Recovering Short Generators of Principal Fractional Ideals in Cyclotomic Fields of Conductor $p^\alpha q^\beta$

Patrick Holzer[1], Thomas Wunderer[1], and Johannes A. Buchmann[1]

TU Darmstadt

Abstract. Several recent cryptographic constructions – including a public key encryption scheme, a fully homomorphic encryption scheme, and a candidate multilinear map construction – rely on the hardness of the *short generator principal ideal problem* (SG-PIP): given a $\mathbb{Z}$-basis of some principal (fractional) ideal in an algebraic number field that is guaranteed to have an exceptionally short generator with respect to the logarithmic embedding, find a shortest generator of the principal ideal. The folklore approach to solve this problem is to split it into two subproblems. First, recover some arbitrary generator of the ideal, which is known as the *principal ideal problem (PIP)*. Second, solve a bounded distance decoding (BDD) problem in the *log-unit lattice* to transform this arbitrary generator into a shortest generator of the ideal. The first problem, i.e., solving the PIP, is known to be solvable in polynomial time on *quantum* computers for arbitrary number fields under the *generalized Riemann hypothesis* due to Biasse and Song. Cramer, Ducas, Peikert, and Regev showed, based on the work of Campbell, Groves, and Shepherd, that the second problem can be solved in polynomial time on *classical* computers for *cyclotomic number fields of prime-power conductor*.

In this work, we extend the work of Cramer, Ducas, Peikert, and Regev to cyclotomic number fields $K = \mathbb{Q}(\xi_m)$ of conductor $m = p^\alpha q^\beta$, where p, q are distinct odd primes.

In more detail, we show that the second problem can be solved in classical polynomial time (with quantum polynomial time precomputation) under some sufficient conditions, if (p, q) is an (α, β)-*generator prime pair*, a new notion introduced in this work. We further provide experimental evidence that suggests that roughly 35% of all prime pairs are (α, β)-generator prime pairs for all α and β. Combined with the work of Biasse and Song our results show that under sufficient conditions the SG-PIP can be solved in quantum polynomial time in cyclotomic number fields of composite conductor of the form $p^\alpha q^\beta$.

Keywords: Lattice-based cryptography, principal ideal lattices, SG-PIP, SVP, key recovery, cryptanalysis.