SHERRY WANG, University of Ottawa
Post-quantum Technologies: Password Authentication and Digital Credentials

In a post-quantum world, where attackers may have access to full-scale quantum computers, all public key cryptosystems will be compromised. In this talk, we'll look at two possible post-quantum-secure systems. We'll look at an implementation of a password authentication scheme on a quantum computer. Briefly, we'll also talk about post-quantum digital credentials, which are a privacy technology that allows users to disclose information about an attribute without revealing the attribute itself during transactions.