Advanced Signatures from Lattice Isomorphism Problem

Veronika Kuchta

Florida Atlantic University, USA

Digital signatures help verify authenticity and protect data integrity. Blind and aggregate signatures extend these capabilities to privacy-preserving and space-efficient settings, respectively, making them crucial for applications such as anonymous credentials and blockchain scalability. In this talk, we present a new construction of an aggregate signature and challenges for constructing a blind from the Lattice Isomorphism Problem (LIP), a hard problem conjectured to be resistant to quantum attacks. We explore how LIP provides a structured yet difficult setting for designing secure signature schemes and discuss the challenges and open questions of our approach.

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

MCA 2025 internal code: SS55-T06