# On the hull attacks against Construction A lattices

Jean-François Biasse, Alexandra Hostetler, and Anuvrat Jaindungarwal

University of South Florida

**Abstract.** In this paper, we present an algorithm for solving the Lattice Isomorphism Problem between input lattices that are isometric to the Construction A lattice of a certain code $C$. Our algorithm is a direct extension of a method due to Ducas and Gibbons (PKC 2023). We prove that the run time of our algorithm is $2^{O(n)}$ and that its success probability is $1 + o(1)$ over a random choice of $C$. Crucially, our method works when the hull $\mathcal{H}(C) = C \cap C^{\perp}$ has arbitrary dimension while the method of Ducas and Gibbons is restricted to the case of a trivial hull.

**Keywords:** Lattice based cryptography · Code based cryptography · Lattice Isomorphism Problem · Code Equivalence Problem · Hull attacks

## 1 Introduction

The *lattice isomorphism problem* (LIP) asks, given two full-rank lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ (typically represented by bases), to decide whether there exists an orthogonal transformation $O \in O(n)$ such that $O(\Lambda_1) = \Lambda_2$, and in the search version to recover such an isometry when it exists. In other words, LIP is the Euclidean analogue of classical isomorphism problems where the hidden object is a linear isometry. In particular, several digital signature schemes relying on the hardness of computing linear isometries were proposed to the on-ramp selection process of NIST: HAWK [13] (based on LIP), LESS [4] (based on the permutation and linear equivalence problems), and MEDS [16] (based on the rank-metric code equivalence problem – which did not advance to Round 2).

In this context, LIP has emerged as a credible alternative foundation for quantum-resistant public-key cryptography. A central motivation is that many *remarkable* lattices enjoy strong geometric and decoding properties, and one may hope to obtain faster or more compact cryptographic constructions by taking such a lattice as a trapdoor and hiding it via a secret isometry. This philosophy was articulated and instantiated in the framework of Ducas–van Woerden [20] and the independent work of Bennett et al [9]. In [20] cryptographic schemes for identification, KEM, and signature constructions based on (variants of) LIP were proposed, aiming to leverage decodable lattices while retaining conjectured hardness of recovering the hidden isometry. Bennett et al. [9] gave concrete instantiations where the public object is (a rotation of) $\mathbb{Z}^n$, analyzing both algorithms and cryptographic uses of such hidden rotations. In the HAWK

cryptosystem [19], LIP is instantiated with a rank-2 module over the ring of integers of a cyclotomic number field to take advantage of algorithmic optimizations available in ideal lattices (at the risk of potential vulnerabilities to algebraic attacks).

From an algorithmic standpoint, the best known *generic* algorithms for LIP remain super-polynomial in the rank. The state of the art is the $n^{O(n)}$-time algorithm of Haviv–Regev [21], which (among other consequences) places LIP in the complexity class $\mathsf{SZK}$ and gives a canonical route to solve LIP in the absence of structure. This gap between practical parameter sizes and worst-case generic algorithms is precisely what makes structured families attractive for cryptography—and also what makes them potentially vulnerable to *structure-exploiting* cryptanalysis. Recent work showed that module-LIP was computationally easy when the underlying field was totally real [25], or even when as few as one real embedding was known [2]. On the other hand, when the underlying number field is a CM field, Module-LIP was shown to reduce to the problem of finding a generator of a principal ideal in a quaternion algebra given its norm [14]. While no efficient algorithm for the principal ideal problem in quaternion algebra exists, its analogue in number fields can be solved in quantum polynomial-time [12]. This discrepancy between the hardness of LIP in general lattices and its instantiation with ideal lattices has been the motivation of a flurry of recent works on algorithms for solving module-LIP [15, 22–24, 29].

A particularly important alternative structured family arises from *Construction A*: given a linear code $C \subseteq \mathbb{F}_p^n$, one builds a lattice

$$\Lambda(C) \;=\; \{x \in \mathbb{Z}^n : x \bmod p \in C\},$$

(possibly with scaling conventions). Construction A lattices are natural cryptographic candidates because they tightly connect Euclidean geometry (lattices) with Hamming geometry (codes), and they inherit rich symmetry from the underlying code. This connection also enables attacks: Ducas and Gibbons [18] introduced the *hull attack*, adapting the classical notion of the *code hull* $C \cap C^\perp$ to a lattice setting via an $s$-hull operator, and showed that for certain Construction A instantiations one can reduce LIP to easier isomorphism tasks, effectively reducing the cost of solving LIP to $2^{O(n)}$ (instead of $n^{O(n)}$ for generic lattices via [21]). In particular [18, Sec. 5.1] analyzes the case where the relevant hull is *trivial* (the analogue of LCD behavior on the code side), which yields a reduction to the Signed Permutation Code Equivalence Problem.

Independently, there has been notable recent progress on *provable* (worst-case) algorithms for related isomorphism problems on the code side motivated by the emergence of cryptosystems based on the code equivalence problem [5, 6, 11]. In particular, Bennett et al. [7, 8] give new provable algorithms for Linear Code Equivalence (LCE) and Permutation Code Equivalence (PCE) based on prior work of Babai [3], improving the best known exponents in several regimes and clarifying fine-grained relationships between code equivalence variants and other isomorphism problems. Since Construction A provides an interface between lattices and codes, such results are directly relevant to the security landscape of

Construction A-based LIP assumptions: they inform what can be proven about the complexity of recovering hidden permutations/isometries in the associated code instances, and they provide algorithmic subroutines that can potentially be composed with lattice-side distinguishers.

*Our goal and contribution.* This paper revisits the hull attack framework of Ducas–Gibbons for Construction A lattices and targets the main obstacle to broader applicability: the assumption that the relevant hull is trivial in the sense of [18, Sec. 5.1].

**Theorem** (Main result)**.** *Let $p > 0$ be a prime. There is an algorithm that solves LIP between two input lattices that are Construction A of linear codes over $\mathbb{F}_p^n$ in time $2^{O(n)}$ with probability $1 + o(1)$ over the choice of the underlying linear code.*

Note that the above formulation hides a factor in $\mathrm{Poly}(\log(p))$ that is made explicit in Corollary 4. The algorithm presented in Ducas and Gibbon's previous work [18, Sec. 5.1] also works in time $2^{O(n)}$, but the restriction to a trivial hull means that when the underlying linear code is drawn uniformly at random among the linear codes over $\mathbb{F}_p^n$, its probability of success is bounded by $1 - 1/p$ (i.e. the bound on the probability that the hull is trivial [26]). In other words, by hoping that the hull is trivial, we can treat a fraction $1 - 1/p$ of the instances. By contrast, our method achieves a fraction $1 - o(1)$ of all instances. From an algorithmic point of view, or method is a direct adaptation of the Ducas-Gibbons LIP algorithm for Construction A lattices with trivial hulls. Given $O_1, O_2 \in O(n)$ and two lattices $\Lambda_1 = O_1\Lambda(C), \Lambda_2 = O_2\Lambda(C)$ for a linear code $C \subseteq \mathbb{F}_p^n$, it consists in isolating a basis of $O_1 \cdot p\mathbb{Z}^n$ and a basis of $O_2 \cdot p\mathbb{Z}^n$, and then to solve 2 LIP instances: one between $O_1 \cdot p\mathbb{Z}^n$ and $p\mathbb{Z}^n$ and another one between $O_2 \cdot p\mathbb{Z}^n$ and $p\mathbb{Z}^n$. Then the resolution of LIP between $\Lambda_1$ and $\Lambda_2$ reduces to an instance of the Signed Permutation Code Equivalence problem. When the hull of $C$ is trivial, the $p$-hull of $\Lambda_i$ is exactly $O_i \cdot p\mathbb{Z}^n$. Our main technical contribution is to prove that even when the hull is non-trivial, known lattice reduction techniques give us a basis of $O_i \cdot p\mathbb{Z}^n$ with high probability over the choice of the underlying code.

This paper is organized as follows: Section 2 contains the necessary background on Euclidean lattices and linear codes. Then we give a high-level description of the overall LIP procedure in Section 3. Section 4 contains statements on the expected number of vectors of a given length in the $p$-hull that are essential to the analysis of the algorithm. Then Section 5 shows how these bounds can be used to analyze the cost of sampling all vectors of length $p$ in the $p$-hull. Finally, Section 6 gives the overall cost of the LIP procedure.

## 2 Background

### 2.1 Euclidean lattices

**Definition 1 (Euclidean lattice).** *A (full-rank)* Euclidean lattice $\Lambda \subset \mathbb{R}^n$ *is a discrete additive subgroup of $\mathbb{R}^n$. Equivalently, there exists a basis $B =$*

$(\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$ *such that*

$$\Lambda = \{B\mathbf{z} : \mathbf{z} \in \mathbb{Z}^n\}.$$

*The integer $n$ is called the* rank *of $\Lambda$.*

Two bases generate the same lattice if and only if they differ by right multiplication by a matrix in $\mathrm{GL}_n(\mathbb{Z})$.

**Definition 2 (Dual lattice).** *The* dual lattice *of $\Lambda$ is defined as*

$$\Lambda^* \;=\; \{y \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in \Lambda\}.$$

The dual lattice is invariant under orthogonal transformations and plays a central role in the analysis of Gaussian measures over lattices.

**Definition 3 (Theta series).** *The* theta series *of a lattice $\Lambda$ is*

$$\Theta_\Lambda(q) \;=\; \sum_{\mathbf{x} \in \Lambda} q^{\|\mathbf{x}\|^2}.$$

*It is invariant under lattice isometries, though generally not complete (i.e. it does not identify isometry classes).*

**Definition 4 (Discrete Gaussian distribution).** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\sigma > 0$. The* discrete Gaussian distribution $D_{\Lambda,\sigma}$ *assigns probability the mass*

$$\Pr[\mathbf{x}] \;=\; \frac{e^{-\pi \|\mathbf{x}\|^2/\sigma^2}}{\sum_{\mathbf{y} \in \Lambda} e^{-\pi \|\mathbf{y}\|^2/\sigma^2}} \quad \text{for } \mathbf{x} \in \Lambda.$$

**Theorem 1 (ADRS Gaussian sampling [1, Thm. 1.1]).** *There exists a randomized algorithm that, given a basis of an $n$-dimensional lattice $\Lambda \subset \mathbb{R}^n$ and any parameter $\sigma > 0$, outputs $2^{n/2}$ independent and identically distributed samples from the discrete Gaussian distribution $D_{\Lambda,\sigma}$ using $2^{n+o(n)}$ time and space.*

This result, due to Aggarwal, Dadush, Regev, and Stephens-Davidowitz [1], enables *exact* discrete Gaussian sampling below the smoothing parameter and underlies several modern lattice algorithms.

**Definition 5 (Lattice Isomorphism Problem (LIP)).** *Given two Euclidean lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$, the* Lattice Isomorphism Problem *asks to determine whether there exists an orthogonal transformation $O \in O(n)$ such that*

$$\Lambda_2 = O(\Lambda_1),$$

*and, if so, to compute such a transformation.*

**Definition 6 (Matrix variant of LIP).** *Let $B_1, B_2 \in \mathbb{R}^{n\times n}$ be full-rank matrices. The* matrix lattice isomorphism problem *asks to determine whether there exists an orthogonal matrix $O \in O(n)$ such that*

$$B_2 = OB_1U$$

*for some unimodular matrix $U \in \mathrm{GL}_n(\mathbb{Z})$, and, if so, to compute such a pair $(O, U)$.*

*Remark 1.* The matrix lattice isomorphism problem is equivalent to the lattice isomorphism problem. Indeed, the matrices $B_1$ and $B_2$ define lattices $\Lambda_i = B_i\mathbb{Z}^n$, and the condition $B_2 = OB_1U$ is equivalent to $\Lambda_2 = O(\Lambda_1)$. The right multiplication by $U \in \mathrm{GL}_n(\mathbb{Z})$ accounts for the choice of basis of the lattice.

**Theorem 2 (Haviv–Regev [21]).** *The Lattice Isomorphism Problem for general $n$-dimensional Euclidean lattices can be solved in deterministic time $n^{O(n)}$.*

**Definition 7 ($\mathbb{Z}$-Lattice Isomorphism Problem ($\mathbb{Z}$-LIP)).** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice that is isometric to $\mathbb{Z}^n$, i.e., $\Lambda = O(\mathbb{Z}^n)$ for some unknown linear isometry $O \in O(n)$. The $\mathbb{Z}$-Lattice Isomorphism Problem ($\mathbb{Z}$-LIP) is the problem of recovering an orthogonal basis of $\Lambda$, equivalently of finding the rotation $O$ up to signed permutations of the coordinates.*

*Remark 2.* For a rotation $\Lambda$ of $\mathbb{Z}^n$, the set of shortest vectors of $\Lambda$ is exactly $\{\pm\mathbf{e}_i\}_{i=1}^n$, where $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ is an orthogonal basis of $\Lambda$. Consequently, solving Z-LIP is equivalent to recovering all shortest vectors of $\Lambda$.

**Theorem 3 (Bennett et al. [10]).** *$\mathbb{Z}$-LIP in dimension $n$ can be solved in time $2^{n/2+o(n)}$ by a polynomial-time reduction to $\gamma$-GapSVP in dimension $n$ with constant $\gamma > 1$.*

**Theorem 4 (Ducas [17]).** *$\mathbb{Z}$-LIP in dimension $n$ can be solved by a deterministic algorithm making polynomially many calls to an SVP oracle in dimension at most $n/2 + 1$.*

### 2.2 Linear codes

**Definition 8 (Linear code).** *Let $\mathbb{F}_q$ be a finite field. A* linear code *$C \subseteq \mathbb{F}_q^n$ is a linear subspace of dimension $k$, called an $[n, k, q]$-code. The* minimum distance *$d(C)$ is the minimum Hamming weight of a nonzero codeword of $C$.*

A code $C$ may be represented by a generator matrix $G \in \mathbb{F}_q^{k\times n}$ whose rows form a basis of $C$.

**Definition 9 (Dual code and hull).** *The* dual code *of $C$ is*

$$C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{y}\rangle = 0 \text{ for all } \mathbf{x} \in C\}.$$

*The* hull *of $C$ is*

$$\mathcal{H}(C) \;=\; C \cap C^\perp.$$

**Definition 10 (Code equivalence).** *Let $C_1, C_2 \subseteq \mathbb{F}_q^n$ be $[n, k, q]$ codes with generator matrices $G_1, G_2$.*

- *They are* permutation equivalent *if there exists a permutation matrix $P$ and an invertible matrix $S$ such that $G_2 = SG_1P$.*
- *They are* signed permutation equivalent *if $G_2 = SG_1PD$, where $S$ is invertible, $P$ is a permutation matrix and $D$ is diagonal entries in $\{\pm 1\}$.*
- *They are* linearly equivalent *if there exist $S$ invertible, a permutation matrix $P$, and a diagonal matrix $D$ such that $G_2 = SG_1PD$.*

The Linear Equivalence Problem (LEP) is precisely the problem of finding a *linear isometry for the Hamming metric* $\tau \in \mathcal{S}_n \ltimes \mathbb{F}_q^{*n}$ such that $\tau(C_1) = C_2$. The Permutation Equivalence Problem (PEP) is the problem of finding a permutation $\pi \in \mathcal{S}_n$ such that $\pi(C_1) = C_2$, and the Signed Permutation Equivalence Problem (SPEP) is the problem of retrieving a signed permutation $\tau \in \mathcal{S}_n \rtimes \{\pm 1\}$ such that $\tau(C_1) = C_2$.

The complexity of code equivalence depends strongly on the dimension of the hull. Sendrier's Support Splitting Algorithm (SSA [27]) is particularly effective when $\dim \mathcal{H}(C)$ is small, and recent work provides provable bounds and improved worst-case algorithms for several equivalence variants [7]: PEP and LEP can be solved in $2^{O(n)}$ arithmetic operations in $\mathbb{F}_q$, and using an analogue of the closure method that reduces LEP to PEP [28], Ducas and Gibbons [18, Sec. 5.2] showed that SPEP can also be solved in time $2^{O(n)}$.

### 2.3 Construction A lattices and $s$-hulls

**Definition 11 (Construction A).** *Let $C \subseteq \mathbb{F}_p^n$ be a linear code over a prime field. The associated* Construction A lattice *is*

$$\Lambda(C) \;=\; \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \bmod p \in C\}.$$

Construction A provides a direct bridge between coding-theoretic and lattice-theoretic structure.

**Definition 12 ($s$-hull of a lattice [18, Def. 12]).** *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $s \in \mathbb{Z}_{\geq 0}$. The* $s$-hull *of $\Lambda$ is the sublattice*

$$H_s(\Lambda) \;=\; \Lambda \cap s\Lambda^*,$$

*where $\Lambda^*$ denotes the dual lattice.*

The $s$-hull is invariant under lattice isometries and captures the structured part of $\Lambda$ visible at scale $s$.

**Lemma 1 (Ducas–Gibbons [18, Lem. 4]).** *Let $C \subseteq \mathbb{F}_p^n$ be a linear code and let $\Lambda(C)$ be its Construction A lattice. Then*

$$H_p(\Lambda(C)) \;=\; \Lambda(\mathcal{H}(C)),$$

*where $\mathcal{H}(C) = C \cap C^\perp$ denotes the hull of $C$.*

Lemma 1 shows that, for Construction A lattices, the $p$-hull operation commutes with Construction A and directly reflects the hull of the underlying code. This correspondence is the core structural observation enabling hull-based attacks on the lattice isomorphism problem and forms the starting point for extending such attacks beyond the trivial-hull regime.

For any $x \in \mathbb{F}_p$, where $p$ is odd, we denote its *lift*

$$\overline{x} \in \{0, \pm 1, \ldots, \pm(p-1)/2\}$$

to be the unique integer such that $\overline{x} = x \bmod p$, i.e., the "zero-centered" distinguished representative of $x$. For $p = 2$, we simply take $\overline{x} = x \bmod 2$.

**Definition 13 (Theta Function).** *For any prime $p$ and $a \in \mathbb{F}_p$, the* theta function *for $a$ is defined by*

$$\theta_a(q) := \sum_{z \in \mathbb{Z}} q^{(\overline{a}+pz)^2}.$$

*Note that this is equivalent to the theta series of a one-dimensional coset of a Construction A lattice.*

**Lemma 2 (Theta Series of Construction A Lattice).** *For any positive integer $n$, prime $p$, and linear code $\mathcal{C} \subseteq \mathbb{F}_p^n$, the theta series of the corresponding Construction A lattice $\mathcal{L} = \Lambda(\mathcal{C})$ can be written as*

$$\Theta_{\mathcal{L}}(q) = \sum_{(c_1,\ldots,c_n) \in \mathcal{C}} \prod_{i=1}^{n} \theta_{c_i}(q).$$

*Proof.* By definition 11, each lattice vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{L}$ can be written as $\mathbf{x} = \overline{\mathbf{c}} + p\mathbf{z}$ for some $\mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{C}$ and $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{Z}^n$, so that each coordinate has the form $x_i = \overline{c_i} + pz_i$. Then by definition 3 and some straightforward manipulation, we obtain

$$\begin{aligned}\Theta_{\mathcal{L}}(q) &= \sum_{\mathbf{x} \in \mathcal{L}} q^{\|\mathbf{x}\|^2} = \sum_{\mathbf{x} \in \mathcal{L}} \prod_{i=1}^{n} q^{x_i^2} = \sum_{\mathbf{c} \in \mathcal{C}} \sum_{\mathbf{z} \in \mathbb{Z}^n} \prod_{i=1}^{n} q^{(\overline{c_i}+pz_i)^2} \\ &= \sum_{\mathbf{c} \in \mathcal{C}} \prod_{i=1}^{n} \sum_{z_i \in \mathbb{Z}} q^{(\overline{c_i}+pz_i)^2} = \sum_{\mathbf{c} \in \mathcal{C}} \prod_{i=1}^{n} \theta_{c_i}(q).\end{aligned}$$

**Definition 14 (Gaussian Binomial Coefficient).** *For any non-negative integers $m$ and $k$, the* Gaussian binomial coefficient *is the polynomial in the indeterminate $q$ given by*

$$\binom{m}{k}_q := \prod_{i=0}^{k-1} \frac{(q^{m-i}-1)}{(q^{i+1}-1)} = \frac{(q^m-1)(q^{m-1}-1)\cdot\ldots\cdot(q^{m-k+1}-1)}{(q-1)(q^2-1)\cdot\ldots\cdot(q^k-1)}.$$

Note that for $k > m$, the expression evaluates to 0; for the case where $k = 0$, the expression evaluates to 1, as both the numerator and denominator are empty products.

We will be particularly interested in the case when $q$ set to be a prime power, as this expression gives the number of $k$-dimensional subspaces in the vector space $\mathbb{F}_q^m$ over the finite field $\mathbb{F}_q$.

## 3 High level description of the LIP algorithm

We describe a hull-based algorithm for the lattice isomorphism problem that follows the framework of [18, Section 5.1]. We work under the promise that the input lattices are of the form

$$\Lambda_i \;=\; O_i\big(C + p\mathbb{Z}^n\big) \subset \mathbb{R}^n, \qquad i = 1, 2,$$

where $C \subseteq \mathbb{F}_p^n$ is a fixed linear code and $O_1, O_2 \in O(n)$ are unknown orthogonal transformations. The goal is to find a linear isometry $\Lambda_1 \to \Lambda_2$.

**Theorem 5 (Correctness of Algorithm 1).** *Algorithm 1 returns either a linear isometry between the input lattices, or declares a failure.*

*Proof.* By Lemma 4 of [18], the $p$-hull of each lattice satisfies

$$H_p(\Lambda_i) \;=\; \Lambda_i \cap p\Lambda_i^* \;=\; O_i\big(\mathcal{H}(C) + p\mathbb{Z}^n\big),$$

where $\mathcal{H}(C) = C \cap C^\perp$ denotes the hull of the code. In particular, $H_p(\Lambda_i)$ contains the sublattice $O_i(p\mathbb{Z}^n)$, which is independent of the code hull component. We attempt to recover $O_i(p\mathbb{Z}^n)$ by using discrete Gaussian sampling on $H_p(\Lambda_i)$ with parameter $\sigma = cp/\sqrt{n}$. In particular, we hope that the lists $A_i$ contain the images of the $2n$ vectors $\pm p\mathbf{e}_j$ where the $\mathbf{e}_j$ are the canonical vectors of $\mathbb{Z}^n$. If $|A_i| < 2n$, we declare a failure. If $|A_i| > (2 + \delta)n$, we also declare a failure (only to simplify the analysis of the run-time). Each time we pick an $n$-tuple of elements of $A_i$, we work under the assumption that they generate the sublattice $O_i(p\mathbb{Z}^n) \subseteq H_p(\Lambda_i)$. Solving the resulting instance of $\mathbb{Z}$-LIP between $O_i(p\mathbb{Z}^n)$ and $p\mathbb{Z}^n$ yields an orthogonal transformation

$$O_i' = O_i \circ \sigma_i,$$

where $\sigma_i$ is a signed permutation, i.e., an automorphism of $p\mathbb{Z}^n$. Indeed, two isometries $O_i, O_i' : p\mathbb{Z}^n \to B_i\mathbb{Z}^n$ satisfy $O_i^{-1}O_i' \in \mathrm{Aut}(p\mathbb{Z}^n)$, which is the group of signed permutations.

Conjugating the input lattices by $O_i'^{-1}$ produces Construction A lattices of codes equivalent to $C$:

$$L_i \;=\; O_i'^{-1}\Lambda_i \;=\; \sigma_i^{-1}(C) + p\mathbb{Z}^n.$$

The original lattice isomorphism problem thus reduces to a Signed Permutation Equivalence Problem (SPEP) between the codes $C_1 = \sigma_1^{-1}(C)$ and $C_2 = \sigma_2^{-1}(C)$.

**Algorithm 1** LIP for Construction A lattices

**Require:** Two lattices $\Lambda_i = O_i(C + p\mathbb{Z}^n) \subset \mathbb{R}^n$, $i \in \{1, 2\}$. Constants $c, \delta, \varepsilon > 0$.
**Ensure:** An isometry $\varphi$ such that $\varphi(\Lambda_1) = \Lambda_2$, or failure

Set $\sigma \leftarrow cp/\sqrt{n}$
For $i = 1, 2$, compute the $p$-hull

$$H_p(\Lambda_i) = \Lambda_i \cap p\Lambda_i^*$$

Draw $2^{n/2}$ samples from $D_{H_p(\Lambda_i),\sigma}$.
For $i = 1, 2$, enumerate vectors of norm $p$ inside $H_p(\Lambda_i)$. Let $A_i$ be the corresponding lists.
**if** $|A_i| \notin [2n, (2+\delta)n]$ **then**
  **return** failure
**else**
  **for all** $n$-tuples $\mathcal{B}_1$ of $A_1$ and $n$-tuples $\mathcal{B}_2$ of $A_2$ **do**
    Let $B_i$ be a basis of the sublattice generated by these vectors.
    For $i = 1, 2$, solve $\mathbb{Z}$-LIP between $B_i$ and $p\mathbb{Z}^n$ to get an orthogonal matrix $O'_i$.
    Compute the Construction A lattice

$$L_i \leftarrow O_i'^{-1}\Lambda_i = \sigma_i^{-1}(C) + p\mathbb{Z}^n$$

    Reduce $L_1, L_2$ modulo $p$ to obtain codes $C_1 = \sigma_1^{-1}(C)$ and $C_2 = \sigma_2^{-1}(C)$
    Solve SPEP between $C_1$ and $C_2$.
    **if** SPEP has a solution $\sigma$ **then**

      **return** $\varphi = O'_2 \circ \sigma \circ O_1'^{-1}$
    **end if**
  **end for**
  **if** no solution to SPEP was found **then**
    **return** failure
  **end if**
**end if**

Solving this SPEP instance recovers the relative signed permutation $\sigma_2^{-1}\sigma_1$ up to an automorphism of $C_1$: $\sigma = \sigma_2^{-1}\sigma_1\sigma'$ with $\sigma'(C_1) = C_1$. With that we have

$$\begin{aligned} O'_2 \circ \sigma \circ O_1'^{-1}(\Lambda_1) &= O'_2 \circ \sigma_2^{-1}\sigma_1\sigma'(L_1) \\ &= O'_2 \circ \sigma_2^{-1}\sigma_1(L_1) \\ &= O'_2 \circ \sigma_2^{-1}\sigma_1 \circ O_1'^{-1}(\Lambda_1) \\ &= (O_2\sigma_2) \circ \sigma_2^{-1}\sigma_1 \circ (\sigma_1^{-1}O_1^{-1})(\Lambda_1) \\ &= O_2O_1^{-1}(\Lambda_1) = \Lambda_2. \end{aligned}$$

*Remark 3.* Algorithm 1 relies on the identification of $O_i(p\mathbb{Z}^n)$ for $i = 1, 2$. It is possible to collect length-$p$ vectors directly in $\Lambda_i$ instead of $H_p(\Lambda_i)$. However this impacts the performance both asymptotically and practically, since the dimension of $\mathcal{H}(C)$ is typically small. In the analysis of Algorithm 1, we rely on the fact that the expected length of the lists $A_i$ are close to $2n$. Working with

$H_p(\Lambda_i)$ instead of $\Lambda_i$ makes this estimate tighter, thus enlarging the range of parameters for which the success probability is $1 + o(1)$.

## 4 A bound on the average number of $p$-length vectors

In this section, we provide a bound on the expected number $N_p(C)$ of length $p$ vectors in $H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$. Our proof requires first to bound the probability that a given vector $\mathbf{u} \in \mathbb{F}_q^n$ belongs to $\mathcal{H}(C)$ where $C$ is drawn uniformly at random among the $k$-dimensional linear codes of $\mathbb{F}_q^n$. Then we use this to derive an upper bound on the expected value of the term in $p^2$ of the theta series $\Theta_{\Lambda(\mathcal{H}(C))}$ to obtain our estimate on the number of vectors of length $p$.

### 4.1 Probability of belonging to the Hull of a Random Linear Code

**Lemma 3.** *For any positive integers $q, n$, and $k < n$, let $C \subseteq \mathbb{F}_q^n$ be a linear code chosen uniformly at random from all $k$-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$ and let $\mathcal{H}(C) = C \cap C^\perp$ be its hull. Then, for a fixed nonzero vector $\mathbf{u} \in \mathbb{F}_q^n$,*

1. *If $\langle \mathbf{u}, \mathbf{u} \rangle \neq 0$, then $\Pr[\mathbf{u} \in \mathcal{H}(C)] = 0$.*
2. *If $\langle \mathbf{u}, \mathbf{u} \rangle = 0$, then*
$$\Pr[\mathbf{u} \in \mathcal{H}(C)] = \frac{\binom{n-2}{k-1}_q}{\binom{n}{k}_q},$$
*where the probability is over the random choice of $C$.*

*Proof.* First note that a vector $\mathbf{u}$ is in the hull $\mathcal{H}(C)$ if and only if $\mathbf{u} \in C$ and $\mathbf{u} \in C^\perp$. Since $C$ is a linear code, $\mathbf{u} \in C$ if and only if its span $\langle \mathbf{u} \rangle := \{a \cdot \mathbf{u} : a \in \mathbb{F}_q\} \subseteq C$. By definition of the dual code, $\mathbf{u} \in C^\perp$ if and only if $\langle \mathbf{u}, \mathbf{c} \rangle = 0$ for all codewords $\mathbf{c} \in C$, which is equivalent to $C \subseteq \mathbf{u}^\perp := \{\mathbf{x} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{x} \rangle = 0\}$. Hence,
$$\mathbf{u} \in \mathcal{H}(C) \iff \langle \mathbf{u} \rangle \subseteq C \subseteq \mathbf{u}^\perp. \tag{1}$$
We consider each case for $\langle \mathbf{u}, \mathbf{u} \rangle$:

*Case 1:* $\langle \mathbf{u}, \mathbf{u} \rangle \neq 0$. If $\mathbf{u} \in \mathcal{H}(C)$, then by eq. (1), $\langle \mathbf{u}, \mathbf{c} \rangle = 0$ for all $\mathbf{c} \in C$. Since $\mathbf{u} \in C$, this implies that $\langle \mathbf{u}, \mathbf{u} \rangle = 0$, which contradicts the assumption. Thus, $\Pr[\mathbf{u} \in \mathcal{H}(C)] = 0$ in this case.

*Case 2:* $\langle \mathbf{u}, \mathbf{u} \rangle = 0$. We count the number of codes $C$ that satisfy $\langle \mathbf{u} \rangle \subseteq C \subseteq \mathbf{u}^\perp$ and call these *admissible codes*. Since $\mathbf{u}$ is a nonzero vector, the map $\mathbf{x} \mapsto \langle \mathbf{u}, \mathbf{x} \rangle$ is a nonzero linear functional on $\mathbb{F}_q^n$, so $\mathbf{u}^\perp$ has dimension $\dim(\mathbf{u}^\perp) = n - 1$. By the assumption that $\langle \mathbf{u}, \mathbf{u} \rangle = 0$, we have $\mathbf{u} \in \mathbf{u}^\perp$ and so the quotient $\mathbf{u}^\perp / \langle \mathbf{u} \rangle$ has dimension $\dim(\mathbf{u}^\perp / \langle \mathbf{u} \rangle) = \dim(\mathbf{u}^\perp) - 1 = n - 2$. Consider the map
$$\Phi : \{C : \langle \mathbf{u} \rangle \subseteq C \subseteq \mathbf{u}^\perp,\ \dim(C) = k\} \to \{C' \subseteq \mathbf{u}^\perp / \langle \mathbf{u} \rangle : \dim(C') = k - 1\}$$
defined by $\Phi(C) := C / \langle \mathbf{u} \rangle$. This map is a bijection. It is well defined, as for any $C$ in the domain, the quotient $\Phi(C) = C / \langle \mathbf{u} \rangle$ is a $(k-1)$-dimensional subspace

of $\mathbf{u}^\perp/\langle\mathbf{u}\rangle$. If $C_1 \neq C_2$ are in the domain, they admit bases $\{\mathbf{u}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}\}$ and $\{\mathbf{u}, \mathbf{y}_1, \ldots, \mathbf{y}_{k-1}\}$ respectively, with at least one index $i$ such that $\mathbf{y}_i \notin C_1$. This means that $\Phi(\mathbf{y}_i) \notin \operatorname{span}\{\Phi(\mathbf{x}_1), \ldots, \Phi(\mathbf{x}_{k-1})\} = \Phi(C_2)$, and hence $\Phi(C_1) \neq \Phi(C_2)$ meaning that $\Phi$ is injective. Conversely, any $(k-1)$-dimensional subspace $C' = \operatorname{span}\{\mathbf{x}'_1, \ldots, \mathbf{x}'_{k-1}\} \subseteq \mathbf{u}^\perp/\langle\mathbf{u}\rangle$ admits the preimage $\operatorname{span}\{\mathbf{u}, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}\}$ under the quotient map $\mathbf{u}^\perp \to \mathbf{u}^\perp/\langle\mathbf{u}\rangle$ where each $\mathbf{x}_i$ is an arbitrary lift of $\mathbf{x}'_i \in \mathbf{u}^\perp/\langle\mathbf{u}\rangle$ in $\mathbf{u}^\perp$. Hence, the number of admissible $C$ is the number of $(k-1)$-dimensional subspaces of an $(n-2)$-dimensional $\mathbb{F}_q$-space; this is given precisely by the Gaussian binomial coefficient $\binom{n-2}{k-1}_q$. Similarly, the number of $k$-dimensional subspaces of $\mathbb{F}_q^n$ is $\binom{n}{k}_q$. Therefore,

$$\Pr[\mathbf{u} \in \mathcal{H}(C)] = \frac{\left|\{C : \langle\mathbf{u}\rangle \subseteq C \subseteq \mathbf{u}^\perp,\ \dim(C) = k\}\right|}{\left|\{C \subseteq \mathbb{F}_q^n : \dim(C) = k\}\right|} = \frac{\binom{n-2}{k-1}_q}{\binom{n}{k}_q}.$$

This completes the proof.

**Lemma 4.** *For any positive integers $q$ and $k = k(n)$ with $k < n$, linear code $C \subseteq \mathbb{F}_q^n$ chosen uniformly at random from all $k$-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$, and nonzero vector $\mathbf{u} =\in \mathbb{F}_q^n$ with $\langle\mathbf{u}, \mathbf{u}\rangle = 0$,*

$$\Pr[\mathbf{u} \in \mathcal{H}(C)] = q^{-(n-1)} \cdot \frac{(1-q^{-k})(1-q^{-(n-k)})}{(1-q^{-n})(1-q^{-(n-1)})} \in q^{-(n-1)}\left(1 - 2q^{-1}, 1\right].$$

*Proof.* By lemma 3 and definition 14, rearranging the terms in the Gaussian binomial coefficients, and simplifying,

$$\begin{aligned}
\Pr[\mathbf{u} \in \mathcal{H}(C)] &= \left(\prod_{i=0}^{k-2} \frac{q^{n-2-i}-1}{q^{i+1}-1}\right)\left(\prod_{i=0}^{k-1} \frac{q^{i+1}-1}{q^{n-i}-1}\right) \\
&= \left(\prod_{i=0}^{k-2} \frac{q^{n-2-i}-1}{q^{n-i}-1}\right) \cdot \frac{q^k-1}{q^{n-k+1}-1} \\
&= \frac{(q^{n-k}-1)(q^k-1)}{(q^n-1)(q^{n-1}-1)} \\
&= q^{-(n-1)} \cdot \frac{(1-q^{-k})(1-q^{-(n-k)})}{(1-q^{-n})(1-q^{-(n-1)})} \\
&\in q^{-(n-1)} \cdot \left(1 - 2q^{-1}, 1\right],
\end{aligned}$$

where the inequalities follow from the hypotheses $1 \leq k \leq n-1$ and $q \geq 1$.

### 4.2 Expected value of the number of length $p$ vectors in $H_p(\Lambda(C))$

We are now ready to bound the expected number of lattice vectors in the $p$-hull of a Construction A lattice of a code drawn uniformly at random that have length $p$. To find this number, we determine the relevant coefficient of the expected

theta series of these lattices. In this section, we use the simplified notation $\mathcal{L} := H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$ where $C$ is drawn uniformly at random among the $k$-dimensional linear codes over $\mathbb{F}_p^n$. We also say that two series $\theta_1(q), \theta_2(q)$ satisfy $\theta_i(q) \leq \theta_2(q)$ if the inequality holds coefficient-wise, and we denote by $[q^\ell]\theta(q)$ the coefficient of order $\ell$ in $\theta(q)$.

**Lemma 5 (Expected Theta Series of $\mathcal{L}$).** *Let $p$ be a prime number. For any linear code $C \subseteq \mathbb{F}_p^n$ chosen uniformly at random from all $k$-dimensional subspaces of $\mathbb{F}_p^n$, the expected theta series of $\mathcal{L} := H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$ satisfies*

$$\mathbb{E}[\Theta_{\mathcal{L}}(q)] \leq \theta_0(q)^n + c_{n,k,p}p^{1-n}\left(\Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big)^n - \theta_0(q)^n\right),$$

*where $c_{n,k,p} = \frac{(1-p^{-k})(1-p^{-(n-k)})}{(1-p^{-n})(1-p^{-(n-1)})} \in \big(1-2p^{-1}, 1\big]$ and where the expectation is over the random choice of $C$. The inequality of series is to be understood coefficient-wise.*

*Proof.* We rewrite the theta series of $\mathcal{L}$ as a sum over all words in $\mathbb{F}_p^n$. For any vector $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_p^n$, define $F(\mathbf{u}) := \prod_{i=1}^n \theta_{u_i}(q)$. Then by lemma 2, the theta series of $\mathcal{L}$ can be written as

$$\Theta_{\mathcal{L}}(q) = \sum_{\mathbf{c}\in\mathcal{H}(C)}\prod_{i=1}^n \theta_{c_i}(q) = \sum_{\mathbf{u}\in\mathbb{F}_p^n} 1_{\{\mathbf{u}\in\mathcal{H}(C)\}}\cdot F(\mathbf{u}),$$

where $1_{\{\mathbf{u}\in\mathcal{H}(C)\}}$ denotes the indicator random variable of the event $\mathbf{u} \in \mathcal{H}(C)$. Taking the expectation of the above expression over the randomness of the code, by linearity of expectation we have

$$\mathbb{E}[\Theta_{\mathcal{L}}(q)] = \sum_{\mathbf{u}\in\mathbb{F}_p^n}\mathbb{E}[1_{\{\mathbf{u}\in\mathcal{H}(C)\}}]\cdot F(\mathbf{u}) = \sum_{\mathbf{u}\in\mathbb{F}_p^n}\Pr[\mathbf{u}\in\mathcal{H}(C)]\cdot F(\mathbf{u}). \tag{2}$$

The probability that a fixed nonzero vector $\mathbf{u} \in \mathbb{F}_p^n$ is in the hull $\mathcal{H}(C)$ of a the random linear code $C$ is $\Pr[\mathbf{u} \in \mathcal{H}(C)] = c_{n,k,p}p^{1-n}$ if $\langle \mathbf{u}, \mathbf{u}\rangle = 0$ for $\mathbf{u} \neq \mathbf{0}$, $\Pr[\mathbf{u} \in \mathcal{H}(C)] = 0$ if $\langle \mathbf{u}, \mathbf{u}\rangle \neq 0$ and $\Pr[\mathbf{0} \in C] = 1$. The sum over vectors in $\mathbb{F}_p^n$ in eq. (2) can be factorized coordinate-wise as

$$\sum_{\mathbf{u}\in\mathbb{F}_p^n} F(\mathbf{u}) = \sum_{u_1\in\mathbb{F}_p}\cdots\sum_{u_n\in\mathbb{F}_p}\prod_{i=1}^n\theta_{u_i}(q) = \prod_{i=1}^n\Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big) = \Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big)^n.$$

By these facts, eq. (2) implies the inequality coefficient-wise

$$\begin{aligned}\mathbb{E}[\Theta_{\mathcal{L}}(q)] &\leq F(\mathbf{0}) + c_{n,k,p}p^{1-n}\Big(\sum_{\mathbf{u}\in\mathbb{F}_p^n}F(\mathbf{u}) - F(\mathbf{0})\Big)\\ &= \theta_0(q)^n + c_{n,k,p}p^{1-n}\left(\Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big)^n - \theta_0(q)^n\right).\end{aligned}$$

**Lemma 6.** *Let $p$ be a prime number. For any integer $\ell \geq 0$ and any linear code $C \subseteq \mathbb{F}_p^n$ chosen uniformly at random from all $k$-dimensional subspaces of $\mathbb{F}_p^n$, the expected number of lattice vectors in $\mathcal{L} := H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$ of Euclidean norm $\ell$ satisfies*

$$\mathbb{E}[N_\ell(C)] \leq [q^{\ell^2}]\theta_0(q)^n + c_{n,k,p}p^{1-n}\left([q^{\ell^2}]\Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big)^n - [q^{\ell^2}]\theta_0(q)^n\right),$$

*where the expectation is over the random choice of $C$.*

*Proof.* By definition 3 and linearity of expectation, we have

$$\mathbb{E}[\Theta_{\mathcal{L}}(q)] = \sum_{\ell=0}^{\infty}\mathbb{E}[N_\ell(C)]\cdot q^{\ell^2}.$$

Equivalently, for each non-negative integer $\ell$, the coefficient of $q^\ell$ in the series above is

$$\mathbb{E}[N_\ell(C)] = [q^{\ell^2}]\mathbb{E}[\Theta_{\mathcal{L}}(q)].$$

The claimed identity then follows from substituting the expression from lemma 5 and summing over all the coefficients of $q^\ell$ in each series and partial sum term.

**Theorem 6 (Expected Number of Lattice Vectors of Length $p$).** *For any prime $p$ and any linear code $C \subseteq \mathbb{F}_p^n$ chosen uniformly at random from all $k$-dimensional subspaces of $\mathbb{F}_p^n$, the expected number of lattice vectors in $\mathcal{L} := H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$ of length $p$ is bounded as follows*

$$2n \leq \mathbb{E}[N_p(C)] \leq 2n + c_{n,k,p}p^{1-n}\big(2n(p-1)\big)^{p^2+1},$$

*where the expectation is over the random choice of $C$ and*

$$c_{n,k,p} = \frac{(1-p^{-k})(1-p^{-(n-k)})}{(1-p^{-n})(1-p^{-(n-1)})} \in \big(1-2p^{-1}, 1\big].$$

*Proof.* As $p\mathbb{Z}^n \subseteq H_p(\Lambda(C))$, we always have $N_p(C) \geq 2n$. To upper bound $\mathbb{E}[N_p(C)]$, we use the identity from lemma 6 for norm $\ell = p$, truncate each term in the expression, and then use a combinatorial argument to explicitly find the coefficient of $q^{p^2}$.

By lemma 6,

$$\mathbb{E}[N_p(C)] \leq [q^{p^2}]\theta_0(q)^n + c_{n,k,p}p^{1-n}\left([q^{p^2}]\Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big)^n - [q^{p^2}]\theta_0(q)^n\right). \quad (3)$$

Each series and partial sum in the equality above can be written as a sum of terms of degree at most $p^2$ and the remaining higher-degree terms.

By definition 13, the theta function for 0 can be written as

$$\begin{aligned}\theta_0(q) &= \cdots + q^{(-2p)^2} + q^{(-p)^2} + q^{0^2} + q^{p^2} + q^{(2p)^2} + \cdots \\ &= 1 + 2q^{p^2} + R_0(q), \end{aligned} \tag{4}$$

where $R_0(q) := 2\sum_{z=2}^{\infty} q^{(pz)^2}$ contains all terms of degree at least $4p^2$. Now we find the coefficient of $q^{p^2}$ in the product $\theta_0(q)^n = (1 + 2q^{p^2} + R_0(q))^n$. Observe that since $R_0(q)$ only contains terms of degree greater than $p^2$, it cannot contribute to the coefficient of $q^{p^2}$. Thus, the only way to obtain a degree-$p^2$ term in the product is by multiplying the term $2q^{p^2}$ from one of the $n$ factors with the term 1 from each of the other $n-1$ factors. Since there are $n$ possible ways to do this, we have

$$[q^{p^2}]\theta_0(q)^n = 2n. \tag{5}$$

By definition 13, for any nonzero $a \in \mathbb{F}_p$ with $1 \le \overline{a} \le \lceil (p-1)/2 \rceil$,

$$\begin{aligned}\theta_a(q) = \theta_{-a}(q) &= \cdots + q^{(2p-\overline{a})^2} + q^{(p-\overline{a})^2} + q^{\overline{a}^2} + q^{(p+\overline{a})^2} + q^{(2p+\overline{a})^2} + \cdots \\ &= q^{\overline{a}^2} + q^{(p-\overline{a})^2} + R_a(q), \end{aligned} \tag{6}$$

where $R_a(q) := \sum_{z \in \mathbb{Z}\setminus\{0,-1\}} q^{(\overline{a}+pz)^2}$ contains all terms of degree strictly greater than $p^2$. Let $B(q) := 1 + 2\sum_{j=1}^{(p-1)/2}(q^{j^2} + q^{(p-j)^2})$ for odd $p$ and $B(q) := 1 + 2q$ for $p = 2$. Then, by eqs. (4) and (6) and gathering small-degree terms in the truncated polynomial, we have the following identity modulo $q^{p^2+1}$ when $p$ is odd

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} \theta_a(q) &= \theta_0(q) + \sum_{a\in\mathbb{F}_p\setminus\{0\}} \theta_a(q) \\ &= 1 + 2q^{p^2} + R_0(q) + 2\sum_{j=1}^{(p-1)/2} \left(q^{j^2} + q^{(p-j)^2} + R_j(q)\right) \\ &\equiv 1 + 2q^{p^2} + 2\sum_{j=1}^{(p-1)/2} \left(q^{j^2} + q^{(p-j)^2}\right) \bmod q^{p^2+1} \\ &= B(q) + 2q^{p^2}. \end{aligned}$$

For $p = 2$ we similarly get

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} \theta_a(q) &= \theta_0(q) + \sum_{a\in\mathbb{F}_p\setminus\{0\}} \theta_a(q) \\ &= \theta_0(q) + \theta_1(q) \\ &= 1 + 2q^{p^2} + R_0(q) + 2q + R_1(q) \\ &\equiv B(q) + 2q^{p^2} \bmod q^{p^2+1}. \end{aligned}$$

Now we find the coefficient of $q^{p^2}$ in the product $(\sum_{a\in\mathbb{F}_p}\theta_a(q))^n$. Using the congruence above and expanding the product, and observing that the only degree-$p^2$ terms come from the first and second terms of the sum,

$$\begin{aligned}
[q^{p^2}]\Big(\sum_{a\in\mathbb{F}_p}\theta_a(q)\Big)^n &= [q^{p^2}]\big(B(q)+2q^{p^2}\big)^n \\
&= [q^{p^2}]\Big(B(q)^n + n\cdot B(q)^{n-1}\cdot 2q^{p^2} + \sum_{i=2}^{n}\binom{n}{i}\cdot B(q)^i\cdot(2q^{p^2})^{n-i}\Big) \\
&= [q^{p^2}]B(q)^n + 2n.
\end{aligned}$$

The coefficient $[q^{p^2}]B(q)^n$ admits the following combinatorial interpretation. Defining the set $S := \{j^2, (p-j)^2 : j \in \{1,\dots,(p-1)/2\}\}$ for odd $p$ and $S := \{1\}$ for $p = 2$, we can rewrite $B(q) = 1 + 2\sum_{s\in S} q^s$. Then expanding the product $B(q)^n$ amounts to choosing $n$ terms, where each term is either the constant term 1 or one of the monomials $2q^e$ with $e \in S$. Thus, a monomial of total degree $p^2$ corresponds to choosing

- an index set $I \subseteq \{1,\dots,n\}$ such that $|I| = t \le p^2$, and
- for each $i \in I$, choosing an exponent $s_i \in S$ such that $\sum_{i\in I} s_i = p^2$.

Since every $s \in S$ satisfies $s \ge 1$, any choice of $I$ must have size $|I| = t \le p^2$. Each such choice contributes a factor of $2^t$, reflecting the two sign choices associated with each nonzero residue class. For a fixed integer $t \ge 0$, there are $\binom{n}{t}$ possible index sets $I \subseteq \{1,\dots,n\}$ of size $|I| = t$. Then, for any $t$, the number of monomial choices is bounded by

$$m_t := \big|\{(I,(s_i)_{i\in I}) : |I| = t,\ s_i \in S,\ \sum_{i\in I} s_i = p^2\}\big| \le \binom{n}{t}\cdot|S|^t \le n^t\cdot(p-1)^t,$$

where the second inequality follows by definition of $S$ and a trivial bound on the binomial coefficient. Consequently, we obtain

$$\begin{aligned}
[q^{p^2}]B(q)^n &= \sum_{t=0}^{p^2} 2^t\cdot m_t \le \sum_{t=0}^{p^2}(2n(p-1))^t \\
&= \frac{\big(2n(p-1)\big)^{p^2+1}-1}{2n(p-1)-1} \le \big(2n(p-1)\big)^{p^2+1}. \qquad (7)
\end{aligned}$$

Therefore, by substituting eqs. (5) and (7) into eq. (3), we obtain

$$\begin{aligned}
\mathbb{E}[N_p(C)] &\le 2n + c_{n,k,p}p^{1-n}\Big([q^{p^2}]B(q)^n + 2n - 2n\Big) \\
&\le 2n + c_{n,k,p}p^{1-n}\big(2n(p-1)\big)^{p^2+1},
\end{aligned}$$

as claimed.

Theorem 6 shows that on average the expected number of vectors of length $p$ in $\Lambda(\mathcal{H}(C))$ is very close to $2n$, i.e. the images of $\pm p\mathbf{e}_i$ under the secret isometry where the $\mathbf{e}_i$ are the canonical basis vectors of $\mathbb{Z}^n$. This allows us to argue that in the regime where $\lim_{n\to\infty} p^{1-n}\big(2n(p-1)\big)^{p^2+1} = 0$, we know the images of the $\pm p\mathbf{e}_i$ with high probability. In particular, in Corollary 1 below, we specify this result for the case of $p$ a constant.

**Corollary 1 (Expected Number of Lattice Vectors of Length $p$).** *For any prime $p \in O(1)$ and any linear code $C \subseteq \mathbb{F}_p^n$ chosen uniformly at random from all $k$-dimensional subspaces of $\mathbb{F}_p^n$, the expected number of lattice vectors in $\mathcal{L} := H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$ of length $p$ satisfies*

$$2n \le \mathbb{E}[N_p(C)] \le 2n + p^{-n} \cdot O(n^{p^2+1}),$$

*where the expectation is over the random choice of $C$.*

*Proof.* By theorem 6 and since $p$ is fixed, as $n$ grows

$$\mathbb{E}[N_p(C)] \le 2n + c_{n,k,p} p^{1-n}\big(2n(p-1)\big)^{p^2+1} = 2n + p^{-n} \cdot O(n^{p^2+1}).$$

## 5 A sampling procedure to collect all vectors of length $p$

Let $p$ be a prime and let $C \le \mathbb{F}_p^n$ be a uniformly random $k$-dimensional code. Let $\Lambda = \Lambda(C) \subset \mathbb{Z}^n$ be the (unscaled) Construction A lattice and

$$S_p(C) := \{\mathbf{x} \in H_p(\Lambda) : \ \|\mathbf{x}\| = p\}, \qquad N_p(C) := |S_p(C)|.$$

In this section, we provide an upper bound on the number of independent samples $T(C)$ from $D_{H_p(\Lambda),\sigma}$ required to collect all of the $N_p(C)$ vectors of length $p$ in $H_p(\Lambda)$ for $\sigma = cp/\sqrt{n}$ for some constant $c > 0$. At its core, the argument relies on the coupon collector problem framework. The distribution $D_{H_p(\Lambda),\sigma}$ satisfies

$$\Pr_{\mathbf{x}\leftarrow D_{H_p(\Lambda),\sigma}}[\mathbf{x} = \mathbf{y}] = \frac{e^{-\pi\|\mathbf{y}\|^2/\sigma^2}}{\rho_\sigma(H_p(\Lambda))}, \qquad \rho_\sigma(H_p(\Lambda)) := \sum_{\mathbf{z}\in H_p(\Lambda)} e^{-\pi\|\mathbf{z}\|^2/\sigma^2}.$$

Hence the probability $p_C$ of sampling a vector of length $p$ satisfies

$$p_C \ := \Pr_{\mathbf{x}\leftarrow D_{H_p(\Lambda),\sigma}}[\|\mathbf{x}\| = p] = \frac{\rho_\sigma(S_p(C))}{\rho_\sigma(H_p(\Lambda))} = \frac{N_p(C)\, e^{-\pi p^2/\sigma^2}}{\rho_\sigma(H_p(\Lambda))}.$$

**Lemma 7.** *Given a code $C$, the conditional expectation of $T(C)$ satisfies*

$$\mathbb{E}[T(C)|C] \le (\ln(N_p(C)) + 1)\rho_\sigma(H_p(\Lambda))e^{\pi p^2/\sigma^2}$$

*Proof.* Conditioned on the event that we draw a vector of length $p$, the distribution on $S_p(C)$ is uniform (all vectors of $S_p(C)$ have the same Gaussian weight). Hence, by the standard coupon collector argument, the number of successful samples of a vector $\mathbf{x} \in S_p(C)$ required to collect all elements of $S_p(C)$ is on average $N_p(C)H_{N_p(C)}$ where

$$H_{N_p(C)} := \sum_{j=1}^{N_p(C)} \frac{1}{j} \leq \ln(N_p(C)) + 1.$$

Since the average number of samples required to draw $\mathbf{x} \in S_p(C)$ is $1/p_C$, the average total number of samples required to draw all elements of $S_p(C)$ satisfies

$$\mathbb{E}[T(C)|C] = \frac{N_p(C)H_{N_p(C)}}{p_C} \leq (\ln(N_p(C)) + 1)\rho_\sigma(H_p(\Lambda))e^{\pi p^2/\sigma^2}.$$

**Proposition 1.** *When the code $C$ is drawn uniformly at random over dimension $k$ linear codes over $\mathbb{F}_p^n$, the average number of samples $\mathbb{E}_C[T(C)]$ from $D_{H_p(\Lambda),\sigma}$ required to collect all vectors of $S_p(C)$ satisfies*

$$\mathbb{E}_C[T(C)] \leq e^{\pi p^2/\sigma^2} \left(\frac{1 + e^{-\pi/\sigma^2}}{1 - e^{-\pi/\sigma^2}}\right)^n (\ln(\mathbb{E}_C[N_p(C)]) + 1)\,.$$

*Proof.* The expected value of $T(C)$ satisfies

$$\mathbb{E}_C[T(C)] = \mathbb{E}_C[\mathbb{E}[T(C)|C]] \leq e^{\pi p^2/\sigma^2}\mathbb{E}_C[(\ln(N_p(C)) + 1)\rho_s(\Lambda)].$$

First, since $H_p(\Lambda) \subseteq \mathbb{Z}^n$ we have the (instance-independent) bound

$$\rho_\sigma(H_p(\Lambda)) \leq \rho_\sigma(\mathbb{Z}^n) = \left(\sum_{m\in\mathbb{Z}} e^{-\pi m^2/\sigma^2}\right)^n \leq \left(\frac{1 + e^{-\pi/\sigma^2}}{1 - e^{-\pi/\sigma^2}}\right)^n.$$

Additionally, by concavity of the logarithm function and Jensen's inequality, we have

$$\mathbb{E}_C[\ln(N_p(C)) + 1] \leq \ln(\mathbb{E}_C[N_p(C)] + 1).$$

Together, these inequalities show that

$$\mathbb{E}_C[(\ln(N_p(C)) + 1)\rho_\sigma(H_p(\Lambda))] \leq \left(\frac{1 + e^{-\pi/\sigma^2}}{1 - e^{-\pi/\sigma^2}}\right)^n (\ln(\mathbb{E}_C[N_p(C)]) + 1)\,.$$

**Corollary 2.** *Assume $C$ is drawn uniformly at random over $k$-dimensional linear codes over $\mathbb{F}_p^n$ for a prime number $p \in O(n^{1/2-\varepsilon})$ with $\varepsilon > 0$, and that $\mathbb{E}_C[N_p(C)] \in \mathrm{Poly}(n)$. The expected number of independent samples drawn from $D_{H_p(\Lambda),\sigma}$ for $\sigma = cp/\sqrt{n}$ where $c > 0$ to collect all vectors of $S_p(C)$ satisfies*

$$\mathbb{E}_C[T(C)] \in \tilde{O}\left(2^{\left(\log_2(e)\frac{\pi}{c^2}\right)n}\right)$$

*Proof.* Given the definition of $\sigma$, we have

$$e^{-\pi/\sigma^2} = e^{-\frac{\pi}{c^2}\frac{n}{p^2}} \leq e^{-\frac{\pi}{c^2 d}n^{2\varepsilon}}$$

for some constant $d > 0$. Hence $\lim_{n\to\infty}\left(\frac{1+e^{-\pi/\sigma^2}}{1-e^{-\pi/\sigma^2}}\right)^n = 1$ which means that $\left(\frac{1+e^{-\pi/\sigma^2}}{1-e^{-\pi/\sigma^2}}\right)^n$ is bounded by a global constant. Additionally, by assumption, $(\ln(\mathbb{E}_C[N_p(C)]) + 1) \in \tilde{O}(1)$, hence the result.

## 6 Overall cost of the LIP procedure

In this section, we use the expected values of the number of length $p$ vectors in $H_p(\Lambda(C))$ for a random code $C$ calculated in Section 4.2 and the average number of samples from $D_{H_p(\Lambda),\sigma}$ to obtain all vectors of length $p$ calculated in Section 5 to derive the success probability of the LIP algorithm described in Section 3.

**Proposition 2.** *Let $\varepsilon, \delta > 0$ be constants, and assume the prime field size satisfies $p < n^{1/2-\varepsilon}$. Then over a choice of linear code $\mathcal{C} \subseteq \mathbb{F}_p^n$ uniformly at random from all $k$-dimensional subspaces of $\mathbb{F}_p^n$, the probability that the number $N_p(C)$ of length $p$ vectors in $\mathcal{L} := H_p(\Lambda(C)) = \Lambda(\mathcal{H}(C))$ is larger than $2n + \delta n$ satisfies*

$$\Pr[N_p(C) > (2+\delta)n] = o(1).$$

*Proof.* Given $p < n^{1/2-\varepsilon}$, we first show that $\mathbb{E}_C[N_p(C)] = 2n + o(n)$ and we conclude using Markov's bound. We know from Theorem 6 that

$$2n \leq \mathbb{E}[N_p(C)] \leq 2n + p^{1-n}\big(2n(p-1)\big)^{p^2+1}$$

Let $\alpha = 1/2 - \varepsilon$, so that $p < n^\alpha$. The excess term satisfies

$$\begin{aligned} p^{1-n}\big(2n(p-1)\big)^{p^2+1} &\leq n^{\alpha(1-n)} n^{\left(1+\alpha+\frac{\log(2)}{\log(n)}\right)(n^{2\alpha}+1)} \\ &= n e^{\log(n)\left(-\alpha n + (1+\alpha+\frac{\log(2)}{\log(n)})n^{2\alpha} + 2\alpha + \frac{\log(2)}{\log(n)}\right)} \end{aligned}$$

Since $2\alpha < 1$, we have

$$\log(n)\left(-\alpha n + (1+\alpha+\frac{\log(2)}{\log(n)})n^{2\alpha} + 2\alpha + \frac{\log(2)}{\log(n)}\right) \sim -\alpha n \log(n),$$

and therefore

$$e^{\log(n)\left(-\alpha n + (1+\alpha+\frac{\log(2)}{\log(n)})n^{2\alpha} + 2\alpha + \frac{\log(2)}{\log(n)}\right)} = o(1).$$

Let $\Delta_p(C) := N_p(C) - 2n$. We have $\mathbb{E}_C[\Delta_p(C)] = \mathbb{E}_C[N_p(C)] - 2n = o(n)$. Since $N_p(C) \geq 2n$, $\Delta_p(C)$ is non-negative and we can apply Markov's inequality

$$\Pr[N_p(C) > (2+\delta)n] = \Pr[\Delta_p(C) > \delta n] \leq \frac{\mathbb{E}_C[\Delta_p(C)]}{\delta n} = \frac{o(n)}{n} = o(1).$$

Similarly, we use Markov's inequality to bound the probability that the number of samples $T(C)$ required to collect all vectors of length $p$ exceeds the number of samples $2^{n/2}$ we collect via the ADRS procedure.

**Proposition 3.** *Let $\varepsilon > 0$ and $c > \sqrt{2\log_2(e)\pi}$ be constants. Assume $C$ is drawn uniformly at random over the $k$-dimensional linear codes over $\mathbb{F}_p^n$ with $p < n^{1/2-\varepsilon}$ prime. Then the probability that the number $T(C)$ of independent samples from $D_{H_p(\Lambda(C)),\sigma}$ with $\sigma = cp/\sqrt{n}$ required to draw all length $p$ vectors of $H_p(\Lambda(C))$ satisfies*

$$\Pr[T(C) > 2^{n/2}] = o(1).$$

*Proof.* We show that the number of samples produced by ADRS exceed the expected number of required samples to obtain all vectors of length $p$ with overwhelming probability. With our choice of $c$, we have $\log_2(e)\frac{\pi}{c^2} < \frac{1}{2}$. Since $T(C)$ is a non negative random variable, we can apply Markov's inequality to obtain:

$$\Pr[T(C) > 2^{n/2}] \leq \frac{\mathbb{E}_C[T(C)]}{2^{n/2}} = o(1),$$

since in this regime, $\mathbb{E}_C[N_p(C)] = 2n + o(n) \in \mathrm{Poly}(n)$, and hence by Corollary 2, $\mathbb{E}_C[T(C)] \in \tilde{O}\left(2^{\left(\log_2(e)\frac{\pi}{c^2}\right)n}\right)$.

**Corollary 3 (Cost of Algorithm 1).** *Let $\varepsilon > 0$ and $c > \sqrt{2\log_2(e)\pi}$ be constants. Assume $C$ is drawn uniformly at random over the $k$-dimensional linear codes over $\mathbb{F}_p^n$ with $p < n^{1/2-\varepsilon}$ prime. Then the cost of Algorithm 1 is in $2^{O(n)}$, and its success probability is $1 + o(1)$.*

*Proof.* The cost of producing $2^{n/2}$ samples from $D_{H_p(\Lambda(C)),\sigma}$ with the ADRS procedure in each of the input lattices is in $2^{n+o(n)}$. From Proposition 3, all $N_p(C)$ length $p$ vectors of $H_p(\Lambda(C))$ are among the $2^{n/2}$ vectors selected. Then in time $2^{O(n)}$ we can identify all $N_p(C)$ vectors of length $p$. If that number is larger than $(2+\delta)n$, we declare a failure with probability $o(1)$. We sort through all $n$-uplets of length $p$ vectors in time $\binom{(2+\delta)n}{n} \in 2^{O(n)}$, and each time we have a pair of $n$-tuples of length-$p$ vectors in the input lattices, we attempt to solve the corresponding pair of instances of $\mathbb{Z}$-LIP in time $2^{O(n)}$, and in case of success, we solve the SPEP instance also in time $2^{O(n)}$, hence the bound on the overall cost of Algorithm 1.

Notably, the above bounds hold independently of $\dim(\mathcal{H}(C))$. When $p$ grows larger than the range specified in Corollary 3, the probability that $\mathcal{H}(C)$ is trivial is at least $1 - 1/p = 1 + o(1)$. In this regime, it suffices to invoke the original method of Ducas–Gibbons.

**Corollary 4.** *Assume $C$ is drawn uniformly at random over the $k$-dimensional linear codes over $\mathbb{F}_p^n$ where $p$ is prime. There is an algorithm that solves LIP between two lattices isometric to $\Lambda(C)$ in time $\mathrm{Poly}(\log(p)) \cdot 2^{O(n)}$, with success probability $1 + o(1)$.*

*Proof.* In the large $p$ regime, the cost of the $\mathbb{Z}$-LIP instances as well as of SPEP is $2^{O(n)}$ arithmetic operations of integers with size bounded by $O(\log(p))$, hence the additional $\mathrm{Poly}(\log(p))$ term in the complexity.

## 7 Conclusion

We have shown that there is a Monte Carlo algorithm for solving LIP between two input lattices that are isometric to $\Lambda(C)$ for some code $C \subseteq \mathbb{F}_p^n$ in time $2^{O(n)}$ with success probability $1 + o(1)$ over a random choice of $C$. A direct improvement would be to turn this method into a Las Vegas algorithm with average run time bounded by $2^{O(n)}$. The collection of all vectors of length $p$ already runs in average time $2^{O(n)}$, however it is unclear whether or not the same is true for the attempt to solve SPEP for all $n$-tuples of length $p$ vectors. Indeed, even if the probability of a high number of length $p$ vectors is small, the time required to go through all of them gets exponentially large, thus impacting the expected time. In our Monte Carlo algorithm, we simply declare a failure when more than $(2 + \delta)n$ vectors of length $p$ are found. One possible way to overcome this hurdle would be to account for the low likelihood that $n$-tuples of length $p$ vectors are all orthogonal. This necessary property of the image of the vectors $\pm p\mathbf{e}_j$ is not exploited in our algorithm. If such analysis was successfully carried, it would likely reduce the probability that $n$-tuples of length $p$ vectors other than the images of $\pm p\mathbf{e}_j$ are tested.

A more ambitious line of future work would be to design an algorithm that works on all (rotations of) Construction A lattices as opposed to random instances. If such a solution exist, it would likely require substantial new ideas since the properties of the lattices that enable the run time of our algorithm to be bounded by $2^{O(n)}$ are instrinsic to the geometry of the instances (number of vectors of a given length).

## References


1. Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in $2^n$ time using discrete gaussian sampling. *Journal of the ACM*, 64(2):1–42, 2017.
2. Bill Allombert, Alice Pellet-Mary, and Wessel P. J. van Woerden. Cryptanalysis of rank-2 module-lip: A single real embedding is all it takes. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 184–212. Springer, 2025.
3. László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. Code equivalence and group isomorphism. In Dana Randall, editor, *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pages 1395–1408. SIAM, 2011.

4. Marco Baldi, Alessandro Barenghi, Luke Beckwith, Jean-François Biasse, Andre Esser, Kris Gaj, Kamyar Mohajerani, Gerardo Pelosi, Edoardo Persichetti, Markku-Juhani O. Saarinen, Paolo Santini, and Robert Wallace. Less, 2023. Additional Digital Signature Schemes - Round 1 Submissions.
5. Alessandro Barenghi, Jean-François Biasse, Tran Ngo, Edoardo Persichetti, and Paolo Santini. Advanced signature functionalities from the code equivalence problem. *Int. J. Comput. Math. Comput. Syst. Theory*, 7(2):112–128, 2022.
6. Alessandro Barenghi, Jean-François Biasse, Edoardo Persichetti, and Paolo Santini. LESS-FM: fine-tuning signatures from the code equivalence problem. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings*, volume 12841 of *Lecture Notes in Computer Science*, pages 23–43. Springer, 2021.
7. Huck Bennett, Drisana Bhatia, Jean-François Biasse, Medha Durisheti, Lucas LaBuff, Vincenzo Pallozzi Lavorante, and Phillip Waitkevich. Asymptotic improvements to provable algorithms for the code equivalence problem. In *IEEE International Symposium on Information Theory, ISIT 2025, Ann Arbor, MI, USA, June 22-27, 2025*, pages 1–6. IEEE, 2025.
8. Huck Bennett, Drisana Bhatia, Jean-François Biasse, Medha Durisheti, Lucas LaBuff, Vincenzo Pallozzi Lavorante, and Philip Waitkevich. Asymptotic improvements to provable algorithms for the code equivalence problem. *IEEE Transactions on Information Theory*, 72(2):1093–1108, 2026.
9. Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 252–281. Springer, 2023.
10. Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice. In *EUROCRYPT*, 2023.
11. Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. LESS is more: Code-based signatures without syndromes. In Abderrahmane Nitaj and Amr M. Youssef, editors, *Progress in Cryptology - AFRICACRYPT 2020 - 12th International Conference on Cryptology in Africa, Cairo, Egypt, July 20-22, 2020, Proceedings*, volume 12174 of *Lecture Notes in Computer Science*, pages 45–65. Springer, 2020.
12. Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902. SIAM, 2016.
13. Joppe W. Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W. Postlethwaite, Thomas Prest, Ludo N. Pulles, and Wessel van Woerden. Hawk, 2023. Additional Digital Signature Schemes - Round 1 Submissions.
14. Clémence Chevignard, Guilhem Mureau, Thomas Espitau, Alice Pellet-Mary, Heorhii Pliatsok, and Alexandre Wallet. A reduction from hawk to the principal ideal problem in a quaternion algebra. In Serge Fehr and Pierre-Alain Fouque, editors,

*Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 154–183. Springer, 2025.

15. Clémence Chevignard and Guilhem Mureau. Ideally HAWKward: How not to break module-LIP. Cryptology ePrint Archive, Paper 2025/1095, 2025.
16. Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Lars Ran, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Meds, 2023. Additional Digital Signature Schemes - Round 1 Submissions.
17. Léo Ducas. Provable lattice reduction of $\mathbb {Z}ˆn$ with blocksize n/2. *Des. Codes Cryptogr.*, 92(4):909–916, 2024.
18. Léo Ducas and Shane Gibbons. Hull attacks on the lattice isomorphism problem. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I*, volume 13940 of *Lecture Notes in Computer Science*, pages 177–204. Springer, 2023.
19. Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 65–94. Springer, 2022.
20. Léo Ducas and Wessel P. J. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 643–673. Springer, 2022.
21. Ishay Haviv and Oded Regev. On the lattice isomorphism problem. *Theory of Computing*, 8(15):389–418, 2012.
22. Cong Ling, Jingbo Liu, and Andrew Mendelsohn. On the spinor genus and the distinguishing lattice isomorphism problem. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IV*, volume 15487 of *Lecture Notes in Computer Science*, pages 329–358. Springer, 2024.
23. Cong Ling, Andrew Mendelsohn, and Christian Porter. Number field algorithms for quaternion ideal-svp. *IACR Cryptol. ePrint Arch.*, page 1448, 2025.
24. Guilhem Mureau. Special genera of hermitian lattices and applications to HAWK. In Benny Applebaum and Huijia (Rachel) Lin, editors, *Theory of Cryptography - 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1-5, 2025, Proceedings, Part IV*, volume 16271 of *Lecture Notes in Computer Science*, pages 289–317. Springer, 2025.
25. Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet. Cryptanalysis of rank-2 module-lip in totally real number fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic*

*Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*, volume 14656 of *Lecture Notes in Computer Science*, pages 226–255. Springer, 2024.
26. Nicolas Sendrier. On the dimension of the hull. *SIAM Journal on Discrete Mathematics*, 10(2):282–293, 1997.
27. Nicolas Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. *IEEE Trans. Inf. Theory*, 46(4):1193–1203, 2000.
28. Nicolas Sendrier and Dimitris E. Simos. The hardness of code equivalence over and its application to code-based cryptography. In Philippe Gaborit, editor, *Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings*, volume 7932 of *Lecture Notes in Computer Science*, pages 203–216. Springer, 2013.
29. Franciele C. Silva, Maja Lie, and Cong Ling. On hull attacks on the module lattice isomorphism problem. Cryptology ePrint Archive, Paper 2025/1376, 2025.