MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2025-2026

PROPUESTA

Título:	*Implementación hardware de multiplicadores polinómicos para criptografía post-cuántica basada en retículos*
Título en inglés:	*Hardware implementation of polynomial multipliers for lattice-based post-quantum cryptography*
Tutor/es:	*José Luis Imaña Pascual (DACyA), Juan José Vegas Olmos (Nvidia)*
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 códigos, los basados en retículos, criptosistemas multivariables y los basados en hash. 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).

Debido al avance en el desarrollo de los computadores cuánticos, la criptografía post-cuántica (PQC) está comenzando a usarse masivamente en comunicaciones (como TLS, VPNs y redes móviles) respaldada por una abundante documentación técnica y guías de implementación que facilitan su adopción global.

La criptografía basada en retículos es un término genérico referido a la construcción de primitivas criptográficas que emplean retículos, en la construcción o en las pruebas de seguridad. El fundamento teórico de muchos protocolos basados en retículos recae en el problema LWE (*Learning with errors*) y sus variantes, como Ring-LWE y Module-LWE. Mientras que los protocolos basados en LWE involucran operaciones modulares sobre enteros, las operaciones sobre Ring-LWE y Module-LWE requieren operaciones aritméticas en un anillo de polinomios con coeficientes enteros módulo *q*. La multiplicación de polinomios en un anillo constituye la operación computacionalmente más costosa, por lo que su optimización es fundamental para la obtención de implementaciones eficientes de estos criptosistemas.

La multiplicación de polinomios se puede realizar de forma optimizada empleando la NTT (*Number Theoretic Transform*), que es una variante de la FFT (*Fast Fourier Transform*). Sin embargo, otros métodos como Karatsuba o Toom-Cook podrían ser utilizados para dicha multiplicación. En este trabajo se estudiará alguno de los métodos de multiplicación de polinomios aplicables a la criptografía post-cuántica basada en retículos junto con algún método de reducción modular. Para los métodos elegidos, se propondrán diferentes arquitecturas que serán implementadas en un

hardware seleccionado utilizando para ello las herramientas de diseño apropiadas. 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 los algoritmos estandarizados basados en retículos.
- Estudio de los diferentes métodos de multiplicación de polinomios y de reducción modular y su utilización en los estándares PQC.
- Aprendizaje de los lenguajes de descripción y de las herramientas de diseño seleccionadas.
- Descripción e implementación hardware de distintas arquitecturas para los métodos de multiplicación y reducción elegidos.
- Comparación y análisis de los resultados obtenidos.

Conocimientos previos recomendados:

- Conocimientos de programación en lenguajes de alto nivel.

Bibliografía:

- R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler, D. Stehlé. CRYSTALS-Kyber. Algorithm Specifications and Supporting Documentation.
- S. Bai, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé. CRYSTALS-Dilithium. Algorithm Specifications and Supporting Documentation.
- P-A. Fouque, J. Hoffstein, P. Kichner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU.
- 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.