PIMS
Pacific Institute for the Mathematical Sciences

ANDREW FIORI

Mathematics & Computer Science

University of Lethbridge

Title: Lattice Based Cryptography

This talk is open to all, and very little background is required.

Abstract:
Cryptography has become the foundation on which our modern digital world is built. The most widely used public key crypto-systems are largely built around the difficulty of certain mathematical problems. Ongoing advancements in quantum computing seem precipitously close to reducing that difficulty and putting a crack in this foundation.

There are several recently proposed crypto-systems which are expected to be secure against "quantum attacks", one of these is largely referred to as lattice based cryptography.

In this talk we will explain, by working through an explicit example, how lattice based cryptography works. We will explain:
- How to encrypt using primarily linear algebra, eg: (8,2,4) + (6,9,5) = (14,11,9), and long division to reduce modulo 11, eg: (14,11,9) % 11 = (3,0,9).
- How to decrypt using primarily dot products: eg: (3,0,9) * (4,1,4) = 3*4 + 0*1 + 9*4 = 48, and more long division, eg: 48 % 11 = 4.

Friday—March 22, 2019
12:00—12:50 pm
UHall B650
SNACKS!