Approx-SVP in Ideal Lattices with Pre-processing

Alice Pellet--Mary Damien Stehlé

The Learning With Errors problem (LWE) introduced by Regev in [Reg05] has proved invaluable towards designing cryptographic primitives. However, as the problem instances involve unstructured matrices whose dimensions need to grow at least linearly with the security parameter, LWE often results in primitives that are not very efficient. In order to improve the efficiency, Stehlé, Steinfeld, Tanaka and Xagawa [SSTX09] introduced the search Ideal-LWE problem which involves polynomials modulo $X^n + 1$ for n a power of two, and Lyubashevsky, Peikert and Regev [LPR10] exhibited the relationship to power-of-two cyclotomic fields, gave a reduction from the latter search problem to a decision variant, and tackled more general rings. This is now referred to as Ring-LWE, and leads to more efficient cryptographic constructions. To support the conjecture that Ring-LWE is computationally intractable, the authors of [SSTX09, LPR10] gave two distinct polynomial-time quantum reductions from approx-SVP restricted to ideal lattices to Ring-LWE. Approx-SVP consists in finding a non-zero vector of an input lattice, whose norm is within a prescribed factor larger than the lattice minimum. Ideal lattices are lattices corresponding to ideals of the rings of integers of power-of-two cyclotomic fields. A third quantum reduction from approx-SVP for ideal lattices to Ring-LWE was recently proposed by Peikert, Regev and Stephens-Davidowitz [PRS17]. It has the advantage of working for all number fields. As always, the value of these reductions is highly dependent on the intractability of the starting problem, i.e., approx-SVP for ideal lattices in our case. In this work, we investigate the intractability of ideal approx-SVP for power-of-two cyclotomic fields, in a situation where we allow pre-processing depending only on the field and not on the input ideal (this is a non-uniform model of computation).

In arbitrary lattices, the best known trade-off between the time complexity and the approximation factor is given by Schnorr's hierarchy of reduction algorithms [Sch87], whose most popular variant is the BKZ algorithm [SE94]. For any real number $\alpha \in [0, 1]$ and any lattice L of dimension n given by an arbitrary basis, it allows to compute a non-zero vector of L which is no more than $2^{\widetilde{O}(n^{\alpha})}$ times longer than a shortest non-zero one, in time $2^{\widetilde{O}(n^{1-\alpha})}$. In the case of ideal lattices in a cyclotomic ring of prime-power conductor (i.e., the ring of integers of $\mathbb{Q}(\zeta_m)$ where m is a prime power and ζ_m is a complex primitive m-th root of unity), it has been shown that it is possible to obtain a better trade-off than the BKZ algorithm, in the quantum setting. More precisely, building upon a blueprint given in [CGS14] and on the blog page of Dan Bernstein,[1] the solver of Biasse and Song [BS16] and the work of Cramer, Ducas, Peikert

[1] See https://blog.cr.yp.to/20140213-ideal.html

and Regev [CDPR16] gave a quantum polynomial-time algorithm which solves approx-SVP with a $2^{\widetilde{O}(\sqrt{n})}$ approximation factor, for *principal* ideal lattices. This work was then extended by Cramer, Ducas and Wesolowski [CDW17] to any ideal lattice of a cyclotomic ring of prime-power conductor. Put together, these results give us the trade-off between approximation factor and time complexity drawn in red dashes in Figure 1. This is better than the BKZ algorithm when the approximation factor is larger than $2^{\widetilde{O}(\sqrt{n})}$. However, for smaller approximation factors, Schnorr's hierarchy remains the record holder. One could also hope to improve the trade-off for classical computing, by replacing the quantum principal ideal solver of [BS16] by the classical one of Biasse, Espitau, Fouque, Gélin and Kirchner [BEF$^+$17]. However, this classical principal ideal solver runs in sub-exponential time $2^{\widetilde{O}(\sqrt{n})}$, hence combining it with the works of [CDPR16, CDW17] results in a classical approx-SVP algorithm for a $2^{\widetilde{O}(\sqrt{n})}$ approximation factor in time $2^{\widetilde{O}(\sqrt{n})}$. Up to the $\widetilde{O}(\cdot)$ terms, this is exactly the trade-off obtained using Schnorr's hierarchy.

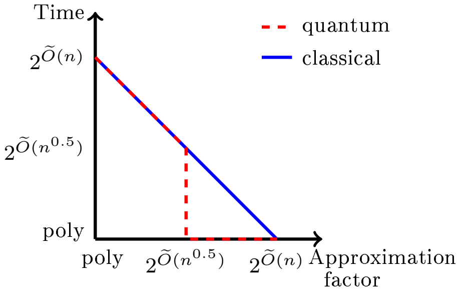

Figure 1: Prior time/approximation trade-offs for approx-SVP in ideal lattices in cyclotomic rings of prime power degree.

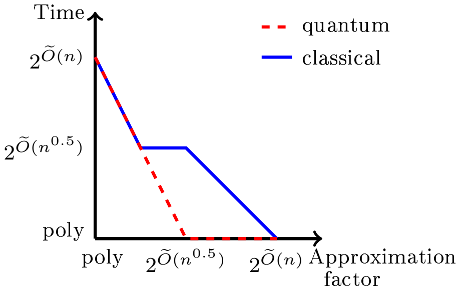

Figure 2: New trade-offs for ideal lattices in cyclotomic rings of power-of-two degree (with a pre-processing of cost $2^{\widetilde{O}(n)}$).

Contributions. We improve the trade-off above by allowing the algorithm to perform some pre-computations on the cyclotomic ring. More precisely, we consider only cyclotomic rings whose conductor is a power of two, that is, rings of the form $R = \mathbb{Z}[X]/(X^n + 1)$ where n is a power of two. For these rings, our algorithm performs some pre-processing on the ring R, in exponential time $2^{O(n)}$. Once this pre-processing phase is done and for any $\alpha \in [0, 1/2]$, the algorithm can, given any ideal lattice I of R, output a $2^{\widetilde{O}(n^{\alpha})}$ approximation of the shortest vector of I in time $2^{\widetilde{O}(n^{1-2\alpha})} + T_{\text{PIP}}(n)$, where $T_{\text{PIP}}(n)$ is the time needed to find a generator of a principal ideal in the ring R. Using the results of [BEF$^+$17] and [BS16], we can replace $T_{\text{PIP}}(n)$ by $2^{\widetilde{O}(\sqrt{n})}$ for a classical computer and by poly(n) for a quantum computer. The correctness and complexity analyses of the algorithm rely on heuristic assumptions. Our contribution is formalized in the theorem below.

Theorem (heuristic). *Let $\alpha \in [0, 1/2]$ and $R = \mathbb{Z}[X]/(X^n + 1)$ for n a power of two. Under some conjectures and heuristics, there exist two algorithms $\mathcal{A}_{\text{pre-proc}}$ and $\mathcal{A}_{\text{query}}$ such that*

- *Algorithm $A_{\text{pre-proc}}$ takes as input the ring R, runs in time $2^{O(n)}$ and outputs a hint w of bit-length $2^{\widetilde{O}(n^{1-2\alpha})}$.*
- *Algorithm A_{query} takes as input any ideal I of R (whose algebraic norm is bounded by $2^{\text{poly}(n)}$) and the hint w output by $A_{\text{pre-proc}}$, and outputs an element $x \in I$ such that $\|x\|_2 \leq 2^{\widetilde{O}(n^{\alpha})} \cdot \lambda_1(I)$, where $\lambda_1(I)$ is the length of the shortest non zero vector of I. It runs in classical time $\max(2^{\widetilde{O}(n^{1-2\alpha})}, 2^{\widetilde{O}(\sqrt{n})})$ or in quantum time $2^{\widetilde{O}(n^{1-2\alpha})}$.*

Varying α between 0 and 1/2, we obtain the trade-offs represented in Figure 2. These improve upon the prior trade-offs, both for quantum and classical computers. Note that in Figure 2, we only plot the time needed for the query phase of the algorithm, but there is a pre-processing phase of exponential time performed before on the ring R. Also, the new algorithm is no better than Schnorr's hierarchy in the classical setting when the time complexity is smaller than $2^{\widetilde{O}(\sqrt{n})}$. Hence, in Figure 2, we plotted the trade-offs obtained using Schnorr's hierarchy when they are better than the one obtained with the new algorithm. The new algorithm gives a quantum acceleration for approx-SVP for ideal lattices in power-of-two cyclotomic rings, for all approximation factors $2^{\widetilde{O}(n^{\alpha})}$ with $\alpha \in (0,1)$. This extends [CDW17, CDPR16, BS16], which obtained such a quantum acceleration for $\alpha \in [1/2, 1)$. The new algorithm also gives a classical acceleration, but only for $\alpha \in (0, 1/2)$. One may wonder whether the trade-offs corresponding to time complexity no greater than $2^{\widetilde{O}(\sqrt{n})}$ (which rely on Schnorr's hierarchy) can be improved.

We note that the new algorithm can also be seen as a non-uniform algorithm. Indeed, the pre-computation part of our algorithm only relies on the dimension n of the cyclotomic ring. Hence, our result also states that, for any dimension n which is a power of two and any $\alpha \in [0, 1/2]$, there exists a (non-uniform) algorithm that solves approx-SVP for ideal lattices in the cyclotomic ring of degree n, with approximation factor $2^{\widetilde{O}(n^{\alpha})}$ and in time $2^{\widetilde{O}(n^{1-2\alpha})} + T_{\text{PIP}}(n)$.

Technical overview.

Our algorithm is inspired from [CDPR16, CDW17]. We first focus on solving approx-SVP in principal ideals, as they are simpler to work with. Then, following [CDW17], we extend our result from principal ideals to arbitrary ideals.

In [CDPR16], Cramer *at al.* show, by analyzing the log-unit lattice, that given an arbitrary generator of a principal ideal, then one can compute in polynomial time another generator which is a $2^{\widetilde{O}(\sqrt{n})}$ approximation of the minimum of the lattice. Combined with the principal ideal solver of Biasse *et al.* [BS16] which computes a generator of any principal ideal in quantum polynomial time, this gives a quantum polynomial time approx-SVP solver with approximation factor $2^{\widetilde{O}(\sqrt{n})}$. Cramer *et al.* find a short generator by transforming the problem into a Closest Vector Problem (CVP) in the log-unit lattice, where the target vector is the logarithm of the generator output by the principal ideal solver of Biasse *et al.*. In order to efficiently solve the CVP instance, Cramer *et al.* also exhibit a 'good' basis of the log-unit lattice, which enables them to obtain a generator which is a $2^{\widetilde{O}(\sqrt{n})}$ approximation of the lattice minimum. One could then wonder whether it is possible to find an even better basis of the log-unit lattice, in order to find shorter generators. However, Cramer *at al.* also proved that the generator they output is the smallest possible for general ideals (up to a poly-logarithmic factor in the exponent). This is because the log-unit lattice is not sufficiently dense, and so some generators of principal ideals may be far from all vectors of the log-unit lattice.

In order to find smaller vectors of the ideal (which will not be generators in the general case), the idea underlying our algorithm is to increase the density of the log-unit lattice by adding to it elements of small algebraic norms.[2] We show that by adding sufficiently many such elements to the log-unit lattice, we obtain a lattice whose covering radius is heuristically sufficiently small so that given a generator of a principal ideal we may find a non-zero vector of the ideal whose Euclidean norm is only polynomially larger than the first minimum of the ideal. However, even if we know that the closest vector to some generator will lead to a short vector, it can stop being possible to find such a vector efficiently. Indeed, we do not a priori have a 'good' basis of the new lattice, which could allow us to solve the involved CVP instance with a small approximation factor.

As a second contribution, we describe a strategy to solve the approx-CVP instance in this lattice L. At first glance, it may seem that we transformed an approx-SVP instance in a structured lattice into an approx-CVP instance in a lattice that is algebraically less appealing. However, it is important to observe that the lattice L does not depend on the ideal in which we want to solve the approx-SVP instance, but only on the cyclotomic ring we work with. The only part of the CVP instance that depends on the ideal is the target point (which will be given by a generator of the ideal). Hence, one could consider performing some pre-processing on the lattice L, in order to improve the time complexity of the query phase. To solve this approx-CVP instance with pre-processing on the lattice L, we use an algorithm of Laarhoven [Laa16]. This gives us the time/approximation trade-off drawn in Figure 2.

Finally, we extend the algorithm for principal ideals to arbitrary ideals. This is done using the same ideas as Cramer *et al.* in [CDW17]. The goal is, given any ideal I, to find an ideal J such that IJ is principal and then find a small vector in IJ (which will also be a vector of I) using the approx-SVP solver for principal ideals. It can be proven that if v is a $2^{\widetilde{O}(n^\alpha)}$ approximation of the shortest vector in IJ, then it is a $\max(\mathcal{N}(J)^{1/n}, 2^{\widetilde{O}(n^\alpha)})$ approximation of the shortest vector in I (where $\mathcal{N}(J)$ is the algebraic norm of J). In [CDW17], Cramer *et al.* are interested in generalizing the approx-SVP solver of [CDPR16] with approximation factor $2^{\widetilde{O}(n^{0.5})}$. Hence, they show how to construct in polynomial time an ideal J with algebraic norm smaller than $2^{\widetilde{O}(n^{1.5})}$. In our case, we would like to decrease the algebraic norm of the ideal J to $2^{\widetilde{O}(n^{1+\alpha})}$ (for $\alpha \in [0, 1/2]$). For this, we allow ourselves to increase the computation time up to $2^{\widetilde{O}(n^{1-2\alpha})}$ and to perform some pre-computations on the ring. This is in line with the algorithm for principal ideals described above. Looking more into the details, the way the authors

[2] Adding elements to the log-unit lattice was also suggested by Dan Bernstein in the 'S-unit attacks' post on the online forum https://groups.google.com/forum/#!forum/cryptanalytic-algorithms. We note that we only focus on the magnitude of the algebraic norms of the elements we add, and not on their arithmetic properties as in this forum post.

of [CDW17] find their ideal J is by solving an approx-CVP instance in some lattice, for which they have a 'good' basis. Similarly to the log-unit situation described above, the lattice used in this approx-CVP instance only depends on the cyclotomic ring, and only the target point depends on the ideal. We modify the lattice used by [CDW17], in order to ensure that it is dense enough so that we can find a lattice point sufficiently close to any target. Then, using Laarhoven's algorithm for approx-CVP with pre-computation, we can find a good ideal J whose algebraic norm is at most $2^{\widetilde{O}(n^{1+\alpha})}$. This completes the description of our approx-SVP solver for any ideal.

References

[BEF+17] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin, and P. Kirchner. Computing generator in cyclotomic integer rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 60–88. Springer, 2017.

[BS16] J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 893–902. Society for Industrial and Applied Mathematics, 2016.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In M. Fischlin and J.-S. Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, pp. 559–585. Springer, Heidelberg, May 2016.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. Short stickelberger class relations and application to ideal-svp. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 324–348. Springer, 2017.

[CGS14] P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale, 2014. Available at http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.

[Laa16] T. Laarhoven. Sieving for closest lattice vectors (with preprocessing). In *International Conference on Selected Areas in Cryptography*, pp. 523–542. Springer, 2016.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pp. 1–23. Springer, Heidelberg, May 2010.

[PRS17] C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In *Proceedings of the 49th Annual ACM*

SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017, pp. 461–473. ACM, 2017.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *37th Annual ACM Symposium on Theory of Computing*, pp. 84–93. ACM Press, May 2005.

[Sch87] C. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53:201–224, 1987.

[SE94] C. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In M. Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, pp. 617–635. Springer, Heidelberg, December 2009.