MONICA NEVINS, University of Ottawa, Ottawa, ON, K1N 6N5
NTRU over the Eisenstein Integers

NTRU is a cryptosystem proposed by Hoffstein, Pipher and Silverman in 1996. It is based on polynomials with integer coefficients, where secrecy is obtained by performing operations modulo two different primes in $\mathbb{Z}$. We propose a variant of NTRU, in which $\mathbb{Z}$ is replaced by the Eisenstein integers $\mathbb{Z}[\omega]$. In this talk, we describe this variant, and show how the key property which makes NTRU over $\mathbb{Z}[\omega]$ so efficient and secure is its hexagonal lattice structure in $\mathbb{C}$.

This is joint work with Ali Miri (Ryerson), Camelia Karimianpour (Ottawa) and most recently, Katherine Jarvis (Ottawa).