HONOURS SEMINAR

Sam Jaques

Lattice Cryptography

Supervised by Doug Farenick

Thursday Nov. 10
3:00 pm
Math Lounge, CW 307.14

Abstract: Many NP-complete problems arise from geometric objects called lattices. There are several public key cryptosystems based on these hard lattice problems, but until recently these systems were too inefficient to be practical. However, if the lattices arise from polynomial rings, there are tricks that drastically reduce the time and space requirements. In this talk I will give an overview of several problems in lattices and explain how these relate to the "Ring-Learning With Errors" problem that underlies current lattice cryptography. I will show a few of the properties of polynomial rings that enable fast computation, then outline the basic mechanism of the public key exchange.

University of Regina

Mathematics and Statistics