

MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2026-2027

PROPUESTA

Título:	<i>Multiplicación polinómica mediante el algoritmo de Toom–Cook para criptografía post-cuántica</i>
Título en inglés:	<i>Polynomial Multiplication Using the Toom–Cook Algorithm for Post-Quantum Cryptography</i>
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. Afortunadamente, existen problemas computacionales que son difíciles de resolver incluso por estos computadores, por lo que pueden ser utilizados para construir sistemas criptográficos post-cuánticos seguros. Entre estos criptosistemas, se encuentran los basados en códigos, los basados en retículos, criptosistemas multivariantes 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 para estandarización, tres son basados en retículos (CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon), uno es basado en hash (SPHINCS+) y otro está basado en códigos de corrección de errores (HQC).

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 obtener implementaciones eficientes de estos criptosistemas. Esta multiplicación se suele realizar de forma optimizada empleando la NTT (*Number Theoretic Transform*), aunque se pueden utilizar otros métodos. En este trabajo se estudiará el algoritmo de Toom-Cook para la multiplicación de polinomios en criptografía post-cuántica basada en retículos. 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.

Metodología:

El trabajo constará de las siguientes tareas:

- Adquisición de los conocimientos previos necesarios sobre criptografía clásica y post-cuántica, así como del funcionamiento de los algoritmos basados en retículos.
- Estudio del algoritmo de multiplicación Toom-Cook para su utilización en PQC.
- Aprendizaje de los lenguajes de descripción y de las herramientas de diseño seleccionadas.
- Descripción e implementación hardware de distintas arquitecturas.
- Comparación y análisis de los resultados obtenidos.

Conocimientos previos recomendados:

- Conocimientos de programación en lenguajes de alto nivel.

Bibliografia:

- 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.M. Bermudo, A. Karmakar, I. Verbauwhede. Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography, IACR Trans. Cryptographic HW and Embedded Systems, Vol. 2020 (2), pp. 222–244.