Recent Trends and Future Directions in Post-Quantum Group-based Cryptography in the AI Era

Delaram Kahrobaei

The City University of New York, USA

Post-quantum cryptography has become a central area of research in response to the growing threat posed by quantum computing to classical public-key systems. While lattice-based, code-based, and hash-based constructions have received significant attention, group-based cryptography offers a rich and flexible algebraic framework for designing alternative post-quantum primitives.

In this talk, I will survey recent developments in post-quantum group-based cryptography, highlighting emerging directions involving non-commutative algebra, discrete logarithm-type problems, hash functions, and digital signatures. I will also discuss how the rise of artificial intelligence is reshaping the field, both as a tool for cryptanalysis and as a source of new methods for construction, testing, and security evaluation. The talk will conclude with open problems and future research directions at the intersection of algebra, post-quantum cryptography, and AI.