1106-VQ-1176 **Jean-Francois Biasse*** (jbiasse@uwaterloo.ca), University of Waterloo, 200 University Ave. West, Waterloo, Ontario N2L 3G1, Canada. *Class group and unit group computation in large degree number fields and applications.*

We present a subexponential time method for computing the class group and the unit group of a large degree number field, and we discuss some of its direct applications to the resolution of norm equations and to the analysis of the security of certain cryptosystems.

Computing the class group and the unit group of a number field is a fundamental problem in number theory. There are several unproven conjectures on the structure of the class group such as the Cohen-Lenstra heuristics, while the unit group allows to solve some Diophantine equations, including the Pell equation and more general norm equations. Moreover, our method extends to the computation of a generator of a principal ideal, which applies to lattice-based cryptography. Lattice-based cryptosystems currently receive a lot of attention because they are among the very few proposals for homomorphic and quantum-safe encryption schemes.

Prior to our contribution, computing the unit group and the class group in subexponential time was only possible for classes of number fields of fixed degree. We also represent units by a polynomially bounded amount of information. This task, known as the compact representation, was only possible efficiently for classes of fixed degree number fields. (Received September 11, 2014)