.

ML-DSA-44	SHAKE <i>software</i>	SHAKE <i>hardware</i>	Aceleración
Ciclos ejecución	1 306 595	21 522	x60.7