MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2023-2024

PROPUESTA

TÍTULO: Implementación Hardware de multiplicadores polinómicos basados en NTT para criptografía post-cuántica

TÍTULO EN INGLÉS: Hardware implementation of NTT-based polynomial multipliers for 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*) que ha sido resuelto recientemente. De los algoritmos seleccionados para estandarización, tres son basados en retículos y uno es basado en *hash*, por lo que el estudio de los criptosistemas de retículos resulta de gran interés.

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. La optimización de estas operaciones es, por lo tanto, fundamental para la obtención de implementaciones eficientes de estos criptosistemas.

En este trabajo se pretende realizar la implementación hardware de multiplicadores polinómicos basados en NTT (*number theoretic transform*). NTT es la transformada de Fourier discreta definida sobre el anillo Z_q que es utilizada en diferentes algoritmos de retículos para criptografía post-cuántica. Entre estos algoritmos se encuentran Kyber (KEM – *Key Encapsulation Mechanism*) y Dilithium (firma digital), ambos pertenecientes a CRYSTALS (*Cryptographic Suite for Algebraic Lattices*), que han resultado ganadores del proceso de estandarización para PQC lanzado por el NIST. 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.
- Estudio de CRYSTALS (Kyber/Dilithium) y de NTT.
- Aprendizaje de los lenguajes de descripción y de las herramientas de diseño seleccionadas.
- Descripción e implementación hardware de distintas arquitecturas correspondientes a multiplicadores polinómicos basados en NTT.
- 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. https://pq-crystals.org/kyber/resources.shtml.
- S. Bai, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé. CRYSTALS-Dilithium. Algorithm Specifications and Supporting Documentation. https://pq-crystals.org/dilithium/resources.shtml.
- F. Yaman, A. Can Mert, E. Öztürk, E. Savas. A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme. 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2021, pp. 1020-1025.