Speaker: Veronika Kuchta

Title: Post-Quantum Zero-Knowledge Proofs

Abstract: Quantum computers could undermine cryptographic systems and digital communication. Even though current quantum machines contain just a few dozen qubits, and it is challenging to predict all future quantum applications, cryptographers must prepare for a future when quantum computers will break public-key cryptography.
In this talk I will focus on a specific topic of public-key cryptography – zero-knowledge proofs (ZKPs) and their constructions in the post-quantum setting. ZKPs represent an important cryptographic tool which is crucial for many applications such as blockchain, e-voting, private communication, etc. The more efficient and faster candidates of ZKPs are called Zero-Knowledge Succinct Non-interactive ARguments of Knowledge (ZK-SNARKs). I will explain the main challenges of lattice-based and hash-based ZK-SNARK constructions and discuss some of their applications.