Preparing for a Post-Quantum World: An Introduction to Post-Quantum Cryptography

Catie Adamo

University of Notre Dame, USA

With the rapid advancement of quantum computing, modern cryptographic systems face an existential threat. Classical public-key cryptosystems, such as RSA and ECC, rely on mathematical problems that can be efficiently solved by sufficiently powerful quantum computers using algorithms like Shor's. To address this, researchers have been developing post-quantum cryptographic (PQC) schemes that we believe will remain secure even in the presence of quantum adversaries.In this talk, we will introduce the key ideas behind post-quantum cryptography, exploring the mathematical foundations of lattice-based, code-based, multivariate, hash-based, and isogeny-based cryptosystems. We will highlight why these systems are believed to be resistant to quantum attacks and discuss their role in the NIST PQC standardization process. As quantum computing continues to evolve, understanding these cryptographic advancements is crucial for ensuring long-term security in digital communication. This talk is designed to be accessible to undergraduate and graduate students.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T13