1106-06-1173 **Jean-Francois Biasse*** (jbiasse@uwaterloo.ca), University of Waterloo, 200 University Ave. West, Waterloo, Ontario N2L 3G1, Canada. *Ideal lattice problems and applications to cryptography.*

Ideals in the ring of integers of a number field have a lattice structure, and they are considered for the design of many lattice-based cryptosystems. These rely on the hardness of finding a short vector in a lattice of large dimension presented by an arbitrary basis. The main appeal of these schemes is their potential for quantum resistance and homomorphic encryption, which are two major challenges inpublic-key cryptography.

Using lattices that are embedded in a number field of large degree is interesting for efficiency reasons, but it seems that the surrounding algebraic structure may also be used to design attacks. In particular, in many cases the ideals are principal, and the knowledge of a short generator is enough to break the cryptosystem (finding some arbitrary generator is called the principal ideal problem).

In this talk, we present recent developments in the resolution of the principal ideal problem relying on new subexponential methods for computing the class group and the unit group of a large degree number field, which have fundamental applications in number theory. We will also present work in progress on an algorithm for finding a short generator of a principal ideal which directly applies to the cryptanalysis of ideal lattice-based cryptosystems. (Received September 11, 2014)