Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP

Olivier Bernard[1,2],
joint work with Andrea Lesavourey[1], Tuong-Huy Nguyen[1,3] and Adeline Roux-Langlois[1]

[1] Univ Rennes, CNRS, IRISA
{olivier.bernard, andrea.lesavourey, tuong-huy.nguyen, adeline.roux-langlois}@irisa.fr
[2] Thales, Gennevilliers, Laboratoire CHiffre
[3] DGA Maîtrise de l'Information, Bruz

The Twisted-PHS algorithm, solving Approx-SVP for ideal lattices on any number field, was introduced by Bernard and Roux-Langlois in 2020 [BR20], based on the PHS algorithm by Pellet-Mary, Hanrot and Stehlé in 2019 [PHS19]. The authors of [BR20] performed experiments for prime conductors cyclotomic fields of degrees at most 70, reporting exact approximation factors reached in practice as well as the geometric characteristics of the observed lattices. The main obstacle for these experiments is the computation of a log-$\mathcal{S}$-unit lattice, which requires classical subexponential time.

In this work, we extend these experiments to 210 cyclotomic fields of *any* conductor m and of degree up to 210. Building upon new results from Bernard and Kučera [BK21] on the Stickelberger ideal, we construct a maximal set of independent $\mathcal{S}$-units lifted from the maximal real subfield using explicit Stickelberger generators obtained via Jacobi sums. Hence, we obtain full-rank log-$\mathcal{S}$-unit sublattices fulfilling the role of approximating the full Twisted-PHS lattice. First, we observed the same geometric phenomena as in [BR20] for any cyclotomic field and any sublattice, even in the largest tested dimensions. We also measured the reached approximation factors in this degraded regime, obtaining Fig. 1, which gives a reliable upper bound on the performances of the Twisted-PHS algorithm. These data are of utmost importance to concretely support either way recent discussions on the power of $\mathcal{S}$-unit attacks while been freed of the small dimension barrier, and open the way to obtaining concrete reliable estimations of the reached approximation factors of this class of algorithms in cryptographically relevant dimensions.

As a side result, we use the knowledge of these explicit Stickelberger elements to remove almost all quantum steps in the CDW algorithm, by Cramer, Ducas and Wesolowski in 2021, under the mild restriction that the plus part of the class number verifies $h_m^+ \leq O(\sqrt{m})$.

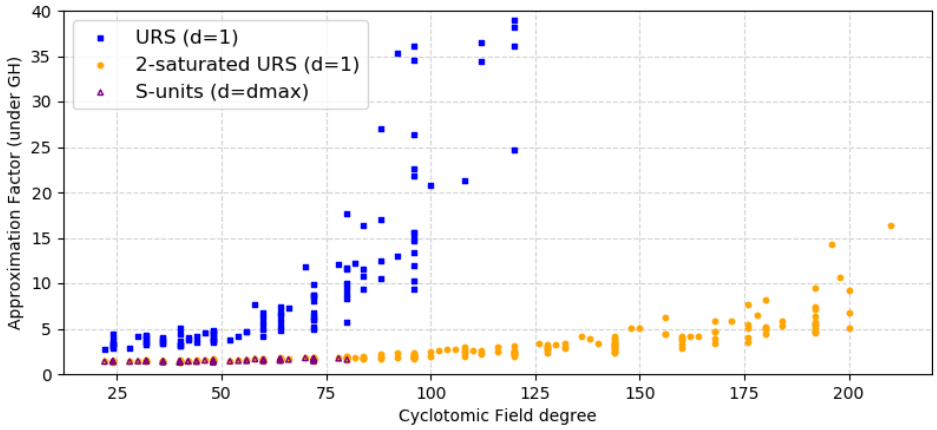

FIG. 1 – Approximation factors, estimated with Gaussian Heuristic, reached by Tw-PHS for cyclotomic fields of degree $\varphi(m) \leq 210$ with $h_m^+ = 1$ on lattices L_{urs}, L_{sat} and L_{su} (when available).

References

BK21. O. BERNARD, R. KUČERA: *A short basis of the Stickelberger ideal of a cyclotomic field.* arXiv:2109.13329 [math.NT], 2021.

BR20. O. BERNARD, A. ROUX-LANGLOIS: *Twisted-PHS: Using the product formula to solve Approx-SVP in ideal lattices.* In *ASIACRYPT*, vol. 12492 of *LNCS*, pp. 349–380, Springer, 2020.

PHS19. A. PELLET-MARY, G. HANROT, D. STEHLÉ: *Approx-SVP in Ideal lattices with pre-processing.* In *EUROCRYPT (2)*, vol. 11477 of *LNCS*, pp. 685–716, Springer, 2019.