AYUDAS SEVERO OCHOA DE INTRODUCCIÓN A LA INVESTIGACIÓN, 2022

Criptografía post-cuántica.

Tutor: Ignacio Luengo Velasco

El objetivo del trabajo es introducir a los alumnos a la criptografía post-cuántica mediante el estudio de esquemas basados en una de las tres teórias abajo indicadas.

La criptografía post-cuántica es la criptografía de clave publica resistente a los futuros ordenadores cuánticos ([1], [3]). El celebre algoritmo de Shor (1994) permite factorizar enteros en tiempo polinomial lo que hace que los estándares actuales de clave publica (RSA, curvas elípticas) sean inseguros contra ordenadores cuánticos. El rápido desarrollo de los ordenadores cuánticos hace necesario disponer cuanto antes de esquemas de cifrado seguros contra ataques cuánticos porque cuando en el futuro se disponga de ordenadores cuánticos potentes toda la información cifrada en la actualidad sera vulnerable, incluyendo el trafico de internet.

El Instituto Americano de Estándares(**NIST**) lanzó en 2018 un concurso abierto para elegir y estandarizar esquemas de clave publica postcuanticos y que esta ahora en la fase final y se espera que el proceso de transición a los nuevos estándares sea largo y complejo y necesite gran cantidad de recursos científicos y humanos. Se presentaron al **NIST** 69 propuestas ([4]), las principales tecnologías matemáticas empleadas en dichas propuestas son:
- Retículos. La seguridad de estos esquemas se basa en la dificultad de encontrar el vector mas corto en un retículo (SVP).
- Polinomios multivariables. La seguridad se basa en la dificultad de resolver sistemas de ecuaciones polinomiales sobre cuerpos finitos. Nosotros presentamos al concurso un esquema multivariables (DME [2]) y seguimos con su desarrollo.
- Codigos correctores de errores. La seguridad se basa en la dificultad de corregir los errores de un código genérico.

Referencias.

[1] D. J. Bernstein, J. Buchmann,E. Dahmen (Ed.), Post-Quantum Cryptography. Springer. 2009
[2] I. Luengo, DME: a public key, signature and kem system based on double exponentiation with matrix exponents, round 1 NIST submissions, https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions,
[3] https://en.wikipedia.org/wiki/Post-quantum_cryptography
[4] https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization

Numero de alumnos : 2
Formato de la tutela: indistinto