Recovering Short Generators of Principal Ideals in Cyclotomic Rings

Léo Ducas, Center for Mathematics and Computer Science (CWI)

A handful of recent cryptographic proposals rely on the conjectured hardness of the following problem in cyclotomic rings: given a basis of an ideal that is guaranteed to have a "rather short" generator, find such a generator. In the past year, Bernstein and Campbell-Groves-Shepherd have sketched potential attacks against this problem. Most notably, the latter authors claimed a quantum polynomial-time algorithm (alternatively, replacing the quantum component with an algorithm of Biasse and Fieker would yield
a classical subexponential-time algorithm). A key claim of Campbell et al. is that one step of their algorithm—namely, decoding the log-unit lattice of the ring to recover a short generator from an arbitrary one—is efficient (whereas the standard approach takes exponential time). However, very few convincing details were provided to substantiate this claim, and as a result it has met with some skepticism.

In this work, we remedy the situation by giving a rigorous theoretical and practical confirmation that the log-unit lattice in indeed efficiently decodable, in cyclotomics of prime-power index. The proof consists of two main technical contributions: the first is a geometrical analysis, using tools from analytic number theory, of the canonical generators of the group of cyclotomic units. The second shows that for a wide class of typical distributions of the short generator, a standard lattice-decoding algorithm can recover it, given any generator.

Authors: Ronald Cramer, Léo Ducas, Chris Peikert, Oded Regev.