MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2022-2023

PROPUESTA

Título:	Implementación reconfigurable de módulos aritméticos para sistemas de cifrado post-cuánticos basados en retículos
Título en inglés	Implementation of reconfigurable arithmetic modules for lattice-based post-quantum encoding systems
Tutor/es	José Luis Imaña Pascual (DACyA)
Correos-e:	jluimana@ucm.es
Lugar de realización:	Facultad Ciencias Físicas, despacho 02.226.0

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) ha lanzado un proceso de estandarización para criptografía de clave pública resistente a ataques de computadores cuánticos (NIST PQC – Post-Quantum Cryptography) que se encuentra actualmente en sus últimas etapas. Entre los algoritmos que han pasado a la tercera ronda de dicha competición, se encuentran varios
criptosistemas basados en retículos, por lo que su estudio 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 pretenden realizar distintas implementaciones reconfigurables sobre dispositivos FPGA de operaciones aritméticas modulares involucradas en criptosistemas postcuánticos basados en retículos. Se propondrán diferentes arquitecturas que serán descritas por medio del lenguaje de descripción de hardware VHDL, utilizando para ello la herramienta de diseño electrónico ISE de Xilinx. 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 post-cuántica.
- Estudio de los sistemas criptográficos basados en retículos y de la aritmética modular involucrada.

- Aprendizaje tanto del lenguaje de descripción de hardware VHDL como de la herramienta de diseño electrónico automatizado de Xilinx.
- Descripción de distintas arquitecturas correspondientes a las operaciones aritméticas estudiadas, empleando para ello VHDL sintetizable.
- Implementación de las distintas descripciones usando la herramienta de Xilinx.
- 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 – Submission to the NIST post-quantum project. https://pq-crystals.org/kyber/data/kyber-specification-round2.pdf.
- U. Banerjee, T.S. Ukyab, A.P. Chandrakasan. Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols. DOI:10.48550/arXiv.1910.07557
- J.-P. D'Anvers, A. Karmakar, S.S. Roy, F. Vercauteren. SABER: Mod-LWR based KEM. NIST PQC documentation.