Department of Mathematics and Statistics Colloquium

Tuesday January 22

AMB 164 4:00 pm

Hash-based cryptography as a solution against quantum computer attacks

Bertrand Cambou

School of Informatics, Computing, and Cyber-Systems
Northern Arizona University

Abstract

Mainstream cryptography schemes, such as the one based on modulo exponentiation (ex: RSA), and elliptic curves (ECC) are vulnerable to quantum computers. Mathematical algorithms such as the one developed by Shor, which can quickly find prime factors, has the potential to break RSA, and ECC. Hash based cryptography (HBC), an invention of the 80's, is currently one of the three candidate technology that is quantum computing resistant technology. Hash functions are complex one-way cryptographic functions that are already used for applications such as blockchains, and cryptocurrencies. The research effort needed to use these functions for mainstream cryptography will be presented and discussed in the talk. Variations of the Winternitz algorithm are the most promising schemes, while the key distribution remain a major challenge.

Refreshments at 3:45