MSIN–4213–QC+CRYPTO+PQ

Facultad de Ingeniería

Curso - Computación Cuántica y Criptografía

06/24/2022

Computación Cuántica y Criptografía

El advenimiento de la computación cuántica tiene el potencial de cambiar radicalmente el panorama infosec en Colombia y el mundo. La posibilidad "fantasmal" de aceleración exponencial de los algoritmos cuánticos podría poner en peligro la seguridad del mundo digital, hoy en día basada en criptografía clásica de arquitecturas von-Neumann. Este curso se enfoca en el análisis de la tecnología cuántica, sus posibilidades de aplicación en el mundo infosec y la forma en que las organizaciones pueden protegerse de los ataques basados en computación cuántica, utilizando los más recientes avances en criptografía post-cuántica.

MSIN–4213–QC+crypto+PQ

COMPUTACIÓNCUÁNTICA,CRIPTOGRAFÍAYCRIPTOGRAFÍAPOSTCUÁNTICA

JUSTIFICACIÓN

Mucho se habla de la revolución cuántica y el enorme impacto que tendrían los computadores cuánticos en algunos de los problemas más apremiantes que en ciencia enfrentamos como especie. Desde la posibilidad de secuenciar en tiempos breves proteínas para crear nuevos medicamentos y más generalmente problemas en química, hasta problemas de optimización y análisis de datos complejos, que sobrepasan la capacidad de cómputo de la computación tradicional.

En efecto, hay consenso en la industria que la "ley de Moore" que ha alimentado la computación clásica (o computación von-Neuman), puede estar alcanzando extremos físicos que no podamos sobrepasar y que, si deseamos seguir disfrutando de capacidad de cómputo creciente, debemos explorar pronto las *fantasmales* capacidades de procesamiento de los computadores cuánticos.

Sin embargo, desde la perspectiva infosec, esta fabulosa capacidad de cómputo prometida por la tecnología cuántica pondría en riesgo la seguridad de muchos de los servicios digitales que como sociedad disfrutamos hoy en día.

En efecto, es claro que muchos de los algoritmos de criptografía clásica para arquitecturas von-Neuman, pueden ser vulnerados mediante ataques de adversarios cuánticos a algoritmos como RSA, DH o curva elíptica.

Es difícil calcular el horizonte con el que se tendrían ataques cuánticos. Algunos analistas de industria hablan de cinco años, algunos otros de quince años. Sin embargo, de los ataques informáticos tan demoledores que recientemente hemos visto en el frente de ciberguerra de Ukrania, pareciera sugerir la posibilidad de una capacidad de cómputo muy sofisticada por parte de las fuerzas armadas Rusas.

De cualquier manera, es importante que estos temas se empiecen a estudiar en la Universidad de los Andes, de manera que la introducción de este tipo de tecnología de cómputo en Colombia y en América Latina, sea liderada efectivamente por UniAndes.

OBJETIVOS

Este curso(s) plantea varios objetivos. El primer objetivo fundamental es entender el potencial de la computación cuántica y su algorítmica asociada.

El segundo objetivo pretende desmitificar esta tecnología, para poner adecuadamente en contexto aquel tipo de problemas que ni aún con capacidades cuánticas podemos resolver.

El tercer objetivo tiene que ver con entender la reciente tecnología de criptografía post-cuántica y cómo el uso inmediato de este tipo de algoritmos en computadores tradicionales puede ayudar a proteger infraestructuras digitales críticas ante ataques de adversarios basados en computación cuántica.

CONTENIDO

Los temas a tratar en el curso son:

1. **Introducción**: panorama actual, el juego del gato y el ratón, posibilidad de ataques basados en computación cuántica en el frente de ciberguerra Ukrania-Russia. El efecto fantasmal (*spooky*) del que hablaba Einstein. La revolución. Milton Quiroga.
2. **Intuición de la computación cuántica**: Por medio de interpretaciones gráficas, se brindará la intuición de cómo opera la computación cuántica de forma muy amigable, para que cuando se entren ver detalles matemáticos estos sean comprendidos con mayor facilidad. Samuel Sabogal.
3. **Bases matemáticas de la computación clásica y cuántica**: Repaso de algebra lineal básica, Notación de Dirac, Compuertas de operaciones cuánticas, mediciones. Samuel Sabogal.
4. **Computación Cuántica:** La esfera Bloch, superposición de estados, discriminación de estados, qubit entanglement, algoritmos de Phase-fun, Phase-kickback, Oracle, Grover, Shor. Programación para computadores cuánticos. QISKit. Samuel Sabogal.
5. **Complejidad y Análisis de Algoritmos**: algoritmos de clasificación (sort) de información, la notación big O. Complejidad en algoritmos para arquitecturas von-Neuman. Complejidad en algoritmos para arquitecturas de cómputo cuánticas. Milton Quiroga.
6. **Criptografía en arquitecturas von-Neuman:** Problemas clásicos: factorización de enteros, logaritmo discreto de enteros, curvas elípticas, el problema del logaritmo discreto en curva elíptica, funciones de hash, paradoja del cumpleaños. Reflexiones acerca de la complejidad de los algoritmos criptográficos clásicos. Milton Quiroga.
7. **Criptografía post-cuántica**: Criptografía en arquitecturas von-Neuman resistente a ataques de computación cuántica: criptografía basada en funciones hash, *Lattices*, *Learning with errors*. Milton Quiroga.

BIBLIOGRAFÍA

Agrawal 2007. Rings and Integer Lattices in Computer Science. Manindra Agrawal.

Akama 2015. Elements of Quantum Computing. Seiki Akama. Springer.

Lipton 2014. Quantum Algorithms via Linear Algebra. Richard J. Lipton Kenneth W. Regan. MIT Press.

Nielsen 2010. Quantum Computation and Quantum Information. 10th Edition. Michael A. Nielsen & Isaac L. Chuang. Cambridge University Press.

RFC 9180. Hybrid Public Key Encryption. R. Barnes, K. Bhargavan, B. Lipp, C. Wood Walker

2010. Codes and Curves. Judy Walker.