MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2025-2026

PROPUESTA

Título:	*Diseño e implementación reconfigurable de la función hash para criptografía post-cuántica HARAKA*
Título en inglés:	*Design and reconfigurable implementation of the HARAKA hash function for post-quantum cryptography*
Tutor/es:	*José Luis Imaña Pascual (DACyA)*
Correos-e:	*jluimana@ucm.es*
Lugar de realización:	Facultad Ciencias Físicas, despacho 226.0

Resumen:

La criptografía de clave pública actual está basada en problemas matemáticos que pueden ser resueltos en tiempo polinómico por un computador cuántico utilizando el algoritmo de Shor. Afortunadamente, existen problemas computacionales que son difíciles de resolver incluso por un computador cuántico y que, por tanto, pueden ser utilizados para construir sistemas criptográficos post-cuánticos seguros. Entre estos criptosistemas, se encuentran los basados en hash, los basados en retículos, los criptosistemas multivariables y los basados en códigos. Para anticiparse a las amenazas de los computadores cuánticos, el NIST (National Institute of Standards and Technology) lanzó un proceso de estandarización para criptografía de clave pública resistente a ataques de computadores cuánticos (NIST PQC – *Post-Quantum Cryptography*). De los algoritmos seleccionados inicialmente para estandarización (en julio de 2022), tres son basados en retículos (CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon) y uno es basado en hash (SPHINCS+). Recientemente (en marzo de 2025), un nuevo algoritmo fue seleccionado para estandarización, esta vez basado en códigos de corrección de errores (HQC).

La criptografía post-cuántica (PQC) basada en hash depende directamente de la eficiencia y seguridad de las funciones hash. Esquemas como XMSS, LMS y SPHINCS+ (elegido como estándar post-cuántico) emplean primitivas hash robustas como SHA-3, pero también se investigan versiones de alto rendimiento como HARAKA, diseñada para entornos de hardware restringido (*lightweight*). La utilización de la función hash HARAKA puede resultar esencial para mejorar la velocidad de procesamiento de los algoritmos post-cuánticos basados en hash porque, aunque ofrecen gran solidez teórica y resistencia a ataques cuánticos, sus firmas y claves suelen ser más grandes y costosas de generar que otros esquemas PQC.

En este trabajo se estudiará la función hash HARAKA y se propondrán diferentes arquitecturas que serán descritas en un lenguaje de descripción hardware e implementadas en una FPGA de Xilinx, empleando para ello las herramientas de diseño adecuadas. La comparación de los resultados obtenidos para las distintas descripciones implementadas permitirá determinar la mejor arquitectura.

Metodología:

El trabajo constará de las siguientes tareas:

- Adquisición de los conocimientos previos necesarios sobre criptografía clásica y post-cuántica.
- Comprensión del funcionamiento de la función hash HARAKA utilizada en criptografía post-cuántica.
- Aprendizaje del lenguaje de descripción VHDL y de las herramientas de diseño adecuadas.

- Descripción e implementación hardware de distintas arquitecturas correspondientes a la función hash HARAKA.
- Comparación y análisis de los resultados obtenidos.

Conocimientos previos recomendados:

- Conocimientos de programación en lenguajes de alto nivel.

Bibliografía:

- J-P. Aumasson, D.J. Bernstein, W. Beullens, et al., SPHINCS+. Submission to the NIST post-quantum project, v.3.
- FIPS PUB 180-4. Secure Hash Standard (SHS).
- FIPS PUB 202. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.
- S. Kölbl, M.M. Lauridsen, F. Mendel, C. Rechberger. Haraka v2 – Efficient Short-Input Hashing for Post-Quantum Applications.
- Y. Dai, Y. Song, J. Tian, Z. Wang. High-Throughput Hardware Implementation for Haraka in SPHINCS+. 24th. International Symposium on Quality Electronic Design ISQED, pp. 1-6, abril 2023.