Propuesta de Trabajo de Fin de Máster

Máster en Matemáticas Avanzadas

Director: Angelo Lucia

Alumna: Laura Castilla Castellano

Título: Computación cuántica segura

Resumen:

La idea fundamental de la computación cuántica es utilizar las propiedades de los sistemas cuánticos para realizar cálculos más allá de los límites de la computación clásica. Si bien durante mucho tiempo ha sido un área de investigación mayormente teórica, en los últimos años hemos observado progresos muy rápidos en la parte experimental, y hoy en día tenemos casos de pequeños chips cuánticos disponibles en entornos de computación en la nube.

Esto lleva a plantearnos varios problemas de seguridad. ¿Cómo podemos garantizar que estas plataformas de computación cuántica en la nube realizan de verdad los programas que hemos enviado, y no alteren su funcionamiento sin que nos podamos dar cuenta? ¿Podemos verificar el resultado devuelto por una máquina cuántica? ¿Podemos estar seguros de que realmente realicen una computación cuántica y no una simulación clásica? ¿Pueden realizar operaciones sobre nuestros datos sin conocerlos?

El objetivo del TFM es presentar algunas respuestas a estos problemas, basadas en modelos criptográficos que se suponen resistentes a ataques cuánticos [Mah18], como es por ejemplo el problema de Learning with Errors [Reg09] y la técnica de cifrado totalmente homomórfico [Gen09]. Conocimientos previos de estos resultados clásicos han sido adquiridos por la estudiante en su precedente TFG.

El proyecto se desarrollará en varias fases. En la primera parte del trabajo se buscará entender los fundamentos de la computación cuántica: cómo la sustitución de bits por qubits da también lugar a algoritmos y sistemas de cómputo, si bien dependientes de las leyes que rigen la física cuántica (superposición, entrelazamiento, medidas...) [Nie02], [Kit02]. En segundo lugar se estudiará cómo este modelo computacional da lugar a clases de complejidad distinta del caso clásico, como la clase BQP que generaliza la clase P de problemas eficientemente computables. Finalmente, se presentarán algunos de los resultados y técnicas contenidos en [Mah18] sobre autenticación de computaciones cuánticas usando el problema de Learning with Errors.

Referencias:

[Mah18] Mahadev, U. (2018, October). Classical verification of quantum computations. In 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS) (pp. 259-267). IEEE.

[Reg09] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 1-40.

[Gen09] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169-178).

[Nie02] Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.

[Kit02] Kitaev, A. Y., Shen, A., Vyalyi, M. N., & Vyalyi, M. N. (2002). Classical and quantum computation (No. 47). American Mathematical Soc..