Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-023-01320-7

Provable lattice reduction of $\mathbb{Z}^n$ with blocksize $n/2$

Léo Ducas[1,2]

Received: 27 March 2023 / Revised: 9 September 2023 / Accepted: 7 October 2023

Abstract
The Lattice Isomorphism Problem (LIP) is the computational task of recovering, assuming it exists, an orthogonal linear transformation sending one lattice to another. For cryptographic purposes, the case of the trivial lattice $\mathbb{Z}^n$ is of particular interest ($\mathbb{Z}$LIP). Heuristic analysis suggests that the BKZ algorithm with blocksize $\beta = n/2+o(n)$ solves such instances (Ducas, Postlethwaite, Pulles, van Woerden, ASIACRYPT 2022). In this work, I propose a provable version of this statement, namely, that $\mathbb{Z}$LIP can indeed be solved by making polynomially many calls to a Shortest Vector Problem oracle in dimension at most $n/2+1$.

Keywords Lattice Isomorphism Problem · Lattice reduction · Provable algorithm

Mathematics Subject Classification 11H06 · 11H55 · 11H56 · 11T71 · 11Y16 · 68Q25

1 Introduction

Two lattices $\Lambda, \Lambda' \subset \mathbb{R}^n$ are said to be isomorphic if there exists a rotation between them, that is a linear orthogonal map $O \in \mathcal{O}_n(\mathbb{R})$ such that $O \cdot \Lambda = \Lambda'$. Determining isomorphism and finding it if it exists is called the Lattice Isomorphism Problem (LIP). The best known provable algorithm [14] has super-exponential time $n^{O(n)}$, but in practice other methods are often preferred [12, 14, 17, 18]. They essentially consist in finding all the shortest vectors, to then solve a (potentially exponentially large) instance of the Graph Isomorphism Problem.

The LIP has recently been proposed as a foundation for cryptographic construction [8, 10], and the case of rotations of $\mathbb{Z}^n$ quickly arose as a natural instantiation for simple and efficient cryptographic design [9, 11]. In this case (coined $\mathbb{Z}$LIP [8]), finding the shortest vectors is sufficient, which generically implies a provable algorithm in time $2^{n+o(n)}$ thanks to the worst-case Shortest Vector Problem (SVP) algorithm [1, 2].

Communicated by D. Stehle.

✉ Léo Ducas
ducas@cwi.nl

[1] Cryptology Group, CWI, Amsterdam, The Netherlands

[2] Mathematical Institute, Leiden University, Leiden, The Netherlands

Published online: 11 November 2023

1.1 Prior provable algorithms for $\mathbb{Z}$LIP

Yet, one might doubt that finding the shortest vector in rotations of $\mathbb{Z}^n$ should be as hard as in a worst-case lattice. It was suggested already by Szydlo [21] than finding rather short yet not necessarily the shortest vector could be sufficient to solve LIP over $\mathbb{Z}^n$, though it was not exactly clear at the time how short of a vector is required nor how costly it would be to find it. The only formal statement of Szydlo is a reduction from $\mathbb{Z}$LIP to a decisional version of LIP for mild sparsification of $\mathbb{Z}^n$.

Bennett et al. [8] indeed proposed a provable algorithm with complexity $2^{n/2+o(n)}$ for this task, via a polynomial time reduction Gap-SVP in the same dimension n, with a constant approximation factor. Despite the relaxation to an Gap version of SVP, block reductions algorithm remain insufficient to reach this result, as they are only known to provide $\Omega(\sqrt{n})$ approximation factors even when the blocksize is close to the full dimension [3, 13, 16]. Instead, they rely on an algorithm of [2] tailored to Gap-SVP; the core of this algorithm is similar to the $2^{n+o(n)}$ algorithm for exact-SVP, in particular it operate on lattices of full dimension n, but the gap allows for some complexity improvements.

1.2 Heuristic algorithms for $\mathbb{Z}$LIP

As for many other lattice problems, the best provable complexity stands in contrast with the heuristic state of the art. Using standard heuristic analysis (see [4] for a survey), Ducas, Postlethwaite, Pulles, and van Woerden [11, Sec. 4.2] argued that the block reduction algorithm BKZ [19, 20] should be successful in finding those shortest vectors using a blocksize of $\beta = n/2 + o(n)$ because the shortest vectors are unusually short compared to that of a random lattice by a factor $\Theta(\sqrt{n})$.

More specifically, it is argued that when the lattice is sufficiently reduced, the last block of the lattice has a large volume, and therefore it is not expected to contain a vector shorter than the ones we are looking for. This step of the reasoning is entirely heuristic. From there, one concludes that an SVP call on this last block should indeed find (a projection[1] of) some unit vectors of the full $\mathbb{Z}^n$ lattice. This heuristic conclusion is confirmed by extensive experiments.

Plugging the best heuristic complexity of $2^{.292\beta+o(\beta)}$ for SVP [7] in dimension β leads to a heuristic complexity of $2^{.146n+o(n)}$.

The result

In this work, I propose a provable variant of the heuristic claim of [11, Sec. 4.2], namely, exhibiting a block reduction algorithm for solving $\mathbb{Z}$LIP, that indeed relies on polynomially many calls to an SVP oracle in dimensions less than $n/2 + 1$. The algorithm is however not exactly BKZ [19, 20], but rather a specialization of the Slide algorithm [3, 13, 16]. The key remark is that projected lattices of $\mathbb{Z}^n$ have a shortest vector of length either 1 or smaller than $\sqrt{1 - 1/n}$ (Lemmas 3 and 4). This implies that the slide algorithm makes significant progress at each iteration, until the first block is itself a rotation of $\mathbb{Z}^k$ where $n = 2k + 1$.

Note that this does not directly improve the best provable complexity for $\mathbb{Z}$LIP, as plugging in the best provable algorithm [1, 2] for SVP in dimension $n/2$ also leads to a $2^{n/2+o(n)}$ complexity, as reached by different means in [8]. While those final complexity are similar,

[1] Lifting this projected solution to a full solution should then be rather easy according to further heuristic reasoning [5, Claim 1].

the complexity theoretic reduction underlying these results are different. The approach of [8] maintain the dimension of the lattice to n, but relax the problem to a gap version with an constant approximation factor.[2] On the other hand the approach of this work divides the SVP dimension but doesn't relax the problem.[3] Another difference is that our reduction is deterministic while that of [8] is probabilistic.

Despite the lack of direct impact on the complexity of $\mathbb{Z}$LIP of our approach, we found it motivating for the following reason. It appears to be the first case where we can prove that block reduction does find the shortest vector with a blocksize $\beta < n$ despite the lack of uniqueness of the shortest vector. Indeed, to the best of my knowledge, this was only proved [3, 16] for lattices with polynomial gap of at least $\Omega(\sqrt{n})$ between the first and second minima $\lambda_1(L)$ and $\lambda_2(L)$. On the contrary, lattices that are rotation of $\mathbb{Z}^n$ have all their successive minima equal $\lambda_1(L) = \lambda_2(L) = \cdots = \lambda_n(L) = 1$.

In that sense, this result is a step toward closing the gap between the theory and practice. Indeed heuristic and experiments suggested that the uniqueness of the shortest vector is essentially irrelevant in practice, what matter is how unusually short it is compared to Minkowski's bound [5, 10, 11].

2 Preliminaries

We write a matrix $B \in \mathbb{R}^{m\times n}$ as $B = (b_0, \ldots, b_{n-1})$ where b_i is the ith column vector of B. We denote by I_n the $n \times n$ identity matrix.

2.1 Lattices

If $B \in \mathbb{R}^{m\times n}$ has full-column rank n, the lattice $\mathcal{L}$ generated by the basis B is denoted by $\mathcal{L}(B) = B \cdot \mathbb{Z}^n = \{B \cdot x \mid x \in \mathbb{Z}^n\}$. We denote by $B^\star = (b_0^\star, \ldots, b_{n-1}^\star)$ the Gram–Schmidt orthogonalization (GS) of the matrix $(b_0, \ldots, b_{n-1})$. For $i \in \{0, \ldots, n-1\}$, we denote the projection orthogonal to the span of $(b_0, \ldots, b_{i-1})$ by π_i; π_0 denotes "no projection", i.e. the identity. For $0 \le i \le j < d$, we denote by $B_{[i:j]}$ the local projected block $(\pi_i(b_i), \ldots, \pi_i(b_j))$, and when the basis is clear from context, by $\mathcal{L}_{[i:j]}$ the lattice generated by $B_{[i:j]}$. Note that both bounds of the interval $[i : j]$ are inclusive in this notation.

2.2 Metric and volumetric properties

The Euclidean norm of a vector v is denoted by $\|v\|$. The volume (or determinant) of a lattice $\mathcal{L}(B)$ is $\mathrm{vol}(\mathcal{L}(B)) = \sqrt{|\det(B^T \cdot B)|} = \prod_i \|b_i^\star\|$. It is an invariant of the lattice, it is also invariant under rotation, and is non-negative for any lattice L. The first minimum of a lattice $\mathcal{L}$ is the norm of a shortest non-zero vector, denoted by $\lambda_1(\mathcal{L})$. We use the abbreviations $\mathrm{vol}(B) = \mathrm{vol}(\mathcal{L}(B))$ and $\lambda_1(B) = \lambda_1(\mathcal{L}(B))$.

The ith minimal distance $\lambda_i(L)$ is defined as the smallest radius $r > 0$ such that L contains i many linearly independent vectors. These quantities are also invariants under rotation.

[2] They in fact propose a trade-off, which can reach larger approximation factors at the cost of making super-polynomially or even exponentially many calls to the Gap-SVP oracle.

[3] or only just a little bit: we remark later on that our approach would survive an tiny approximation factor of $1 + o(n^{-1/2})$

2.3 Primitivity

We write $\pi_X^\perp$ for the projection orthogonal to the space spanned by X for any set $X \subset \mathbb{R}^m$. A sublattice S of L is said to be primitive if $S = \mathrm{Span}_{\mathbb{R}}(S) \cap L$. Equivalently, $S \subset L$ is primitive if and only if there exists another sublattice $S' \subset L$ such the sum $S + S'$ is direct and $L = S \oplus S'$. In particular, if B is a basis of L, then the lattice generated by any subset of the column of B is a primitive sublattice of L.

The main purpose of primitivity in this work is the following property. For a primitive sublattice $S \subset L$ and any $x \in L \backslash S$, it holds that the projection of x orthogonally to S is a non-zero lattice vectors of $\pi_S^\perp(L)$: $\pi_S^\perp(x) \neq 0$.

2.4 Reduction

Definition 1 (*Size reduction*) A basis $B \in \mathbb{R}^{m\times n}$ of a lattice $L \subset \mathbb{R}^m$ is said to be size-reduced if $\langle b_j, b_i^\star\rangle \leq \frac{1}{2}\|b_i^\star\|^2$ for all $j > i$.

We recall that there is a polynomial-time algorithm that size-reduces a basis [6, 15], and that this algorithms does not affect the Gram–Schmidt orthogonalization $B^\star$.

Definition 2 (*SVP and HKZ reduction*) A basis $B \in \mathbb{R}^{m\times n}$ of a lattice $L \subset \mathbb{R}^m$ is said to be SVP-reduced if b_1 is a shortest vector of L. It is said to be HKZ-reduced if it is size-reduced and if each block $B_{[i:n-1]}$ for $i \in \{0, \ldots, n-1\}$ is SVP-reduced.

Note that by the volume invariance, SVP reduction minimizes $\|b_0\| = \|b_0^\star\|$, it also maximizes the remaining volume $\mathrm{vol}(B_{[1:n-1]}) = \prod_{i=1}^{n-1}\|b_i^\star\|$.

2.5 Duality

Definition 3 (*Dual Lattice*) The *dual lattice* $\mathcal{L}^\vee$ of a lattice $\mathcal{L} \subset \mathbb{R}^m$ is the set of all $w \in \mathrm{Span}_{\mathbb{R}}(\Lambda)$ such that $\langle w, \mathcal{L}\rangle \subseteq \mathbb{Z}$.

An important fact for our proof is that $\mathbb{Z}^n$ is self-dual, and so are all of its rotations.

There is a natural correspondence between bases of the primal and bases of the dual, given by the (pseudo-)inverse transpose: if B is a basis of Λ then $D = B \cdot (B^T \cdot B)^{-1}$ is a basis of the dual lattice $\mathcal{L}^\vee$. For our purpose, we will only need the fact that the last dual vector d_n is the reciprocal of the last Gram–Schmidt vector: $d_{n-1} = b_{n-1}^\star/\|b_{n-1}^\star\|^2$; in particular $\|d_{n-1}\| = 1/\|b_{n-1}^\star\|$. We refer to [3, 16] for more background on reduction and duality.

For this reason, it is natural to consider the dual basis in reversed order. In particular, by applying SVP reduction in the dual, we mean to minimize $\|d_{n-1}\|$, or equivalently maximize $\|b_{n-1}^\star\|$.

2.6 $\mathbb{Z}$LIP

Let Λ be a rotation of $\mathbb{Z}^n$. We assume n to be odd and write $n = 2k + 1$ for some integer k. The case of even n can be treated by artificially adding an extra orthogonal component defining a lattice $\Lambda^+ = \Lambda \oplus \mathbb{Z}$. Note that this restriction seemingly prevents direct reduction from $\mathbb{Z}$SVP to $\mathbb{Z}$LIP by induction[4]: instead we will directly solve $\mathbb{Z}$LIP.

[4] or at least makes it less straightforward: the expert reader might see a proof path invoking the random self-reducibility of LIP [10, Lemma 3.9] and the automorphism group of $\mathbb{Z}^n$.

We denote $E = (e_0, \ldots, e_{2k})$ some orthogonal basis of Λ. The problem is to find any such orthogonal basis given any basis of Λ as input,[5] i.e. to find E up to signs and permutation. Note that the set $\{\pm e_i\}$ is precisely the set of shortest vectors of Λ.

Note further that this is equivalent to finding an HKZ-reduced basis of Λ (a statement that is not necessarily true for all lattices). Indeed, the shortest vectors are exactly $\pm e_i$ so an HKZ basis must start with such a vector. Projecting orthogonally to any of those vectors gives a rotation of $\mathbb{Z}^{n-1}$; it remains to unroll the inductive definition of HKZ reduction.

3 A Provable $\mathbb{Z}$LIP algorithm

We consider the following algorithm, which may be viewed as a specialization of the Slide algorithm [3, 13, 16], namely the number of block is fixed to 2 and the stopping condition is tailored to the special case of rotations of $\mathbb{Z}^n$.

Note that the algorithm is invariant by rotation of the input. Hence, it is sufficient to analyze its behavior for the case $\Lambda = \mathbb{Z}^n$.

Algorithm 1 An algorithm for $\mathbb{Z}$LIP

```
Require: A basis $B$ of $\Lambda$, $\Lambda$ being a rotation of $\mathbb{Z}^n$, where $n = 2k + 1$ is odd.
Ensure: An orthonormal basis $B$ of $\Lambda$
while $\mathrm{vol}(B_{[0\ldots k-1]}) > 1$ do
    Dual-SVP reduce the block $B_{[0:k]}$
    Primal-SVP reduce the block $B_{[k:2k]}$
end while
Primal-HKZ reduce the block $B_{[0:k-1]}$
Primal-HKZ reduce the block $B_{[k:2k]}$
return $B$
```

3.1 Partial Correctness

Let us start by explaining why the algorithm succeeds when it terminates. The central argument will be that the first block is isometric to $\mathbb{Z}^k$ (Lemma 2). To establish it, let us first state the following.

Lemma 1 *Let $A, B \in \mathbb{R}^{n \times n}$ be two positive symmetric definite matrices. Then* $\det(A + B) \geq \det(A)$.

Proof This follows directly from the fact that $H \mapsto \det(H)^{1/n}$ is concave on the space of positive symmetric definite matrices.[6] In particular it holds that $\det(A+B)^{1/n} \geq \det(A)^{1/n} + \det(B)^{1/n}$. Because $\det(B) \geq 0$, we have $\det(A + B)^{1/n} \geq \det(A)^{1/n}$, and we conclude. □

Lemma 2 *Any sublattice $L \subset \mathbb{Z}^n$ of rank $k \geq 1$ has non-zero integer squared volume. Furthermore, if* $\mathrm{vol}(L) = 1$, *then L is isomorphic to $\mathbb{Z}^k$.*

[5] There exist an equivalent and sometime advatageous formulation of LIP using positive definite quadratic forms, where basis are replaced by their Gram matrices. In our context, we find the explicit basis formalism to be more convenient. We refer to [10, 14] for this alternative formulation.

[6] See exercises 209, 218 and 219 of http://perso.ens-lyon.fr/serre/DPF/exobis.pdf for three different proofs of this fact. One may alternatively invoke the Brunn–Minkowski theorem.

Proof Let $B \in \mathbb{R}^{n\times k}$ be a basis of L. Because $L \subset \mathbb{Z}^n$, B must be an integer matrix, and $\mathrm{vol}(L)^2 = \det(|B^T \cdot B|)$ is therefore an integer. It is also non-zero, because L is a lattice.

For the second property, consider a basis B of L in Hermite Normal Form. Up to a permutation of the rows, $B = \left[\begin{smallmatrix} X \\ Y \end{smallmatrix}\right]$ where X is lower triangular and non-degenerate. Note that $B^T B = X^T X + Y^T Y$. Lemma 1 gives that $\det(X^T X + Y^T Y) \geq \det(X^T X)$. Because both $X^T X$ is integral and non-degenerate, and since $\det(B^T B) = 1$, we have $\det(X^T X) = 1$. By the properties of Hermite Normal Form, it must therefore be the case that X is the identity matrix I_k.

Let $\eta_1, \ldots, \eta_k \geq 0$ be the eigenvalues of $Y^T Y$. Because the identity I_k is co-diagonalizable with $Y^T Y$, the eigenvalues of $B^T B = I_k + Y^T Y$ are exactly $1 + \eta_1, \ldots, 1 + \eta_k$. It remains to write $\det(B^T B) = \prod(1 + \eta_i)$ to conclude that $\eta_i = 0$ for all i, and therefore that $Y = 0$. That is, up to permutation of the rows, $B = \left[\begin{smallmatrix} I_k \\ 0 \end{smallmatrix}\right]$. The lattice L is indeed isomorphic to $\mathbb{Z}^k$. □

Theorem 1 *Algorithm 1 is partially correct, that is, if it terminates on a valid input, it outputs an orthogonal basis of the input lattice.*

Proof By Lemma 2, when the while loop terminates (Steps 1–4 of Algorithm 1), the block $B_{[0:k-1]}$ has volume 1 and it is therefore isomorphic to $\mathbb{Z}^k$; after HKZ reduction (Step 5) we have recovered k orthogonal unit vectors. Then, the projected block $B_{[k:2k]}$ is also isomorphic to $\mathbb{Z}^{k+1}$ and we recover the remaining $k + 1$ orthogonal vectors at Step 6. □

3.2 Termination

We now move to proving termination, which is done by showing that the volume of the first block decrease significantly at each loop iteration.

Lemma 3 *Let L be a primitive sublattice of $\mathbb{Z}^n$ of rank $k < n$, and let $L' = \pi_L^\perp(\mathbb{Z}^n)$. Then* $\lambda_1(L')^2 \leq 1$.

Proof Because L is not a full rank, there must exist an index j such that $e_j \notin L$. Therefore, by primitivity of L, $\pi_L^\perp(e_j) \in L'$ is non-zero, and $\|\pi_L^\perp(e_j)\| \leq \|e_j\| \leq 1$. □

Lemma 4 *Let L be a primitive sublattice of $\mathbb{Z}^n$ of rank $k < n$ and volume* $\mathrm{vol}(L) > 1$*, and let $L' = \pi_L^\perp(\mathbb{Z}^n)$. Then $\lambda_1(L')^2 \leq 1 - \frac{1}{n}$.*

Proof Consider an HKZ-reduced and size-reduced basis $B = [b_0, \ldots, b_{m-1}] \in \mathbb{Z}^{m\times n}$ of L. Because $\mathrm{vol}(L) > 1$, there is at least one b_i that is not a unit vector e_j. Let i be the minimal such index, and let S be the subset of indices j such at $e_j \in L$. Because the basis is HKZ-reduced and therefore size-reduced, b_i is orthogonal to all the e_k's such that $e_k \in L$. That is, $b_i = \sum_{k\notin S} v_k e_k$ where $v_k \in \mathbb{Z}$.

Now consider an index j that maximizes $|v_j|$, i.e., $|v_j| = \|b_i\|_\infty$; in particular $\langle e_j, b_i\rangle = \|b_i\|_\infty$. Note that e_j does not belong to L and L is a primitive sublattice of $\mathbb{Z}^n$, so $\pi_L^\perp(e_j) \in L'$ is non-zero. Furthermore,

$$\|\pi_L^\perp(e_j)\| \leq \|\pi_{b_i}^\perp(e_j)\| = \left\| e_j - \frac{\langle e_j, b_i\rangle}{\|b_i\|^2} b_i \right\|.$$

We now apply the polar identity $\|x-y\|^2 = \|x\|^2 + \|y\|^2 - 2 \cdot \langle x, y\rangle$ to conclude

$$\begin{aligned}
\|\pi_L^\perp(e_j)\|^2 &\leq 1 + \frac{\langle e_j, b_i\rangle^2 \cdot \|b_i\|^2}{\|b_i\|^4} - 2 \cdot \frac{\langle e_j, b_i\rangle^2}{\|b_i\|^2}\\
&\leq 1 - \frac{\langle e_j, b_i\rangle^2}{\|b_i\|^2}\\
&\leq 1 - \frac{\|b_i\|_\infty^2}{\|b_i\|^2} \leq 1 - \frac{1}{n}.
\end{aligned}$$

□

We are now ready to prove that Algorithm 1 terminates after polynomially many loop iterations.

Theorem 2 *On a valid input $B \in \mathbb{R}^{n\times n}$, Algorithm 1 terminates after at most $O(n^2 \log \max_i \|b_i\|)$ iterations of the main loop.*

Note that the number of iteration is polynomial in the input size. One may further apply the LLL algorithm to the input basis to enforce $\max_i \|b_i\| \leq 2^n$, to bound the number of iteration by $O(n^3)$.

Proof The core claim is that, at each loop iteration (Steps 1–4 of Algorithm 1), the volume of the block $B_{[0:k-1]}$ decreases by at least $\sqrt{1-1/n}$.

Indeed, the primal-SVP reduction step (Step 3) does not affect this block. Furthermore, this Step 3 leaves the Gram–Schmidt norm at position k to a value less than $\sqrt{1-1/n}$, by application of Lemma 4. Then, the dual-SVP reduction step (Step 2) is going to increase this Gram–Schmidt norm to at least 1, by dual application of Lemma 3. This step therefore decreases the volume of the block $B_{[0:k-1]}$ by a factor $\sqrt{1-1/n}$.

Note that at the beginning of the algorithm, the volume of that block is at most $(\max_i \|b_i\|)^k$. There are therefore at most $\log((\max \|b_i\|)^k)/\log(\sqrt{1-1/n}) = O(n^2 \log(\max_i \|b_i\|))$ loop iterations. □

Remark

One may note that the algorithm and its proof should still work if we replace exact SVP solvers with approximate SVP solver with approximation factor strictly less than $1/\sqrt{1-1/n} = 1 + 1/(2n) + O\left(1/n^2\right)$.

Acknowledgements L. Ducas was supported by the ERC-StG-ARTICULATE project (No. 947821). I am grateful to Noah Stephens-Davidowitz, Wessel van Woerden, Eamonn Postlethwaite, Huck Bennett and Thomas Espitau for helpful and inspiring discussions on this problem. I also thanks the anonymous reviewers for valuable feedback and suggestions.

References

1. Aggarwal D., Stephens-Davidowitz N.: Just take the average! an embarrassingly simple 2^n-time algorithm for SVP (and CVP). arXiv preprint (2017). arXiv:1709.01535.
2. Aggarwal D., Dadush D., Regev O., Stephens-Davidowitz N.: Solving the shortest vector problem in 2^n time using discrete Gaussian sampling. In: Proceedings of the 47th Annual ACM Symposium on Theory of Computing, pp. 733–742 (2015).
3. Aggarwal D., Li J., Nguyen P.Q., Stephens-Davidowitz N.: Slide reduction, revisited-filling the gaps in SVP approximation. In: Advances in Cryptology—CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, 17–21 August 2020, Proceedings, Part II, pp. 274–295. Springer, Cham (2020).
4. Albrecht M., Ducas L.: In: Bos J., Stam M. (eds.) Lattice Attacks on NTRU and LWE: A History of Refinements. London Mathematical Society Lecture Note Series, pp. 15– 40. Cambridge University Press, Cambridge (2021).
5. Albrecht M.R., Göpfert F., Virdia F., Wunderer T.: Revisiting the expected cost of solving uSVP and applications to LWE. In: Advances in Cryptology—ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017, Proceedings, Part I 23, pp. 297–322. Springer, Cham (2017).
6. Babai L.: On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica **6**(1), 1–13 (1986).
7. Becker A., Ducas L., Gama N., Laarhoven T.: New directions in nearest neighbor searching with applications to lattice sieving. In: Proceedings of the 27th Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 10–24. SIAM, Philadelphia (2016).
8. Bennett H., Ganju A., Peetathawatchai P., Stephens-Davidowitz N.: Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In: Hazay C., Stam M. (eds.) Advances in Cryptology—EUROCRYPT 2023, pp. 252–281. Springer, Cham (2023).
9. Blanks T.L., Miller S.D.: Generating cryptographically-strong random lattice bases and recognizing rotations of $\mathbb{Z}^n$. In: Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, 20–22 July 2021, Proceedings 12, pp. 319– 338. Springer, Berlin (2021).
10. Ducas L., van Woerden W.: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In: Advances in Cryptology—EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, 30 May–3 June 2022, Proceedings, Part III, pp. 643–673. Springer, Berlin (2022).
11. Ducas L., Postlethwaite E.W., Pulles L.N., van Woerden W.: Hawk: Module LIP makes lattice signatures fast, compact and simple. In: Advances in Cryptology—ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 5–9 December 2022, Proceedings, Part IV, pp. 65–94. Springer, Cham (2023).
12. Dutour Sikiric M., Haensch A., Voight J., van Woerden W.P.: A canonical form for positive definite matrices. ANTS **XIV**, 179 (2020).
13. Gama N., Nguyen P.Q.: Finding short lattice vectors within Mordell's inequality. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, pp. 207–216 (2008)
14. Haviv I., Regev O.: On the lattice isomorphism problem. In: Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 391– 404. SIAM, Philadelphia (2014).
15. Lenstra A.K., Lenstra H.W. Jr., Lovász L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982).
16. Nguyen P.Q.: Hermite's constant and lattice algorithms. In: Nguyen P.Q., Vallée B. (eds.) The LLL Algorithm: Survey and Applications, pp. 19–69. Springer, Berlin (2010).
17. Plesken W., Pohst M.: Constructing integral lattices with prescribed minimum. I. Math. Comput. **45**(171), 209–221 (1985).
18. Plesken W., Souvignier B.: Computing isometries of lattices. J. Symb. Comput. **24**(3–4), 327–334 (1997).
19. Schnorr C.-P.: A hierarchy of polynomial time lattice basis reduction algorithms. Theor. Comput. Sci. **53**(2–3), 201–224 (1987).
20. Schnorr C.-P., Euchner M.: Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Program. **66**(1–3), 181–199 (1994).
21. Szydlo M.: Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 433– 448. Springer, Berlin (2003).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.