STRUCTURED LATTICES AND THEIR APPLICATIONS TO SECURITY

LENNY FUKSHANSKY, CAMILLA HOLLANTI, AND RAHINATOU Y. NJAH NCHIWO

Abstract. Euclidean lattices are an interesting object of study in many regards and can have a rich structure arising from various constructions, e.g., from number field extensions. A particularly interesting class is the one of well-rounded lattices, as they relate to the well-known densest sphere packing problem in geometry, theta function minimization, and the famous Minkowski and Woods conjectures. In addition to being an important mathematical object in their own right, lattices also play a central role in many applications. This paper offers a survey of structured lattices and discusses their recent applications in lattice-based cryptography and secure wireless communications. Our goal is to spark the interest of the mathematics and adjacent communities in these fascinating topics in the intersection of lattices, number theory, cryptography, and wireless communications.

Contents

2020 *Mathematics Subject Classification.* Primary: 11Hxx, 11E12, 11T71; Secondary: 94A60, 94Bxx.

Key words and phrases. algebraic number fields, flatness factor, function fields, information-theoretic security, lattices, lattice-based cryptography, learning with errors, physical layer security, secrecy gain, smoothing parameter, theta functions, well-rounded lattices.

This work was supported in part by the Finnish Research Council (Grant #351271) and in part by the Business Finland Co-Innovation Consortium (Grant #5845483). R. Y. Njah Nchiwo was supported by the Magnus Ehrnrooth Foundation and the Finnish Academy of Science and Letters, Finland.

1. Lattices

1.1. **Introduction to lattice theory.** The theory of Euclidean lattices has its origins in the work of Lagrange and Gauss, who studied lattices in the context of Kepler's sphere packing conjecture and the arithmetic of quadratic forms. Major advances in the theory came with Minkowski's development of geometry of numbers and further connections to number theory, convex and discrete geometry, algebraic geometry, optimization, geometric combinatorics and many other fields of mathematics. Today, lattice theory enjoys a central place within mathematics and its applications. Some of the major breakthroughs of the recent decades included T. Hales's & S. Ferguson's proof of Kepler's conjecture [107], O. Musin's proof of the kissing number conjecture in dimension 4 [138], and M. Viazovska et al. proof of the optimal sphere packing conjecture in dimensions 8 and 24, [183] and [54]. The goal of this survey paper is to give an overview of theory of Euclidean lattices and some of its recent developments with a view towards applications in coding theory and cryptography. We will especially focus on properties and constructions of important classes of lattices with additional structure (*e.g.*, well-rounded, eutactic, perfect), which play a central role in optimization problems and applications. For comprehensive sources on the theory of Euclidean lattices, we refer the reader to the classical books by Conway & Sloane [57], Gruber & Lekkerkerker [106], and Martinet [127]. The first two authors of this paper have recently edited a special collection of research articles on "Euclidean lattices: theory and applications" (Communications in Mathematics, vol 31, no 2, 2023) which is surveyed in [90].

Throughout this paper we view $\mathbb{R}^n$ as a Euclidean space with respect to the usual Euclidean inner-product $\langle\ ,\ \rangle$ and the corresponding Euclidean norm $\|\boldsymbol{x}\| := \sqrt{\langle \boldsymbol{x}, \boldsymbol{x}\rangle}$ for every $\boldsymbol{x} \in \mathbb{R}^n$. A *lattice* $L \subset \mathbb{R}^n$ of *rank* $r \leq n$ (denoted $\mathrm{rk}(L) = r$) is a discrete subgroup of $\mathbb{R}^n$ which is co-compact in the r-dimensional subspace $V(L) := \mathrm{span}_{\mathbb{R}} L$. This is equivalent to saying that there exists a collection of $\mathbb{R}$-linearly independent vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r \in L$ such that

$$L = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r\} = \left\{ \sum_{i=1}^{r} c_i \boldsymbol{a}_i : c_1, \ldots, c_r \in \mathbb{Z} \right\}.$$

The collection $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ is a basis for L and we refer to the $n \times r$ matrix $A = (\boldsymbol{a}_1 \ldots \boldsymbol{a}_r)$ as a *basis matrix* for L, *i.e.*, $L = A\mathbb{Z}^r$. For any $U \in \mathrm{GL}_r(\mathbb{Z})$, AU is another basis matrix for L. The subspace $V(L) \subseteq \mathbb{R}^n$ can be identified with $\mathbb{R}^r$, so from here on we will talk about lattices of *full rank* in $\mathbb{R}^n$, meaning that $r = n$. The space $\mathcal{L}_n$ of full-rank lattices in $\mathbb{R}^n$ can be identified with $\mathrm{GL}_n(\mathbb{R})\backslash \mathrm{GL}_n(\mathbb{Z})$, the set of orbits of $\mathrm{GL}_n(\mathbb{R})$ under the action of $\mathrm{GL}_n(\mathbb{Z})$ by right multiplication.

Two lattices $L_1, L_2 \subset \mathbb{R}^n$ are said to be *similar*, denoted $L_1 \sim L_2$, if there exists $\alpha \in \mathbb{R}^+$, the group of positive real numbers, and $U \in \mathcal{O}_n(\mathbb{R})$, the $n \times n$ real orthogonal group, such that $L_2 = \alpha U L_1$. This is an equivalence relation, and the space $\mathcal{S}_n$ of similarity classes is $(\mathbb{R}^+ \times \mathcal{O}_n(\mathbb{R}))/\mathcal{L}_n$, the set of orbits of the space of full-rank lattices under the action of the group $\mathbb{R}^+ \times \mathcal{O}_n(\mathbb{R})$ by left multiplication. A lattice L is called *integral* if for every $\boldsymbol{x}, \boldsymbol{y} \in L$, $\langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \mathbb{Z}$ and a lattice is called *arithmetic* if it is similar to an integral lattice.

The group of isometries of a full-rank lattice $L \subset \mathbb{R}^n$ is $\mathcal{O}(L) := \{U \in \mathcal{O}_n(\mathbb{R}) : UL = L\}$, which is compact as a subset of $\mathrm{GL}_n(\mathbb{R})$ with respect to the Euclidean metric topology. The automorphisms of L are isometries given by integer linear transformations, so the *automorphism group* of L is $\mathrm{Aut}(L) := \mathrm{GL}_n(\mathbb{R}) \cap \mathcal{O}(L)$.

Since $\mathrm{Aut}(L)$ is the intersection of a discrete subgroup with a compact set, it is finite. In fact, in all but seven exceptional dimensions the lattice with the largest (with respect to size) automorphism group is $\mathbb{Z}^n$, which is the signed permutation group consisting of $2^n n!$ elements: it is generated by independent coordinate sign changes and permutations. When $n = 2, 4, 6, 7, 8, 9, 10$ more symmetric lattices with even larger automorphism groups exist. For example, $|\mathrm{Aut}(\mathbb{Z}^2)| = 8$ whereas the hexagonal lattice

$$\Lambda_h = \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix} \mathbb{Z}^2$$

has 12 automorphisms. This being said, most lattices have just two automorphisms: multiplication by ± 1. The automorphism group is an invariant of the similarity class of a lattice.

The *determinant* (also called *co-volume*) of a lattice $L = A\mathbb{Z}^n$ is defined as $\det(L) := \sqrt{\det(A^\top A)}$ and is equal to the volume the quotient group $\mathbb{R}^n/L$. This is an invariant of L which does not depend on the choice of a basis matrix A. In other words, $\det(L)$ is the volume of any *fundamental domain*, *i.e.* a measurable full set of coset representatives of L in $\mathbb{R}^n$. One example of a fundamental domain is a fundamental parallelotope $\{c_1\boldsymbol{a}_1 + \cdots + c_n\boldsymbol{a}_n : 0 \le c_i < 1 \ \forall\ 1 \le i \le n\}$, corresponding to the basis matrix $A = (\boldsymbol{a}_1 \dots \boldsymbol{a}_n)$. Another object more intrinsically dependent on L is its *Voronoi cell*

$$\mathcal{V}(L) := \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\| \le \|\boldsymbol{x} - \boldsymbol{y}\| \ \forall\ \boldsymbol{y} \in L\}.$$

While $\mathcal{V}(L)$ is not a fundamental domain of L, it is the closure of a fundamental domain, and hence its volume is still equal to $\det(L)$. Now, $\mathbb{R}^n = \bigcup_{\boldsymbol{x}\in L}(\boldsymbol{x} + \mathcal{V}(L))$, where two distinct translates $\boldsymbol{x}_1 + \mathcal{V}(L)$ and $\boldsymbol{x}_2 + \mathcal{V}(L)$ can intersect only at the boundary. A lattice L is called *unimodular* if $\det(L) = 1$.

For a given full-rank lattice $L = A\mathbb{Z}^n \subset \mathbb{R}^n$, its *dual lattice* is defined to be

$$L^* := \{\boldsymbol{x} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{y}\rangle \in \mathbb{Z} \ \forall\ \boldsymbol{y} \in L\} = (A^{-1})^\top \mathbb{Z}^n,$$

then $\det(L^*) = 1/\det(L)$. If L is integral then $L \subseteq L^*$, hence unimodular integral lattices are *self-dual*, *i.e.*, $L = L^*$.

We also define the *successive minima* $0 < \lambda_1(L) \le \cdots \le \lambda_n(L)$ of a full-rank lattice L in $\mathbb{R}^n$ to be

$$\lambda_i(L) := \min\left\{t \in \mathbb{R}^+ : \dim_{\mathbb{R}}\left(\mathrm{span}_{\mathbb{R}}(L \cap \mathbb{B}_n(t)\right) \ge i\right\},$$

where $\mathbb{B}_n(t)$ is a ball of radius t centered at the origin in $\mathbb{R}^n$. In particular, the first successive minimum is the norm of a shortest nonzero vector in L. Additionally, the *covering radius* (also called the *inhomogeneous minimum*) of L is defined as

$$\mu(L) := \min\left\{t \in \mathbb{R}^+ : L + \mathbb{B}_n(t) = \mathbb{R}^n\right\}.$$

The celebrated Minkowski's Successive Minima Theorem (see, *e.g.*, Chapter 2, § 9 of [106]) gives bounds on the product of successive minima of L:

$$\frac{2^n \det(L)}{n!\omega_n} \le \prod_{i=1}^{n} \lambda_i(L) \le \frac{2^n \det(L)}{\omega_n}, \tag{1}$$

where ω_n is the volume of a unit ball in $\mathbb{R}^n$. An immediate implication of (1) is Minkowski Convex Body Theorem (see, *e.g.*, Chapter 2, § 5 of [106]):

$$\lambda_1(L) \le 2\left(\frac{\det(L)}{\omega_n}\right)^{1/n}. \tag{2}$$

We define the set of *minimal vectors* of L to be $S(L) := \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = \lambda_1(L)\}$.

The *sphere packing* associated to L is constructed by inscribing a ball of radius $\lambda_1(L)/2$ into each translate of the Voronoi cell $\mathcal{V}(L)$. The *density* of this packing is the proportion of the space occupied by the spheres, which is the same as ratio of the volume of the ball and volume of the Voronoi cell into which it is inscribed; it can be computed as

$$\delta(L) := \frac{\omega_n \lambda_1(L)^n}{2^n \det(L)} \leq 1.$$

This is a continuous function on the space of lattices $\mathcal{L}_n$ which is constant on any given similarity class, hence we can think of it as a continuous function of the space $\mathcal{S}_n$ of similarity classes. The objective of the *lattice packing problem* in a given dimension is to find a lattice that maximizes $\delta(L)$. Solutions to the lattice packing problem are only known in dimensions $1 \leq n \leq 9$ (with $n = 9$ case being very recent still unpublished work by Dutour Sikirić and van Woerden) and $n = 24$ (see Chapter 1 of [57]). The celebrated Minkowski-Hlawka theorem (see, *e.g.*, Chapter 1 of [57]) asserts that in every dimension $n \geq 2$ there exists a full-rank lattice $L \subset \mathbb{R}^n$ such that

$$\delta(L) \geq \frac{\zeta(n)}{2^{n-1}},$$

where $\zeta(n)$ the value of the Riemann zeta-function at n. The proof of this theorem, however, is not constructive, and in all but finitely many dimensions (up to 1000 or so) no constructions of lattices satisfying the Minkowski-Hlawka bound are known. This being said, the lower bound $\zeta(n)/2^{n-1}$ in the Minkowski-Hlawka theorem can be improved. The most significant improvement is due to B. Klartag [113], who established (also non-constructively) the lower bound $cn^2/2^n$ for some universal constant $c > 0$ in 2025. Notice that maximizing lattice packing density in dimension $n \geq 2$ is equivalent to determining the value of the Hermite's constant

$$\gamma_n := \max_{L \subset \mathbb{R}^n} \frac{\lambda_1(L)}{\det(L)^{1/n}}.$$

While the value of γ_n is only known in the few dimensions mentioned above, an upper bound on it follows, for instance, from Minkowski's theorem (2).

A linearly independent collection of vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in L$ is said to *correspond to successive minima* if $\|\boldsymbol{a}_i\| = \lambda_i$ for each $1 \leq i \leq n$. Finding the successive minima is equivalent to the *shortest independent vector problem* mentioned in Section 2, which is known to be NP-hard. Such a collection is not unique, but there are only finitely many of them in a given lattice. These vectors are known to form a basis for L in dimensions $n \leq 3$, however in dimensions $n \geq 4$ they do not necessarily form a basis. Consider, for example the lattice

$$L_1 = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \frac{1}{2} \sum_{i=1}^{4} \boldsymbol{e}_i \right\} \subset \mathbb{R}^4,$$

where $\boldsymbol{e}_i$ are the standard basis vectors. Then

$$\left\{ \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \frac{1}{2} \sum_{i=1}^{4} \boldsymbol{e}_i \right\} \text{ and } \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4\}$$

are both collections of vectors in L_1 corresponding to successive minima, however the first one forms a basis whereas the second does not. Similarly, the lattice

$$L_2 = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4, \frac{1}{2}\sum_{i=1}^{5} \boldsymbol{e}_i \right\} \subset \mathbb{R}^5 \tag{3}$$

does not have a collection of vectors corresponding to successive minima that would form a basis. These observations raise a natural question: what is the shortest basis in L? Hermite inequality (see, *e.g.* Theorem 2.2.1 of [127]) guarantees that a lattice L of rank n has a basis $\boldsymbol{a}_1, \dots, \boldsymbol{a}_n$ such that $\lambda_1(L) = \|\boldsymbol{a}_1\| \leq |\boldsymbol{a}_2\| \leq \cdots \leq \|\boldsymbol{a}_n\|$ and

$$\prod_{i=1}^{n} \|\boldsymbol{a}_i\| \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} \det(L). \tag{4}$$

On the other hand, Hadamard inequality (see, *e.g.* Theorem 2.1.1 of [127]) states that the *orthogonality defect* of this basis is

$$\nu(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n) := \frac{\prod_{i=1}^{n} \|\boldsymbol{a}_i\|}{\det(L)} \geq 1. \tag{5}$$

Indeed, this basis is orthogonal if and only if $\nu(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n) = 1$ and

$$\frac{\lambda_1(L)^n}{\det(L)} \leq \nu(\boldsymbol{a}_1, \dots, \boldsymbol{a}_n) \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}},$$

implying that maximizing $\frac{\lambda_1(L)^n}{\det(L)}$ to achieve γ_n^n entails maximizing the orthogonality defect.

We also want to mention two related optimization problems on lattices: the *lattice covering problem* and the *kissing number problem*. The covering configuration associated to the lattice L is constructed by circumscribing a sphere of radius $\mu(L)$ around each translate of the Voronoi cell, and the *thickness* of this covering is the ratio of the volume of the ball and volume of the Voronoi cell around which it is circumscribed; it can be computed as

$$\mathfrak{f}(L) := \frac{\omega_n \mu(L)^n}{\det(L)} \geq 1.$$

Again, this is a continuous function of the space $\mathcal{S}_n$ of similarity classes of lattices. The objective of the *lattice covering problem* in a given dimension is to find a lattice that minimizes $\mathfrak{f}(L)$. Solutions to the lattice covering problem are only known in dimensions $1 \leq n \leq 5$ (see Chapter 1 of [57]). Finally, the kissing number problem on lattices asks for the maximal number of spheres centered at points of a lattice L in $\mathbb{R}^n$ that can touch the sphere centered at $\mathbf{0}$. This is equivalent to asking for a lattice with maximal number of minimal vectors in a given dimension, *i.e.*, the kissing number of L is $|S(L)|$. The answer is known in dimensions $1 \leq n \leq 9$ and $n = 24$ (see Chapter 1 of [57]).

1.2. **Well-rounded and related classes.** A lattice $L \subset \mathbb{R}^n$ is called *well-rounded* (abbreviated WR) if $\lambda_1(L) = \cdots = \lambda_n(L)$, which is equivalent to saying that

$$\mathbb{R}^n = \operatorname{span}_{\mathbb{R}} S(L). \tag{6}$$

It is important to remark that WR condition (6) is not equivalent to the condition $L = \operatorname{span}_{\mathbb{Z}} S(L)$, as demonstrated by the example L_2 in (3) above: this second condition is strictly stronger than (6) for $n \geq 5$; if it holds, we say that L is *generated by minimal vectors* (for $n \leq 4$, all WR lattices are generated by their minimal vectors). Further, for all $n \geq 10$ it is possible for a lattice L to be generated by minimal vectors while not containing a basis of minimal vectors: this was first demonstrated for $n \geq 11$ by Conway and Sloane [56] and then extended to $n \geq 10$ by Martinet and Schürmann [130]. On the other hand, for all $n \leq 9$ lattices generated by minimal vectors contain a basis of minimal vectors (see [128], [129], [130]).

WR property is preserved under similarity, hence we can speak of WR similarity classes, of which there are infinitely many in each dimension $n \geq 2$. WR lattices appear in many different contexts in number theory, geometry, combinatorics and optimization. In particular, the space of WR lattices forms a "spine" ($\mathrm{SL}_n(\mathbb{Z})$-equivariant deformation retract) for the space of all lattices in $\mathbb{R}^n$, which is useful for cohomology computations [9], [155], [110]. Further, WR lattices appear prominently in regard to Minkowski conjecture [131]. Let L be a unimodular lattice. For each $\boldsymbol{x} \in L$, define the multiplicative norm $N(\boldsymbol{x}) = |x_1 \cdots x_n|$. Notice that N is preserved under the left-multiplication action by the diagonal group

$$\mathcal{A}_n := \left\{ \begin{pmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \end{pmatrix} : a_i > 0, \prod_{i=1}^{n} a_i = 1 \right\},$$

in other words, $N(\boldsymbol{x}) = N(A\boldsymbol{x})$ for any $A \in \mathcal{A}_n$. Minkowski conjectured that for any unimodular lattice $L \subset \mathbb{R}^n$,

$$\sup_{\boldsymbol{x} \in \mathbb{R}^n} \inf_{\boldsymbol{y} \in L} N(\boldsymbol{x} - \boldsymbol{y}) \leq \frac{1}{2^n}.$$

This conjecture was originally motivated by the study of certain "approximation properties" of algebraic integers in number fields (see [23])). Minkowski proved his conjecture for $n = 2$; up until 2005, the conjecture was proved in dimensions $n \leq 5$. In his seminal paper [131], C. McMullen proved this conjecture for $n = 6$ (see [131] for references to the earlier work). He follows the Remak-Davenport approach (see Section 27.1 of [105] for details and history), splitting the Minkowski's conjecture into two statements from which it follows:

(W_n) For any lattice $L \subset \mathbb{R}^n$, there exists $A \in \mathcal{A}_n$ such that AL is WR.

(C_n) For any unimodular WR lattice $L \subset \mathbb{R}^n$, $\mu(L) \leq \mu(\mathbb{Z}^n) = \sqrt{n}/2$.

In the direction of (W_n), McMullen established that if the closure of the orbit of L under the action of $\mathcal{A}_n$ is bounded, then it contains a WR lattice. This, along with (C_n), turns out to be enough to establish Minkowski's conjecture. The second part (C_n) is known as A. C. Woods' covering conjecture [184]; prior to McMullen's work, it has been proved in dimensions $n \leq 6$ and has since been proved in all dimensions $n \leq 10$ (see [111] and references within). On the other hand, Woods' conjecture has been disproved in dimensions $n \geq 30$ by Regev, Shapira and Weiss [159], whose work has been extended by Chen and Xu to show that the conjecture fails for

$n \geq 24$ [48]. This, however, does not necessarily mean that Minkowski conjecture in those dimensions is not true.

Another important class of lattices (related to WR lattices at least in spirit) is semi-stable lattices: $L \subset \mathbb{R}^n$ is called *semi-stable* if for every sublattice $M \subseteq L$,

$$\det(M)^{1/\operatorname{rk}(M)} \leq \det(L)^{1/\operatorname{rk}(L)}.$$

Semi-stable lattices were first introduced in the context of reduction theory, where this condition was taken to heuristically suggest that the successive minima of L are not too far apart (see [7] and the excellent survey paper of Casselman [45] on semi-stable lattices, which in particular provides many references and the history of development of this subject). This, however, does not mean that WR lattices are necessarily semi-stable: this statement is only true for $n = 2$, whereas for $n \geq 3$ the sets of semi-stable and WR lattices are independent (see, *e.g.*, [85] for explicit examples of non-stable WR lattices in $\mathbb{R}^3$), although they do have an intersection. Similarly to the WR lattices, semi-stable lattices are also well-distributed among the orbits of the diagonal group action on the space of lattices. Specifically, in [171] the authors showed that, analogously to McMullen's observation about WR lattices, if the closure of the orbit of L under the action of $\mathcal{A}_n$ is bounded, then it contains a semi-stable lattice. Remarkably, in [175] Solan strengthened this observations for both, WR and semi-stable lattices, proving that for any lattice $L \subset \mathbb{R}^n$, there exist $A, B \in \mathcal{A}_n$ such that AL is WR and BL is semi-stable. In particular, this establishes the conjecture (W_n) from above.

The two-dimensional distribution of WR and semi-stable lattices can be described very explicitly and deserves some attention due to its connection to the parameterization of elliptic curves; our brief exposition follows [87], [86], [88]. Let $\mathbb{H} = \{\tau = a + bi : b \geq 0\} \subset \mathbb{C}$ be the upper half-plane, and let

$$\mathcal{D} := \{\tau = a + bi \in \mathbb{H} : -1/2 < a \leq 1/2, |\tau| \geq 1\}.$$

Let

$$\mathcal{F} := \{\tau = a + bi \in \mathbb{H} : 0 \leq a \leq 1/2, |\tau| \geq 1\},$$

so, loosely speaking, $\mathcal{F}$ is "half" of $\mathcal{D}$. Every point $\tau = a + bi \in \mathcal{F}$ can be identified with a lattice

$$\Gamma_\tau := \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2$$

in $\mathbb{R}^2$. Every planar lattice L is similar to a unique lattice of the form Γ_τ for some $\tau \in \mathcal{F}$, hence we can say that the similarity class of L is represented by τ. Thus, $\mathcal{F}$ can be thought of as the space of similarity classes of lattices in $\mathbb{R}^2$ (see Figure 1). WR similarity classes correspond to the circular arc $\{\tau \in \mathcal{F} : |\tau| = 1\}$ and semi-stable similarity classes correspond to the set $\{\tau = a + bi \in \mathcal{F} : b \leq 1\}$. On the other hand, the full domain $\mathcal{D}$ can be viewed as the space of isomorphism classes of elliptic curves: a point τ corresponds to the isomorphism class of the elliptic curve given by the complex torus $\mathbb{C}/\Gamma_\tau$, where we are identifying $\mathbb{C}$ with $\mathbb{R}^2$ and thinking of Γ_τ as $\operatorname{span}_{\mathbb{Z}}\{1, \tau\} \subset \mathbb{C}$. This being said, while the lattices Γ_τ and $\Gamma_{\bar{\tau}}$ are similar, the corresponding elliptic curves are not isomorphic: instead, the two elliptic curves have conjugate j-invariants, since $j(-\bar{\tau}) = \overline{j(\tau)}$ (here j is Klein's modular j-function).

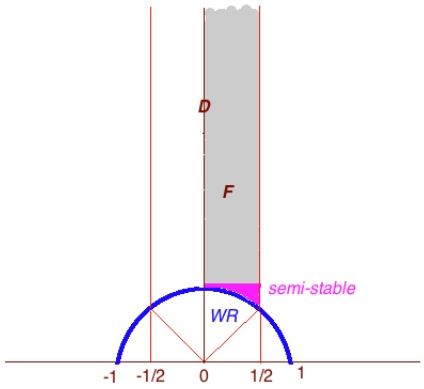

FIGURE 1. Similarity classes of lattices in $\mathbb{R}^2$ with WR and semi-stable subregions marked by colors.

Further, the question of distribution of WR sublattices of a given lattice $L \subset \mathbb{R}^2$ has been investigated by several authors via analysis of the properties of the so-called WR zeta-function

$$\zeta_{\mathrm{WR}}(s) = \sum_{k=1}^{\infty} a_k k^{-s},$$

where a_k is the number of WR sublattices of L of index k and s is a complex variable. Information about the position and order of the pole, as well as the residue at the pole of this function can be used along with Wiener-Ikehara Tauberian theorem and its later variations to establish the order of growth of the counting function $\sum_{k \le n} a_k$, the number of WR sublattices of L of index at most n as $n \to \infty$. The result depends on whether the lattice L is arithmetic or not. Specifically, combining the results of [84] and [114], we obtain:

$$\sum_{k \le n} a_k = \begin{cases} O(n \log n) & \text{if } L \text{ is arithmetic,} \\ O(n) & \text{if } L \text{ is not arithmetic,} \end{cases}$$

as $n \to \infty$. More detailed asymptotic results on the summatory function $\sum_{k \le n} a_k$ have later been obtained in [12].

There are several other contexts in which WR lattices have been investigated, *e.g.* in connection with the Frobenius problem [97]. Most importantly, WR lattices are key in discrete optimization and applications. In particular, the lattice packing problem can be restricted to WR lattices without loss of generality, *i.e.*, any solution to the lattice packing problem in every dimension $n \ge 2$ has to be a WR lattice. In fact, more is true. A lattice $L \subset \mathbb{R}^n$ with $m = |S(L)|$ is called *eutactic* if there exist positive real numbers $c_1, \ldots, c_m$ such that

$$\|\boldsymbol{x}\|^2 = \sum_{i=1}^{m} c_i \langle \boldsymbol{x}, \boldsymbol{y}_i \rangle^2, \tag{7}$$

where $S(L) = \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m\}$. The lattice L is *strongly eutactic* if $c_1 = \cdots = c_m$. On the other hand, if the space of $n \times n$ real symmetric matrices $\mathrm{Sym}_n(\mathbb{R})$ can be

represented as

$$\mathrm{Sym}_n(\mathbb{R}) = \mathrm{span}_{\mathbb{R}} \left\{ \boldsymbol{y}_i \boldsymbol{y}_i^\top : \boldsymbol{y}_i \in S(L) \right\},$$

then the lattice L is called *perfect*. Both, perfect and eutactic properties are preserved under similarity. While the sets of eutactic and perfect lattices are independent (there are perfect non-eutactic and eutactc non-perfect lattices), both of them are WR, but not necessarily semi-stable: an example of a perfect non-stable lattice in dimension 8 has been obtained by Y. Kim [112], where he also proved that all other perfect lattices in dimension ≤ 8 are semi-stable. A lattice is called *extreme* if it is a local maximum of the packing density function in its dimensions, and a classical theorem of Voronoi (see, *e.g.*, Theorem 3.4.6 of [127]) states that a lattice is extreme if and only if it is perfect and eutactic. It is well known that perfect lattices are necessarily arithmetic, hence so are extreme lattices. In every dimension $n \geq 2$ there are only finitely many eutactic and finitely many perfect similarity classes. For instance, up to similarity in $\mathbb{R}^2$, there are only two eutactic lattices ($\mathbb{Z}^2$ and Λ_h) and only one perfect (Λ_h). Further, Bacher proved [15] that the number p_n of perfect similarity classes of lattices in $\mathbb{R}^n$ satisfies the following inequalities for any $\varepsilon > 0$:

$$e^{n^{1-\varepsilon}} < p_n < e^{n^{3+\varepsilon}}.$$

The upper bound has recently been improved by van Woerden [179] to $e^{O(n^2 \log n)}$. The exact value of p_n has so far been published in all dimensions $n \leq 8$ with the 8-dimensional case being an extensive computational project by Dutour Sikirić, Schürmann and Vallentin [173] building on the previous results (see Section 6.6 of [127]): they showed that there are 10916 perfect lattices in $\mathbb{R}^8$, but only 2408 of them are eutactic (hence, extreme) by the work of Riener [160]. The computational project by Dutour Sikirić and van Woerden to count and classify perfect lattices in $\mathbb{R}^9$ has been ongoing for some years and has recently completed: their work is currently being prepared for publication.

We close this section with the notion of *generic well-rounded (GWR)* lattices, which has been considered in [119, 109]: a full-rank WR lattice $L \subset \mathbb{R}^n$ is called GWR if $|S(L)| = 2n$. One immediate example of a GWR lattice is $\mathbb{Z}^n$. GWR lattices can have a relatively high packing density while maintaining a relatively small kissing number, which is a useful property for some coding theory applications we detail below. One steady source of GWR lattices are the nearly orthogonal lattices. Given an ordered basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ for a lattice L, define a sequence of angles $\theta_1, \ldots, \theta_{n-1}$ so that each θ_i is the angle between $\boldsymbol{b}_{i+1}$ and the subspace

$$\mathrm{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}.$$

Then each $\theta_i \in [0, \pi/2]$ and B is called a *weakly nearly orthogonal* basis if $\theta_i \geq \pi/3$ for each $1 \leq i \leq n-1$. A basis B is called *nearly orthogonal* if every ordering of it is weakly nearly orthogonal. If L has such a basis, we say that L is a nearly orthogonal lattice. Nearly orthogonal lattices were introduced in [16], where they were applied to the problem of image compression. Nearly orthogonal lattices that are also WR (and often GWR) have been studied in [92].

1.3. **Algebraic constructions.** Due to their importance in a variety of theoretical contexts and applications, explicit constructions of WR families of lattices (often with additional properties) are of great interest. In particular, a great deal of attention was devoted to the study of constructions coming from different algebraic

settings. To this end, let us start with a number field K of degree $n \geq 2$ over $\mathbb{Q}$ and let us write Δ_K for its discriminant and $\mathcal{O}_K$ for its ring of integers. Assume that K has r_1 real embeddings $\sigma_1, \ldots, \sigma_{r_1} : K \to \mathbb{R}$ and r_2 pairs of complex conjugate embeddings $\tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2} : K \to \mathbb{C}$. Then $n = r_1 + 2r_2$ and we can define the *Minkowski embedding* of K into $\mathbb{R}^n$ by

$$\Sigma_K := (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \to \mathbb{R}^n.$$

Let $J \subset K$ be a fractional ideal, then $\Sigma_K(J) \subset \mathbb{R}^n$ is a lattice of full rank. Lattices like this are called *ideal lattices* via Minkowski embedding. Notice that for any $\alpha, \beta \in K$,

$$\langle \Sigma_K(\alpha), \Sigma_K(\beta) \rangle = \mathrm{Tr}_K(\alpha\bar{\beta}),$$

where Tr_K stands for the number field trace on K. Hence, the Euclidean lattice structure on $\Sigma_K(J)$ is induced by the trace of K. The theory of ideal lattices in a more general form has been developed by Bayer-Fluckiger, among other authors; see [22], [23] for a detailed survey of this area.

WR ideal lattices have first been studied in [96], where it was in particular proved that for totally real and totally imaginary number fields, $\Sigma_K(\mathcal{O}_K)$ is WR if and only if K is cyclotomic (see also [6]). More generally, let us say that an ideal $J \subseteq \mathcal{O}_K$ is WR if the corresponding ideal lattice $\Sigma_K(J)$ is WR. Infinite families of real and imaginary quadratic number fields containing WR ideals have been constructed in [96]. Further, in [89] it has been proved that for squarefree positive integer D, quadratic fields $K(\sqrt{\pm D})$ contain WR ideals when D has a divisor d satisfying

$$\sqrt{\frac{D}{3}} \leq d < \sqrt{D}.$$

This condition is if and only if in the case $K = \mathbb{Q}(\sqrt{-D})$. On the other hand, [176] establishes that $\mathbb{Q}(\sqrt{D})$ contains WR ideals if and only D has a divisor d satisfying

$$\sqrt{\frac{D}{3}} \leq d < \sqrt{3D}.$$

Thus, relatively few of ideal lattices from quadratic number fields are WR. On the other hand, as follows from the results of McMullen [131] and Solan [175], any ideal lattice can be "twisted" into a WR one by the action of the diagonal group $\mathcal{A}_2$. Damir and Karpuk in [65] investigated properties of the specific bases of ideals that result in the minimal basis of such corresponding WR twist. Further, situations when the canonical basis of an ideal in a quadratic number field can be so twisted have been studied in [63]. For higher degree number fields, WR ideals have been proved to exist in cyclic cubic and (some) cyclic quartic number fields [118]. Semi-stable ideal lattices have also been investigated; in particular, infinite families of semi-stable ideal lattices from any real quadratic number field were constructed in [85] (where it was also proved that a positive proportion of ideal lattices from real quadratic fields are semi-stable) and semi-stable twists of canonical bases of ideals in all quadratic number fields were studied in [63]. Well-rounded ideal lattices from totally definite quaternion algebras were recently studied in [49].

There is a different algebraic construction of lattices actively used in cryptography, which has also received the name of ideal lattices. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n and consider the quotient ring $R(f) := \mathbb{Z}[x]/\langle f(x) \rangle$. Define the *coefficient embedding*

$$\rho_f : R(f) \to \mathbb{Z}^n,$$

given by $\rho_f(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = (a_0, a_1, \ldots, a_{n-1})^\top$. This is a linear map between two free $\mathbb{Z}$-modules and an ideal $J \subseteq R(f)$ is mapped onto a sublattice $\rho_f(J) \subseteq \mathbb{Z}^n$. We will call such lattices the *coefficient ideal lattices*; they generalize the original construction of *cyclic lattices* (introduced by Micciancio in [133]), which are the special case $\rho_f(J)$ for $f(x) = x^n - 1$. These lattices were introduced and studied in the cryptographic context by Lyubashevsky and Micciancio [123]. WR cyclic lattices have been investigated in [98], [99], [93].

If $f(x)$ is an irreducible polynomial, then the corresponding map ρ_f is a linear isomorphism of $\mathbb{Z}$-modules $R(f)$ and $\mathbb{Z}^n$ and the coefficient ideal lattices $\rho_f(J)$ have full rank (Lemma 3.2 of [123]). In the special case when $f(x)$ is n-th cyclotomic polynomial of degree $\varphi(n)$, the ring $R(f)$ can be identified with the ring of integers $\mathbb{Z}[\theta_n]$ of the cyclotomic field $\mathbb{Q}(\theta_n)$ via the canonical isomorphism $x \mapsto \theta_n$, where $\theta_n = e^{2\pi i/n}$ is n-th primitive root of unity. One can then ask about the relation between the two embeddings, *i.e.*, between the ideal lattice $\Sigma_{\mathbb{Q}(\theta_n)}(J)$ and the coefficient ideal lattice $\rho_f(J)$ for a given ideal J in this ring. The linear transformation between the two has been worked out by Batson in [21] as we describe in Eq. (11) .

The construction of lattices via Minkowski embedding can start from any free $\mathbb{Z}$-module contained in the number field K, not only from an ideal in $\mathcal{O}_K$. Let, for instance, $\mathcal{M}(\alpha) = \mathrm{span}_{\mathbb{Z}}\{\alpha_1, \ldots, \alpha_n\}$, where $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic conjugates contained in K. A special case of this construction when K is a cyclic number field of odd prime degree has been considered in [68], [69], where families of WR such lattices (in fact, even having bases of minimal vectors) have been obtained. More general such constructions of GWR nearly orthogonal lattices with bases of minimal vectors and large automorphism groups – in particular, coming from Pisot numbers – are currently being explored in [91]. More generally, the so-called *module lattices* in $\mathbb{R}^{nd}$, $n = [K : \mathbb{Q}]$, $d \geq 1$, coming from modules $\mathcal{M} \subset K^d$ via Minkowski embedding $\Sigma_K : K^d \to \mathbb{R}^{nd}$ were used in [117] in the construction of lattice-based crypto-schemes; see Section 2 for more details.

Another explicit algebraic construction of WR lattices comes from curves over finite fields. Let F be an algebraic function field of a single variable with the finite field $\mathbb{F}_q$ as its field of constants. Let $\mathcal{P} = \{P_0, P_1, \ldots, P_{n-1}\}$ be the set of rational places of F and for each P_i, let v_i denote the corresponding normalized discrete valuation. Let $\mathcal{O}_{\mathcal{P}}^*$ be the abelian group of all nonzero functions $f \in F$ whose divisor has support contained in the set $\mathcal{P}$. Then $\sum_{i=0}^{n-1} v_i(f) = 0$ for each $f \in \mathcal{O}_{\mathcal{P}}^*$. Let $n = |\mathcal{P}|$, the number of rational places of F, and define the homomorphism $\phi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* \to \mathbb{Z}^n$ by

$$\phi_{\mathcal{P}}(f) = (v_0(f), v_1(f), \ldots, v_{n-1}(f)).$$

Then $L_{\mathcal{P}} := \phi_{\mathcal{P}}(\mathcal{O}_{\mathcal{P}}^*)$ is a finite-index sublattice of the root lattice

$$A_{n-1} = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \sum_{i=0}^{n-1} x_i = 0 \right\}.$$

These lattices, called *function field lattices*, are described in detail in the well known book [177] by Tsfasman and Vladut (Chapter 5.4); they were originally introduced in [164] by Rosenbloom and Tsfasman, who used this construction to produce asymptotically good families of lattices from the standpoint of packing density. A more systematic investigation of the geometric properties of these lattices was carried out more recently by several authors. In particular, the case of elliptic

curves (algebraic function fields of genus 1) has been considered in [94] and [170], where it has been proved that for $n \geq 5$ the lattice $L_{\mathcal{P}}$ is WR and has a basis of minimal vectors. This, however, is a special case of the more general result of [39] on lattices from finite abelian groups discussed below. For fields of higher genus, the case of Hermitian function fields $\mathbb{F}_q(x, y)$ with $y^q + y = x^{q+1}$ for a prime power q is considered in [40], where it is proved that the corresponding lattice $L_{\mathcal{P}}$ is WR and generated by minimal vectors. On the other hand, examples of hyperelliptic function fields giving rise to non-WR lattice $L_{\mathcal{P}}$ are presented in [10].

We now turn to explicit algebraic constructions of families of extreme lattices. The most standard of these are the *irreducible root lattices* A_n, D_n, E_6, E_7, E_8 and on some occasions their duals (a lattice is called *irreducible* if it is not an orthogonal sum of proper sublattices). We refer the reader to the excellent detailed exposition of the theory of root lattices (as well as related to them Coxeter lattices) in Martinet's book [127] and focus instead on a more recent lesser-known construction. Let $G = \{0_G, z_1, \ldots, z_n\}$ be an additive abelian group and define

$$L_G := \left\{ \boldsymbol{a} \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i = 0,\ \sum_{i=1}^{n} a_i z_i = 0_G \right\},$$

which is a lattice of rank $n-1$. Böttcher et al. [39] proved that the lattice L_G is WR and, in fact, has a basis of minimal vectors for $G \neq \mathbb{Z}/4\mathbb{Z}$. Further, Böttcher et al. [38] established that L_G is strongly eutactic for all G of odd order or elementary abelian 2-groups. Additionally, Ladisch [116] proved that L_G is eutactic for all $G \neq \mathbb{Z}/4\mathbb{Z}$. On the other hand, Bacher [14] proved that for all G of order at least 9, the lattice L_G is perfect. Putting these results together, we see that L_G is extreme for all finite abelian groups G of order at least 9. Additional constructions of strongly eutactic lattices from tight (equiangular) frames and distance transitive graphs have been given in [41] and [95], respectively. We choose, however, not to detail them here since they are somewhat more analytic in nature.

Finally, we mention the notion of *tame* lattices that were introduced in [67] and motivated by the behavior of the trace pairing over tame cyclic number fields as well as by their ability to serve a method to explicitly construct WR lattices. Tame lattices have a *Lagrangian basis* [55] and they have Gram matrices of a nice specific form. Tame lattices are known to exist for any tame number field with a prime conductor [33]. GWR lattices arising from tame ones were constructed and studied in [109], including a discussion on their applicability to wireless security, which we discuss in Section 3.

1.4. **Spherical designs and Epstein zeta-function.** We also briefly discuss spherical designs and their connection to (highly structured) Euclidean lattices. Let $\mathcal{S}_{n-1}(r) \subset \mathbb{R}^n$ be the sphere of radius r centered at the origin in $\mathbb{R}^n$. A finite collection of points $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\} \subset \mathcal{S}_{n-1}(r)$ is called a *spherical t-design* for an integer $t \geq 1$ if for any polynomial $p(y_1, \ldots, y_n) \in \mathbb{R}[y_1, \ldots, y_n]$ of degree $\leq t$,

$$\frac{1}{m} \sum_{i=1}^{m} p(\boldsymbol{x}_i) = \int_{\mathcal{S}_{n-1}(r)} p(\boldsymbol{y}) d\boldsymbol{y},$$

where the measure is normalized so that $\int_{\mathcal{S}_{n-1}(r)} d\boldsymbol{y} = 1$. Spherical t-designs have been originally introduced by Delsarte, Goethals and Seidel [71]. The existence of spherical t-designs in $\mathbb{R}^n$ for any $t, n \geq 1$ was established by Seymour and T.

Zaslavsky [169]) with effective bounds on the size of such designs produced by Bondarenko, Radchenko and Viazovska [37]. We state here a convenient criterion for a $\mathbf{0}$-symmetric set $X \subset \mathcal{S}_{n-1}(r)$ to be a spherical t-design for $t = 2p$ and $t = 2p+1$, $p \geq 1$: such X is a spherical t-design if and only if there exists a constant c_p such that

$$\|\boldsymbol{y}\|^{2p} = \frac{c_p}{r^{2p}|X|} \sum_{\boldsymbol{x} \in X} \langle \boldsymbol{y}, \boldsymbol{x} \rangle^{2p}, \tag{8}$$

for all $\boldsymbol{y} \in \mathbb{R}^n$. An important class of such symmetric spherical designs comes from sets of minimal vectors in lattices. Indeed, comparing (7) with (8), we see that a lattice $L \subset \mathbb{R}^n$ is strongly eutactic if and only its set of minimal vectors $S(L)$ is a spherical 2-design.

The connection between spherical designs and lattices has been studied by several authors, starting with the fundamental paper of B. Venkov [182] (see also Chapter 16 of [127] for a nice exposition of the results of [182]). A lattice whose set of minimal vectors is a spherical 4-design is called *strongly perfect*, and Venkov proves that strongly perfect lattices are extreme (hence, perfect, by Voronoi's theorem, making the notation justified). In the same paper, Venkov also produced a list (albeit not a full classification) of strongly perfect lattices in dimensions $n \leq 24$. Various classification results for strongly perfect lattices and lattices carrying even higher-degree spherical designs have appeared since (see, *e.g.*, [148] and references within). We refer the reader to the paper [145] by Nebe for a detailed survey of Venkov's theory of lattices and spherical designs and related contributions by other authors.

Spherical designs play a role in another important optimization problem on lattices. The *Epstein zeta-function* of a lattice $L \subset \mathbb{R}^n$ is defined as

$$\mathcal{Z}_L(s) = \sum_{\boldsymbol{x} \in L \setminus \{\mathbf{0}\}} \|\boldsymbol{x}\|^{-2s},$$

for a variable $s \in \mathbb{C}$. For each lattice L in each dimension $n \geq 2$, this Dirichlet series converges in the half-plane $\Re(s) > n/2$, has a simple pole at $s = n/2$ and admits a meromorphic continuation to the whole complex plane. The classical minimization problem for the Epstein zeta-function considers a fixed real value $s_0 > 0$, $s_0 \neq n/2$, and asks for a lattice $L_0 \subset \mathbb{R}^n$ such that

$$\mathcal{Z}_{L_0}(s_0) = \min \{\mathcal{Z}_L(s_0) : L \subset \mathbb{R}^n\}.$$

Besides the intrinsic lattice theory interest, this problem also come up in the work of S. Sobolev [174] in regards to numerical integration. In dimension $n = 2$, this problem dates back at least to the work of Rankin [156], Cassels [46], Diananda [73] and Ennola [81], who established that for any such s_0 the minimum occurs only at the hexagonal lattice. In dimension $n = 3$, the minimization problem was solved by Ennola [82] and in dimensions $n = 4, 8, 24$ by Sarnak and Strömbergsson [166]. It was separately proved by Ryškov [165] that the minimizer of $\mathcal{Z}_L(s)$ as $s \to \infty$ corresponds to the densest lattice packing in $\mathbb{R}^n$.

This last observation makes it especially interesting to look for such minimizers, and that is where spherical designs again make an appearance. Given a lattice $L \subset \mathbb{R}^n$, let us define the *spectrum* of L to be the set $\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\}$. We can write the spectrum as an ordered set of real numbers $\{0 < a_1 < a_2 < \dots\}$ and

define the k-th *layer* of L to be

$$\{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = a_k\}.$$

With this notation, we can state a remarkable theorem of Coulangeon [59]: if every layer of L contains a spherical 4-design, then L is a minimizer of $\mathcal{Z}_L(s)$ for every real value of $s > n/2$.

The minimization problem for Epstein zeta-function also has an interesting applied connection. A Dirichlet series $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ and the corresponding power series $f(z) = \sum_{n=1}^{\infty} a_n z^n$ are connected via the *Mellin transform*:

$$\Gamma(s)F(s) = \int_0^{\infty} x^{s-1} f(e^{-x}) dx,$$

where $\Gamma(s)$ is the value of the Γ-function at s. Thus, $\mathcal{Z}_L(s)$ for an integral lattice L corresponds to the power series $\Theta_L(z)$, called the *theta-function* of L. The corresponding minimization problem for $\Theta_L(z)$ has important implications for maximizing the reliability and security of communications when using lattices to construct coding schemes for wireless communications. We discuss this connection in more detail in Section 3.

2. Lattice-based cryptography

Over the last few decades, interest in lattices has grown due to their applications in cryptography. In this chapter, we discuss lattice-based cryptography (LBC), focusing on paradigms whose security depends on hard mathematical problems involving lattices. We describe several complex problems in LBC and examine their worst-case and average-case hardness. In particular, our main focus will be on the Learning with Errors (LWE) problem and its variants, and analyze the relationships among them. For further background, see [50], [125], [158]. We begin with a general introduction to post-quantum cryptography (PQC).

Post-quantum cryptography. Cryptography relies on complex mathematical problems, such as the discrete logarithm and integer factorization problems. The RSA [162] and Diffie-Hellman protocols [74], which protect our communication networks, are based on these two problems. However, rapid progress in quantum computing poses a serious threat to these foundations. The Shor algorithm [172], introduced by Peter Shor in 1994, solves both problems in polynomial time on a large enough quantum computer, rendering the protocols insecure. This leads us to the field of post-quantum cryptography [61], which focuses on cryptographic protocols that are resistant to quantum attacks. This provides an alternative for the soon-to-be-broken schemes. The main post-quantum approaches are code-based, isogeny-based, multivariate, hash-based, and lattice-based cryptography. Among these, lattice-based schemes are central for their simplicity, flexibility, and strong security guarantees.

A problem is considered hard in the worst case if it is hard for at least one instance, and average-case hard if it is hard for most instances from a given distribution. Worst-case hardness provides theoretical assurance but may not guarantee security, as random instances might too often correspond to weak instances. To guarantee strong security, we require random (average) instances that are likely to be as hard as the worst case instances. Proving such a property is done by a process called *worst-case-to-average-case reduction*. We define several widely studied worst-case hard lattice problems in the following section.

2.1. Hard lattice problems.

We define some of the fundamental lattice problems believed to be hard in the worst case.

Shortest vector problem (SVP): Given a basis B of a lattice L, find a shortest non-zero vector of the lattice. Explicitly, find a nonzero vector $\boldsymbol{x} \in L$ such that $\|\boldsymbol{x}\| = \lambda_1(L)$. The approximate version, *approximate SVP* problem (SVP_γ), asks for a nonzero $\boldsymbol{x} \in L$ such that $\lambda_1(L) \leq \gamma(n)\|\boldsymbol{x}\|$ where $\gamma(n) \geq 1$. The *GapSVP*$_\gamma$ problem (decision SVP_γ) asks to decide if $\lambda_1(L) \leq r$ or $\lambda_1(L) \geq \gamma r$ where $r \in \mathbb{Q}$.

Closest vector problem (CVP): Given a basis B, of a lattice L, and a target vector $\boldsymbol{t} \notin L$, find a vector in L that is closest to $\boldsymbol{t}$. When $dist(t, L) \leq d$ where $d \in \mathbb{Z}^+$ we refer to this as a *bounded distance decoding problem (BDD)*. The approximate version, CVP_γ, asks to find a lattice vector at distance at most γ. And the decision version, GapCVP_γ asks to decide whether $dist(t, \mathcal{L}) < 1$ or $dist(t, L) < \gamma$.

Shortest independent vector problem (SIVP): Given a lattice L, find n linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ in L such that $\max_i \|\boldsymbol{v}_i\| \leq \lambda_n(L)$. The approximate

version, SIVP_γ finds these vectors with length at most $\gamma\lambda_n(L)$. On the other hand, the decision version, GapSIVP_γ asks to determine if $\lambda_n(L(B)) \leq d$ or $\lambda_n(L(B)) > \gamma d$.

Generalized shortest independent vector problem ($GIVP^\phi_\gamma$): Given a lattice $L(B)$ of dimension n, find n linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ in L such that $\max_i \|\boldsymbol{v}_i\| \leq \gamma\phi(L(B))$ where ϕ is an arbitrary real valued function of a lattice and $\gamma(n) \geq 1$. When $\phi = \lambda_n$, we get the SIVP_γ.

The hardness of these lattice problems has been widely studied due to their importance in applications. In particular, the SVP and the CVP, along with their approximate versions, form the basis for many secure post-quantum cryptographic schemes. The first results showing that CVP is computationally hard date back to Van Emde Boas [178], who showed that CVP is NP-hard via a deterministic reduction. That is, with high probability, any problem in NP can be reduced in polynomial time to an instance of CVP. Based on the similarities between SVP and CVP, he further conjectured SVP was also NP-hard. After almost two decades, Ajtai in [5] showed that SVP with the l_2-norm is NP-hard for randomized reduction, thus proving the van Emde Boas conjecture.

In practice, one typically works with the approximate variants of SVP and CVP, which are also NP-hard for a small enough approximation factor γ. Arora et al. [8] showed that the approximate CVP is NP-hard within any constant. Micciancio [132] later showed that for any l_p-norm, approximate SVP within any constant factor $\gamma < \sqrt[p]{2}$ is hard under some random reductions. Specifically, in the Euclidean norm, the approximate SVP is NP-hard with any factor $\gamma < \sqrt{2}$. Extending on [8], Dinur *et al.* in [75] later showed that the approximate CVP problem in an n-dimensional lattice is NP-hard for a factor $\gamma = n^{\frac{c}{\log\log n}}$ for some constant $c > 0$.

Further studies on the hardness of these problems have been conducted within an exponential factor. However, the results show that these problems are unlikely to be NP-hard. In particular, the approximate CVP and SVP are highly likely not NP-hard within a factor $\sqrt{n}$ [104, 2]. Despite these limitations, these problems are computationally hard in the worst case and form the basis of modern cryptography. The connection between these worst-case hard lattice problems and security brings us to the field of lattice-based cryptography.

The study of lattice-based cryptography began with Ajtai's ground breaking work in [4], which introduced the first average-case hard problem, *the short integer solution* (SIS). On a high level, the SIS problem asks one to recover a short nonzero vector $\boldsymbol{z} \in \mathbb{Z}^m$ given a random matrix $A \in \mathbb{Z}^{n\times m}$ satisfying $A\boldsymbol{z} = 0 \mod q$. The requirement for $\boldsymbol{z} \neq \boldsymbol{0}$ and short is what makes this problem difficult. This hardness was shown by a worst-case-to-average-case reduction from a well known worst-case hard problem. Building on this, in 2005 Regev introduced the learning with errors (LWE) problem [157], which is a noisy analog of SIS. This problem plays a central role in LBC. On a high level, the LWE problem is the following: given arbitrary independent samples of noisy linear equations $(\boldsymbol{a}, b = \boldsymbol{a}\cdot\boldsymbol{s} + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, recover the secret $\boldsymbol{s} \in \mathbb{Z}_q^n$. The error e, is sampled from a Gaussian distribution. The choice of the error distribution plays a critical role in the hardness of the problem as well as in the correctness of the public key encryption scheme based on the LWE problem. We describe this below.

2.2. **Gaussians, variational distance, and the smoothing parameter.** A continuous Gaussian function centered at $c \in \mathbb{R}^n$ defined over $\mathbb{R}^n$ is given by

$$\rho_{s,c}(\boldsymbol{x}) = \exp \frac{-\pi \|\boldsymbol{x} - \boldsymbol{c}\|^2}{s^2},$$

where $s = \sqrt{2\pi}\sigma$ with σ being the standard deviation. Normalizing this function by $1/s^n$ defines the corresponding probability density function

$$g_{s,c}(\boldsymbol{x}) = \frac{1}{s^n} \exp \frac{-\pi \|\boldsymbol{x} - \boldsymbol{c}\|^2}{s^2}.$$

If $c = 0$, we denote $\rho_{s,0} = \rho_s, g_{s,0} = g_s$.

Let us consider the L-periodic function $g_{s,L}(\boldsymbol{x}) = \sum_{\lambda \in L} g_{s,\lambda}(\boldsymbol{x})$, which is a probability density function when restricted to $\mathbb{R}^n/L$. We can now define the *discrete Gaussian distribution* $D_{L,s,c}$ as

$$D_{L,s,c}(\boldsymbol{x}) = \frac{g_{s,c}(\boldsymbol{x})}{g_{s,L}(c)}$$

for $\boldsymbol{x} \in L$ and zero otherwise. Again, we denote $D_{L,s,0} = D_{L,s}$.

An important tool used in lattice-based schemes is the *smoothing parameter*, which ensures that the noise parameter s is large enough to hide the underlying secret structure. More rigorously, it determines the minimal noise level that guarantees indistinguishability from a uniform distribution by a maximum gap δ. By "gap", we mean the *variational distance* (equivalently, *statistical distance*) between two distributions p_X and p_Y;

$$V(p_X, p_Y) = \int_{\mathbb{R}^n} |p_X(\boldsymbol{x}) - p_Y(\boldsymbol{x})| d\boldsymbol{x}. \tag{9}$$

Smoothing parameter [134]*:* Let $L \subset \mathbb{R}^n$ be a full-rank lattice and $\delta > 0$. The smoothing parameter $\eta_\delta(L)$ is defined as

$$\eta_\delta(L) = \inf \left\{ s > 0 \;\middle|\; \rho_{1/s}(L^* \setminus \{0\}) \;\leq\; \delta \right\}. \tag{10}$$

In other words, fixing s to be the infinimum ensures that the variational distance between the lattice Gaussian and the uniform distribution on the Voronoi cell is at most δ.

The smoothing parameter is closely related to the flatness factor, which we will define in Section 3, Eq. (12).

Remark 2.1. The continuous Gaussian is used for analysis such as defining the smoothing parameter and for reduction proofs. In contrast, the discrete Gaussian is used for the actual cryptographic constructions, such as sampling the errors. We will use both in this work as needed depending on the context.

2.3. **Learning with errors (LWE) and its variants.** We define the LWE problem and some of its variants like the ring learning with errors (RLWE), the polynomial learning with errors (PLWE) problems and the module learning with errors problem (MLWE). We closely follow the definitions in [157], [124], [44].

Learning with errors (LWE) problem. Let $n \geq 1$ and $q = q(n) \geq 2$ be integers. Let $\boldsymbol{s} \in \mathbb{Z}_q^n$ be a secret vector sampled uniformly where n is the security parameter. Additionally, let χ be the error distribution that follows a discrete Gaussian sampled over $\mathbb{Z}$ and reduced modulo q.

LWE distribution: The LWE distribution $\mathcal{A}_{\boldsymbol{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is defined as follows: sample $\boldsymbol{a} \leftarrow \mathbb{Z}_q^n$ uniformly, $e \leftarrow \chi$, and output $(\boldsymbol{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where $b = \langle \boldsymbol{s}, \boldsymbol{a} \rangle + e \pmod q$. The addition is performed modulo q.

Search LWE ($LWE_{q,\chi}$): Given an arbitrary number of independent samples $(\boldsymbol{a}_i, b_i)$, drawn from the LWE distribution $\mathcal{A}_{\boldsymbol{s},\chi}$, the search LWE problem asks to find the secret vector $\boldsymbol{s}$.

Decision LWE: Given arbitrary many independent samples the decision problem asks to determine with non-negligible advantage whether the sample $(\boldsymbol{a}_i, b_i)$, is from the LWE distribution $\mathcal{A}_{\boldsymbol{s},\chi}$ or from a uniform distribution.

In matrix form: $(A, \boldsymbol{b}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$ where A is a matrix whose columns are the vectors $\boldsymbol{a}_i \in \mathbb{Z}_q^n$ and $\boldsymbol{b}^t = \boldsymbol{s}^t A + \boldsymbol{e}^t \pmod q$ with m the number of samples. Let

$$L = \{\boldsymbol{y} \in \mathbb{Z}^m : A^T \boldsymbol{z} = \boldsymbol{y} \pmod q \text{ for some } \boldsymbol{z} \in \mathbb{Z}^n\}.$$

Observe that L is a full rank integer lattice in $\mathbb{R}^n$, when we choose $m = n$ linearly independent $\boldsymbol{a}_i$'s. The LWE problem can be viewed as a bounded distance decoding problem on L where $\boldsymbol{b}$ is a closest vector to a lattice point.

The relevance of LWE lies in its reduction from a worst-case hard problem. We state the hardness result below.

Theorem 2.1. *(*[157]*, Theorem 1.1) Let n, q be integers, $\alpha \in [0, 1)$ be such that $\alpha q > 2\sqrt{n}$ and χ a Gaussian distribution. If there exists an efficient algorithm that solves $LWE_{q,\chi}$, then there exists an efficient quantum algorithm that approximates the decision version of SVP (GapSVP) and SIVP to within $\tilde{O}(n/\alpha)$[1] in the worst case.*

The LWE decision and search versions are equivalent when the integer modulus q is prime [157]. Although LWE offers strong security guarantees, LWE-based schemes have a quadratic overhead in the key size in terms of the security parameter n, rendering them inefficient for practical purposes. To address this concern, Lyubashevsky, Peikert, and Regev [124], [125] introduced the ring variant of LWE, known as the ring learning with errors (RLWE) problem, which only induces a linear overhead. This variant was originally formulated in the so-called dual form. However, the primal version is preferable in practice. Since the dual and primal formulations are known to be equivalent [163], we restrict ourselves to the primal version, which we refer to as RLWE. We closely follow the definition in [78].

Ring learning with errors (RLWE) problem. Let $n \geq 1$ and $q = q(n) \geq 2$ be an integer modulus. Let K be a number field of degree n and $R = \mathcal{O}_K$ its ring of integers. Set $R_q = \mathcal{O}_K / q\mathcal{O}_K$ and let χ be the discrete Gaussian distribution obtained by sampling over the ideal lattice $L = \Sigma(R)$ (see Section 1.3). Let $s \in R_q$ be sampled uniformly at random.

RLWE distribution ($\mathcal{A}_{s,\chi}$): The RLWE distribution $\mathcal{A}_{s,\chi}$ in $R_q \times R_q$ is defined by uniformly sampling $a \leftarrow R_q$, $e \leftarrow \chi$, and returning $(a, b) \in R_q \times R_q$ where $b = as + e \pmod q$.

Search RLWE ($RLWE_{q,\chi}$): For an arbitrary number of independent samples (a_i, b_i), drawn from the RLWE distribution $\mathcal{A}_{s,\chi}$, the $\text{RLWE}_{q,\chi}$ problem asks to recover the

[1]The function $f(n) = O(g(n))$ if there exist constants $c > 0$ and n_0 such that $f(n) \leq c\, g(n)$ for all $n \geq n_0$. We denote $\tilde{O}(f(n)) = O(f(n) poly \log(n))$.

secret s.

Decision RLWE (D-RLWE$_{q,\chi}$): Given an arbitrary number of independent samples (a_i, b_i), the D-RLWE$_{q,\chi}$ asks to determine with non-negligible advantage whether it came from the RLWE distribution $\mathcal{A}_{s,\chi}$ or a uniform distribution.

The following result guarantees the hardness of this problem.

Theorem 2.2 ([124])**.** *Let $K = \mathbb{Q}(\zeta_m)$ be the mth cyclotomic number field with degree $n = \varphi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n)$ and let $q = q(n) \geq 2$, $q \equiv 1 \pmod{m}$ be a poly(n)-bounded prime such that $\alpha q > \omega(\sqrt{\log n})$[2]. Then there is a polynomial time reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate SIVP (or SVP) on ideal lattices in K to the problem of solving D-RLWE$_{q,\chi}$*

The assumption that K is a cyclotomic field is only needed in the reduction from RLWE$_{q,\chi}$ to D-RLWE$_{q,\chi}$. This reduction has been extended to any Galois extension [78]. Unlike LWE-based schemes, cryptographic protocols based on RLWE have linear overhead in the degree of the number field due to the added structure [125]. However, this added structure may introduce weaknesses that are not present in plain LWE [80].

One way to improve the security is by increasing the field extension degree, thereby also increasing the degree of the involved polynomials. This has an obvious adverse effect on the computational complexity. A better alternative is by another structured LWE variant, the general or module LWE framework of [43], later formalized as MLWE with a worst-case hardness reduction by Langlois and Stehlé [117]. We will closely follow [42, 117]. Essentially, in a sample (a, b) we now consider a to be a vector of length d instead of a single ring element or polynomial ($d = 1$), resulting in a module structure over a ring. This enables increasing the security level by increasing the module rank d, while keeping the underlying field extension degree and ring intact. Moreover, instead of a single distribution, we will now need a family of distributions to match the varying d.

Module learning with errors (MLWE) problem. Let K be a number field of degree n, $R = \mathcal{O}_K$, Ψ a family of distributions on $K_\mathbb{R}$ and the torus $\mathbb{T} = K_\mathbb{R}/R$. For q, d positive integers with $q \geq 2$ and $d \geq 1$, let $\boldsymbol{s} \in R_q^d$ be the secret and $\psi \in \Psi$. Let $N = nd$ denote the dimension of the corresponding module lattice. We define the primal version of the problem as presented in [42].

Module learning with errors distribution. The MLWE distribution $\mathcal{A}_{\boldsymbol{s},\psi}^{\mathcal{M}}$ is obtained by sampling $\boldsymbol{a} \leftarrow \mathcal{U}(R_q^d)$, $e \leftarrow \psi$ and returning $(\boldsymbol{a}, b) \in R_q^d \times \mathbb{T}$ where $b = q^{-1}\langle \boldsymbol{a}, \boldsymbol{s} \rangle + e \pmod{R}$.

Search MLWE: Given arbitrary many samples from $\mathcal{A}_{\boldsymbol{s},\psi}^{\mathcal{M}}$, the search MLWE problem, MLWE$_{q,\Psi}$, asks to recover $\boldsymbol{s}$.

Decision MLWE: Let Υ be a distribution on a family of distributions on $K_\mathbb{R}$. The decision MLWE, D-MLWE$_{n,d,q,\Upsilon}$, is to distinguish with non-negligible advantage between arbitrary many independent samples from $\mathcal{A}_{\boldsymbol{s},\psi}^{\mathcal{M}}$ and the same number of independent samples from $\mathcal{U}(R_q^d \times \mathbb{T})$.

The MLWE problem was originally motivated by the goal of building a fully homomorphic scheme without bootstrapping. Langlois *et al.* in [117] later proved that MLWE is as hard as solving approximate SIVP over module lattices in the

[2]The function $\omega(f(n))$ grows asymptotically faster than $f(n)$.

worst case. We refer to their paper for a thorough discussion on the security of MLWE.

Theorem 2.3. *Let $\varepsilon(N) = N^{-\omega(1)}$, $\alpha \in (0,1)$, and $q \geq 2$ of known factorization such that*

$$\alpha q > 2\sqrt{d} \cdot \omega(\sqrt{\log n}).$$

There is a quantum reduction from solving $GIVP^{\eta}_{\gamma,\varepsilon}$ over module lattice in polynomial time (in the worst case, with high probability) to solving $MLWE_{q,\Psi_{\leq\alpha}}$ in polynomial time with non-negligible advantage, where

$$\gamma = \frac{8Nd \cdot \omega(\sqrt{\log n})}{\alpha}.$$

Assume that q is prime, $q \leq \mathrm{poly}(N)$, and that $q \equiv 1 \pmod{m}$ where m is the conductor of a cyclotomic field. Then there exists a polynomial-time reduction from $MLWE_{q,\Psi_{\leq\alpha}}$ to D-$MLWE_{q,\Upsilon_\alpha}$.

As mentioned earlier, the module learning with errors is a generalization of the previous variants of LWE. More precisely, setting $n = d = 1$ corresponds to the basic LWE, while $d = 1, n > 1$ yields RLWE.

Although this is more efficient than standard LWE, in practice, concrete polynomial rings are often preferred for their practical advantages and simplicity. This leads us to the polynomial learning with errors (PLWE) problem, described in the following section.

Polynomial learning with errors (PLWE) problem. Let $n \geq 1$ and $q = q(n) \geq 2$. Set $R(f) = \mathbb{Z}[x]/(f(x))$ to be the polynomial ring and $R_q(f) = R(f)/qR(f)$ and χ be a discrete Gaussian over $\rho_f(R(f))$ (see Section 1.3). Let $s \in R_q$ be sampled uniformly at random.

PLWE distribution ($\mathcal{B}_{f,s,\chi}$): The PLWE distribution $\mathcal{B}_{f,s,\chi}$ in $R_q(f) \times R_q(f)$ is obtained by uniformly sampling $a \leftarrow R_q(f)$, $e \leftarrow \chi$, and returning $(a, b) \in R_q(f) \times R_q(f)$ where $b = as + e \pmod{q}$.

PLWE (Search $PLWE_{f,q,\chi}$): For an arbitrary number of independent samples (a_i, b_i), drawn from the PLWE distribution $\mathcal{B}_{f,s,\chi}$, the $\mathrm{PLWE}_{f,q,\chi}$ search problem asks to find the secret s.

Decision PLWE (D-$PLWE_{f,q,\chi}$): Given an arbitrary number of independent samples (a_i, b_i), the D-$\mathrm{PLWE}_{f,q,\chi}$ asks to determine whether it was drawn from the PLWE distribution $\mathcal{B}_{f,s,\chi}$ or a uniform distribution.

Unlike the RLWE problem, which admits an worst-case-to-average-case reduction, the PLWE problem has such reductions only for powers of two cyclotomic fields. A natural step to extend this reduction to a broader class of fields will be to study the equivalence between RLWE and PLWE. This allows us to enjoy both efficiency and security advantages. In the following section, we define the equivalence between RLWE and PLWE and survey known results on this topic.

2.4. **Equivalence between RLWE and PLWE.** The RLWE and PLWE problems are said to be *equivalent* if there exists an algorithm that transforms a RLWE sample into a PLWE sample and vice versa in polynomial time, incurring a noise increase which is polynomial in the degree of the number field. This sample transformation is performed using the following map.

$$V_f : \mathbb{Z}[x]/(f(x)) \to \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_n(\mathcal{O}_K)$$

$$\sum_{i=0}^{n-1} a_i x^i \mapsto \underbrace{\begin{bmatrix} 1 & \theta_1 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \dots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \dots & \theta_n^{n-1} \end{bmatrix}}_{V_f} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \tag{11}$$

This transformation incurs some noise distortion, which is quantified by the condition number of V_f [163], defined by $\mathrm{Cond}(V_f) = \|V_f\|\|V_f^{-1}\|$, where

$$\|V_f\| = \sqrt{\mathrm{Tr}(V_f V_f^*)}.$$

This reduces the question of equivalence to analyzing the condition number of the transformation matrix V_f. This topic has been widely studied and we highlight some known results.

Ducas and Durmus in [76] showed that equivalence holds for power-of-two cyclotomic fields where the change-of-basis matrix is a scaled isometry. In [163], equivalence was established for a certain ad hoc class of fields. Further results were obtained for cyclotomic fields whose conductors are divisible by two distinct prime factors [27], [167]. This result was later extended in [30] to cyclotomic fields whose conductors are divisible by six distinct prime factors. Later in [72] it was shown that equivalence fails for general cyclotomic fields.

Other classes of fields have also been studied, such as the maximal real subfields of cyclotomic fields [3, 32] and the cyclo-multiquadratic fields (the composition of cyclotomic and multiquadratic fields) [30].

The security of the above structured lattice problems is based on our choice of f, the modulus polynomial, and the defining polynomial of the number field. A wrong choice of f could make the scheme vulnerable to attacks. We review some of the attacks that exploit these additional structures. For a more thorough survey we refer to [147].

2.5. **Cryptanalysis of RLWE/PLWE.** In this section, $R_q = \mathbb{F}_q[x]/(f(x))$ where $f(x)$ is a monic irreducible polynomial in $\mathbb{Z}[x]$ and q prime.

An attack on PLWE that exploits the algebraic structure of R_q, was first introduced by Eisenträger, Hallgren, and Lauter in [78]. Let α be a root of $f(x)$ i.e $f(\alpha) = 0 \mod q$. They showed that when $\alpha = 1$, an attacker, given arbitrary PLWE samples $(a_i, b_i) \in R_q^2$, can efficiently distinguish them from uniform samples. In the same work, they extended this idea to the case where α has a *small multiplicative order* $r \mod q$. Later, Elias, Lauter, Özman, and Stange [80], further constructed a distinguishing attack on PLWE when α has a *small residue*.

Building on these root-based attacks, the authors of [28] constructed a similar attack that makes use of the number-theoretic properties of the trace function without requiring the order of the root to be small. Specifically, they show that if $f(x)$ has a quadratic factor whose root has trace zero, then the adversary can identify whether the given samples are uniform or PLWE. This idea was subsequently generalized in [29], which extended the result from quadratic factors to factors of higher degree: it showed that if $f(x)$ contains a factor of the form $x^n + \rho$, where ρ is an element such that the root has trace zero, then a similar distinguishing attack applies. Furthermore, using a similar strategy of exploiting roots with trace

zero, another attack was designed in [17] on PLWE over a subring $R_{q,0} \times R_q$ of a cyclotomic field, where the integer modulus q does not split completely.

Another attack proposed in [78] and addressed in [13] is the smearing attack. This distinguishing attack is performed by analyzing the behavior of the error to distinguish them from uniform samples.

The natural question that arises is: can some of these attacks on PLWE be extended to RLWE? This question has been answered in the affirmative for some. A natural step in this direction will be to transform RLWE samples into PLWE (see Equation (11)) and then apply one of the listed attacks to the PLWE samples. In [80], the authors demonstrate how the attack described in [78] can be applied to the RLWE decision problem, given that some conditions are satisfied. This result was later extended in [47] to the RLWE search problem, achieving 100% success probability with fewer samples.

It is worth mentioning that these known attacks do not threaten the NIST-standardized schemes. However, these attacks confirm why we should stick to the parameters of the standardized schemes. They also provide a list of parameters to watch for when constructing new schemes or improving standardized ones.

2.6. **Further applications of lattice-based cryptography.** One interesting property of lattice-based cryptographic (LBC) schemes is their flexibility, which enables them to be applied across a wide range of applications. We briefly describe two notable examples below: homomorphic encryption and private information retrieval (PIR). We conclude this section by highlighting the new standardized schemes based on lattices.

Homomorphic encryption. This is a form of encryption that allows computations to be done on encrypted data without decrypting it. The decrypted result matches the result of the same operation performed on the original plain data. There are three main types: partially homomorphic encryption (PHE), which allows for a single type of operation (either addition or multiplication) on encrypted data; somewhat homomorphic encryption (SHE), which allows for a limited, but greater than one, number of operations on encrypted data; and fully homomorphic encryption (FHE), which allows for an unlimited number of either of the two operations. Homomorphic encryption plays an important role in, e.g., cloud computing, secure voting, and medical data analysis.

The problem of constructing a fully homomorphic encryption scheme was first introduced by Rivest, Adleman, and Dertouzos in 1978 [161]. For more than three decades, the existence of a solution remained an open problem. During this period, partial homomorphic schemes like RSA [162] and ElGamal [79] enabled unlimited modular multiplications, while others allowed for unlimited modular arithmetic [154], [26].

Gentry, in [100], [101] gave the first construction of an FHE scheme based on lattice-based cryptography. This FHE scheme supports both addition and multiplication operations on ciphertext, for an arbitrary number of computations. To achieve this, he starts from a somewhat homomorphic encryption scheme, which has limitations due to the noise growth when we add or multiply encrypted data. This noise growth may lead to decryption errors if the noise becomes too high. Addressing this, he shows that in any bootstrapped scheme, this SHE scheme can be converted into an FHE scheme. The security of this scheme is partly based on

worst-case problems over ideal lattices. Furthermore, in [43], this result is extended by removing the ideal lattice condition. Over the years, other schemes based on lattice-based problems have been proposed that offer improved efficiency.

One of the well known applications of homomorphic encryption is the single-database computationally-Private Information Retrieval (cPIR), which we introduce below.

Private information retrieval (PIR) Introduced by Chor *et al.* in [51], PIR allows a user to retrieve an item from a storage system or cloud in possession of a database without revealing which item is retrieved. The main idea is as follows: given a system holding a database consisting of a set of elements $D_1, \ldots, D_m$, retrieve the ith element D_i without revealing i to the system owner. A naive solution will be to retrieve the entire database and discard all entries but the one of interest. However, this will be at a cost proportional to the number of data items $O(m)$, and therefore not practical when the database is large. It has been shown that this is the only way to guarantee information-theoretic privacy if we store the database on one server. However, using *multi-server schemes* we can do much better. Here, the user sends masked queries to different non-colluding servers, ensuring that no subset of servers of size below a design threshold learns the original query. The methods utilized in this approach typically draw from coding theory, and various extensions to the problem have been made. The literature is vast and as our core topic is lattices, we refrain from expanding our reference list by these coding-theoretic works and simply refer to the brief tutorial [77] and the references therein.

Another way is to only use a single server but instead rely on computational security and hence cryptographic techniques to hide the query from the server, originally introduced in [115] where a scheme based on quadratic residues was constructed. This method is generally known as *single-server computationally private information retrieval (cPIR).* The drawback of the original cPIR scheme is that it is computationally more expensive than the naive method of downloading everything and therefore not practical [115]. This aspect has later been improved by several works, notably in [1] where, using LBC, much more efficient cPIR schemes based on LWE and RLWE were constructed.

NIST standardized schemes. Due to the fast progress in the field of quantum computing, the National Institute of Standards and Technology (NIST) launched a PQC standardization process (competition) in 2016 aimed at identifying quantum-safe cryptographic protocols. A call for proposals [139] was made in which researchers were invited to submit candidates which were evaluated at several rounds based criteria that included security, efficiency, and practical implementation. A total of 82 algorithms were submitted, of which 69 were accepted into the first round[140], 26 advanced to the second round [141], and 15 selected as third round finalist [142]. Of these candidates, 4 was chosen for standardization [143] and the rest moved to the fourth round [144] and are currently undergoing further analysis. Among the four schemes chosen for standardization, CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium (ML-DSA), and Falcon are based on hard lattice-problems. In particular, Kyber and Dilithium are based on hard problems over module lattices [11] such as MLWE. It is worth noting that the above listed attacks on RLWE/PLWE do not threaten any of these standardized schemes.

3. Lattice codes for wireless security

In the previous section, we have seen how lattices can be applied to provide computational security due to several hard lattice problems, such as the shortest vector problem. In addition to computational security where we assume that the adversary has bounded computational resources, lattices can also be used to provide *physical layer security* (PLS), which for its part relies on the concept of *information-theoretic security*. Here, the adversary can have unlimited computational power, since the security is based on (full or partial) lack of relevant information.

While traditional cryptographic methods like AES (the Advanced Encryption Standard) or RSA operate at higher protocol layers, PLS provides a complementary layer of defense. As the 6th generation (6G) communication networks move toward high-mobility, low-latency, and decentralized networks (e.g., Internet of Vehicles), traditional key exchange mechanisms can become bottlenecks. Lattice-based PLS offers a way to establish security guarantees by leveraging the intrinsic physical properties of the wireless medium, making it a vital research area for future secure communication systems against both classical and potential quantum threats. We refer to the recent white paper [53] for a general introduction to the utility of physical layer security.

Let us start by defining relevant notions in information theory.

3.1. Basic notions in information theory and related security paradigms.

For a general reference for information theory and information-theoretic security, we refer to [60, 31]. Let X and Y be two discrete random variables taking values from respective sets $\mathcal{X}$ and $\mathcal{Y}$. The *entropy* of X is

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log p(x),$$

where $p(x)$ is the probability of x. The entropy of a continuous random variable is defined analogously.

Let us denote the conditional entropy of X given Y by $H(X|Y)$. The *mutual information* can then be defined as

$$I(X;Y) = H(X) - H(X|Y).$$

Assume now that we are sending a message X and the adversary is gaining access to Y. The secrecy can be measured by how much information can be obtained based on Y, quantized by *information leakage* $I(X;Y)$. The mutual information is zero, yielding *perfect secrecy*, if and only if X and Y are independent. In cryptography, typically operating over positive characteristic and finite structures, this can be achieved by adding uniformly random noise to X, referred to as one-time pad. On a wireless (physical) channel, however, the noise is not *selected* by the user as in cryptography but is *induced* by the physical conditions of the channel and the equipment used and as such largely beyond our control. Such noise is typically real or complex Gaussian, and we cannot (non-asymptotically) obtain perfect secrecy anymore. Instead, the goal in physical layer security is to minimize information leakage while guaranteeing good decoding probability for the legitimate user. This will be our focus in the rest of this section. We refer the interested reader to [151, 24, 52, 58] and references therein for more details on lattice-based reliable and secure wireless communications.

3.2. **Wiretap channels and lattice coset codes.** Lattice codes, defined as finite collections of lattice vectors within a bounding region, are effective tools for wireless communications. The channel model for single-input single-output (SISO) is described as

$$\mathbf{y} = H\mathbf{x} + \mathbf{n} \in \mathbb{R}^n,$$

where $\mathbf{x} \in L$ is the message, $\mathbf{n} \in \mathbb{R}^n$ is additive white Gaussian noise (AWGN), and $H \in \mathbb{R}^{n\times n}$ represents random fading. For an *AWGN channel*, $H = I_n$, while for a *Rayleigh fast fading channel*, H is a diagonal matrix with independent Rayleigh distributed entries. Maximum-likelihood (ML) decoding here is equivalent to the closest vector problem in a (distorted) lattice. This may sound counter-intuitive after the previous section on lattice-based cryptography, where it was pointed out that many lattice problems, including the CVP, are computationally hard. Fortunately for us, now the security is based on information-theoretic notions, not on computational hardness. This means that, in practice, we can resort to relatively low-dimensional lattices making the CVP feasible for the legitimate receiver. However, in order to approach the theoretical perfect secrecy capacity [149], high-dimensional lattices are still needed.

In a channel with not too much fading and noise with respect to the signal power, measured by *signal-to-noise ratio (SNR)*, reliability is optimized by maximizing the *modulation diversity* $\ell := \min_{0\neq\mathbf{x}\in L} |\{i : x_i \neq 0\}|$ and the *minimum product distance*

$$d_{p,min}(L) := \inf_{0\neq\mathbf{x}\in L} \prod_{i=1}^{n} |x_i|$$

for a full diversity lattice ($\ell = n$) [151]. At low SNR, the minimum distance $\lambda_1(L)$ dominates the decoding performance. Note that the minimum product distance coincides with the multiplicative norm defined in 1.

Wyner's coset coding, introduced by Aaron Wyner in 1975 [185, 153] for the *wiretap channel*[3], is a foundational technique in information-theoretic security that achieves secure communication without relying on unproven computational assumptions or shared cryptographic keys. The original core mechanism involves partitioning a standard error-correcting code into distinct, non-overlapping subsets, *i.e.*, (cosets), where each coset corresponds to a specific secret message. To transmit a message, the sender selects the appropriate coset and deliberately introduces structured randomness by transmitting a randomly chosen codeword from the coset. This approach is useful in physical-layer security as it exploits the differences in the channel quality between the legitimate user and an eavesdropper. A legitimate receiver with a stronger channel (*i.e.*, lower noise) can successfully decode to identify the correct coset and recover the message, while an eavesdropper on a noisier channel is overwhelmed by the errors. Due to the random codeword selection, the eavesdropper's degraded signal lacks enough information to even determine which coset was used, mathematically ensuring that the intercepted data reveals (practically) zero information about the original message regardless of the attacker's computing power. We refer to [126, Ch. 3] and the references therein for a nice exposition on coset codes and wiretap channels for error-correcting codes, as well as their intimate connection to *(homomorphic) secret sharing*.

[3]Here, in addition to the legitimate receiver, we have an eavesdropper who is "tapping the wire" in order to intercept secret messages. With slight abuse of language, we also call a wireless channel with an eavesdropper a wiretap channel, even though there is no wire.

In our lattice code context, instead of quotients of vector spaces we consider quotients of lattices, both of which have an analogous additive group structure. A message $\mathbf{m}$ is masked by a random sublattice vector $\mathbf{r} \in L_s \subset L$, and $\mathbf{x} = \mathbf{m} + \mathbf{r} \in L/L_s$ is transmitted. Again, assuming the eavesdropper experiences relatively stronger noise, the legitimate receiver decodes reliably while the eavesdropper gains negligible information. For more details and examples, we refer to [150].

Next, let us make the "negligible information" more rigorous.

3.3. **The flatness factor and connections to theta functions.** The *flatness factor* $\mathcal{E}_L(\sigma)$ bounds from above the deviation of the lattice Gaussian g_σ from uniformity on the Voronoi cell $\mathcal{V}(L)$ (cf. variational distance, Eq. (9)):

$$\mathcal{E}_L(\sigma) := \max_{\mathbf{x}\in\mathcal{V}(L)} \left| \frac{g_{\sigma,L}(\mathbf{x})}{1/\operatorname{Vol}(L)} - 1 \right|. \tag{12}$$

The flatness factor bounds from above both the eavesdropper's correct decoding probability and information leakage [120, 121, 66], and minimizing it makes the channel appear "flatter" (more uniform) to the eavesdropper.

The flatness factor can be related to the primal and dual theta series (via the Poisson summation formula) as follows:

$$\begin{aligned} & \operatorname{Vol}(L) g_{\sigma,L}(\boldsymbol{x}) - 1 \\ \leq\ & \operatorname{Vol}(L) g_{\sigma,L}(0) - 1 \\ =\ & \frac{\operatorname{Vol}(L)}{(\sqrt{2\pi}\sigma)^n} \Theta_L(e^{-1/2\sigma^2}) - 1 \\ =\ & \Theta_{L^*}(e^{-2\pi\sigma^2}) - 1 \\ =\ & \mathcal{E}_L(\sigma) \end{aligned} \tag{13}$$

where σ^2 is the noise variance.

A practical complication now arises. Namely, if we want to compare different lattices (of the same volume) and compare their flatness factors, how do we efficiently compute the theta function, known to be notoriously hard? In a relatively low dimension, one can use truncations and brute force point enumeration or, more efficiently, resort to the theta function approximation proposed in [19]. However, as mentioned by the authors, the approximation is not universally good and gets worse with growing dimension or if the lattice is very skewed.

To make a connection to lattice-based cryptography, we point out that the flatness factor and the smoothing parameter (cf. Eq. (10)) are closely related [120]. To this end, let us slightly redefine the smoothing parameter up to constants by changing the variable s to $\sigma = s/\sqrt{2\pi}$:

$$\eta_\delta(L) = \inf\{\sigma > 0 \,|\, \sum_{0\neq\lambda\in\Lambda^*} e^{-2\pi^2\sigma^2||\lambda||^2} \leq \delta\}.$$

Then we have

$$\mathcal{E}_L(\eta_\delta(L)) = \delta.$$

Essentially, if we compare two lattices (of the same volume), the one with the smaller flatness factor allows for adding smaller noise while maintaining the same variational distance, helping the correct decoding/decryption of the legitimate receiver.

3.4. **Well-rounded lattices as theta minimizers.** Well-rounded lattices were studied and constructed for the SISO wiretap channel in [103, 64]. Interestingly, it has been shown that the minimizer of the flatness factor is well-rounded [66]. Since they also maximize the minimum product distance [63] and support dense packings [166, 59, 70], WR lattices are excellent candidates for secure, reliable communication. As minimizing the theta function globally is difficult, [109] focused on generic WR lattices — increasing the first minimum and decreasing the kissing number reduces the dominating term, motivating the study of dense GWR lattices for physical layer security.

3.5. **Related topics and generalizations.** Here, we have concentrated on the single-antenna channel model. For multi-antenna wireless communications, so-called *space-time lattice codes* based on *cyclic division algebras and their maximal orders* can be used [152, 168, 108, 181]. Lattice coset codes and related design criteria for such a *multiple-input multiple-output (MIMO)* wiretap channel have also been considered [137, 122]. The utility of well-rounded lattices for MIMO channels have been demonstrated in [102, 20]. Furthermore, an analogous design criterion to minimize the lattice theta series in the ℓ^1 (taxicab) norm instead of the euclidean norm was proposed in [135], and related kissing number problems in [136].

The setting of point-to-point communications can be extended to *relay channels*, where the message is relayed by an intermediate node. Lattice coset codes also come into play here via *physical layer network coding*, the security of which has been considered in [180] for the so-called compute-and-forward channels. Generalized theta series was considered in [36], motivated by connections to the identification of stable lattices, the *lattice isomorphism problem*, and the so-called isodual *secrecy gain conjecture*. The secrecy gain is closely related to the flatness factor, and measures how much better the coding lattice used is with respect to "no coding", *i.e.*, the $\mathbb{Z}^n$ lattice, by looking at the ratio of the respective theta functions called the *secrecy function* [25, 150]. Its ultimate goal is the same as that of the flatness factor minimization: to minimize the the theta function of the eavesdropper's lattice (the reader can think of this as the "noise" lattice, which is used to confuse Eve). While the flatness factor directly bounds the eavesdroppers correct decoding probability and information leakage, hence making comparison to the integer lattice obsolete, the *secrecy gain* does allow the use of somewhat different type of analytical tools by looking at the maximum of the secrecy function. For more details on the secrecy gain and various conjectures related to it, we refer to [25, 150, 83, 34]. Finally, we mention that the maximization of the flatness factor has been studied in [35].

For a more general and broader introduction to many of the topics discussed in Sections 2 and 3, we refer the reader to the following PhD theses: [62, 146, 18, 126].

4. Conclusion and open problems

In this survey, we have discussed the theory of structured Euclidean lattices and its applications — a very active area of current research. A great deal of research here is motivated by the original discrete optimization problems on lattices, such as packing, covering, and kissing number problems. This being said, the field of potential work here is much wider than suggested by these classical problems, both in terms of theory and applications. We mention here some additional directions for future work.

Minkowski conjecture has been proved in dimensions $n \leq 10$, and the related Woods' covering conjecture has been disproved in dimensions $n \geq 24$. However, it is not clear that the failure of Woods' conjecture in higher dimensions implies the failure of Minkwoski's conjecture. It would be interesting to understand whether Minkowski conjecture holds in some dimensions where Woods' conjecture fails. In addition, the question of which subclasses of lattices satisfy the Woods' conjecture either in dimensions where the question is open or for those where the general conjecture fails is intresting.

Classification of perfect and eutactic lattices is known only in low dimensions. In fact, there are not even known asymptotic formulas for the number of perfect or eutactic similarity classes of lattices in growing dimensions: the upper and lower bounds known for perfect similarity classes are of different orders of magnitude as functions of the dimension. An important avenue for future research would be to obtain stronger general bounds with a view toward asymptotic formulas.

Zeta-function of well-rounded sublattices in a fixed planar lattice was studied by several authors and its behavior is generally understood. However, there seem to be no analogous results in higher dimensions. Studying the analytic property of this function in higher dimensions would provide insight into the quantitative distribution properties of well-rounded sublattices and their dependence on the arithmetic structure of the ambient lattice.

Algebraic constructions of well-rounded lattices have received some attention in the recent years. In particular, ideal well-rounded lattices from quadratic number fields are fairly well understood. On the other hand, there are few results for number fields of higher degree. Also, constructions of well-rounded lattices from more general free $\mathbb{Z}$-modules in number fields deserve more attention as they can often display interesting properties, such as large automorphism groups. Further investigation of tame lattices is also an interesting related project.

Further constructions of lattices with special geometric properties, such as well-roundedness, stability, eutaxy, and perfection coming from function fields, graph theory, theory of tight frames and other areas of mathematics are of great interest. Connections between lattices and spherical designs is a topic of research that also naturally falls here. Continuing investigations in these directions is certainly worthwhile.

Studying the local and global extrema of theta functions and finding close-to-optimal constructions is a very natural question in mathematics and, as discussed in this survey, also motivated by applications both in lattice-based cryptography and physical layer security via the variational distance. The question of finding the precise minimum and the lattice(s) achieving it is generally very hard,

and the answer is known only in a few small dimensions. Hence, any new insight toward this goal will be valuable.

The equivalence of variants of the LWE problem such as RLWE and PLWE has been studied in the literature for some classes of number fields. These equivalence results enable the construction of cryptographic schemes with improved efficiency while maintaining strong security guarantees. Extending these results to broader classes of number fields would provide more options for designing secure and efficient protocols. This will be particularly important if the currently standardized lattice-based schemes (e.g. Kyber) would render themselves vulnerable to fatal attacks.

Analyzing the hardness of approximate versions of worst-case hard problems such as SVP and SIVP for varying approximation factors remains an important research direction. In particular, understanding the hardness of approximate SVP or SIVP over structured lattices may either strengthen the security guarantees of the newly standardized schemes or reveal potential weaknesses in their underlying hardness assumptions.

Cryptanalysis of variants of LWE has also been extensively studied in the literature. This line of research helps maintain robust security by identifying vulnerable instances before they are exploited by adversaries. Exploring the algebraic structures of the underlying schemes may reveal additional weak instances of these problems.

Constructions of explicit lattice coset codes for wireless communications under varying channel conditions and dimensions. In particular, it would be interesting to see which further lattice properties (in addition to the density, flatness factor, and product distance) may contribute toward high performance. Moreover, constructing WR lattices from cyclic division algebras and studying their properties in terms of multi-antenna communications would be useful as existing constructions thus far are scarce, especially beyond quaternion algebras.

Acknowledgments

We would like to thank Dr. Ragnar Freij-Hollanti and Prof. Russell Lai for useful discussions and helpful comments on the original manuscript.

References

[1] C. Aguilar Melchor, J. Barrier, L. Fousse, and M.-O. Killijian. XPIR : Private information retrieval for everyone. *Proceedings on Privacy Enhancing Technologies*, pages 155–174, Apr 2016.

[2] D. Aharonov and O. Regev. Lattice problems in NP ∩ coNP. *J. ACM*, 52(5):749–765, Sept. 2005.

[3] J. Ahola, I. Blanco-Chacón, W. Bolaños, A. Haavikko, C. Hollanti, and R. M. Sánchez-Ledesma. Fast multiplication and the PLWE–RLWE equivalence for an infinite family of maximal real subfields of cyclotomic fields. *Designs, Codes and Cryptography*, 93:2947–2969, 2025.

[4] M. Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108, 1996.

[5] M. Ajtai. The shortest vector problem in l2 is np-hard for randomized reductions. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 10–19, 1998.

[6] C. Alves, J. E. Strapasson, and R. R. de Araujo. On well-rounded lattices and lower bounds for the minimum norm of ideal lattices. *Arch. Math. (Basel)*, 124(2):121–130, 2025.

[7] Y. André. On nef and semistable hermitian lattices, and their behaviour under tensor product. *Tohoku Math. J. (2)*, 63(4):629–649, 2011.

[8] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *Journal of Computer and System Sciences*, 54(2):317–331, 1997.

[9] A. Ash and M. McConnell. Cohomology at infinity and the well-rounded retract for general linear groups. *Duke Math. J.*, 90(3):549–576, 1997.

[10] L. Ateş and H. Stichtenoth. A note on short vectors in lattices from function fields. *Finite Fields Appl.*, 39:264–271, 2016.

[11] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, et al. Crystals-kyber algorithm specifications and supporting documentation. *NIST PQC Round*, 2(4):1–43, 2019.

[12] M. Baake, R. Scharlau, and P. Zeiner. Well-rounded sublattices of planar lattices. *Acta Arith*, 166(4):301–334, 2014.

[13] L. Babinkostova, A. Chin, A. Kirtland, V. Nazarchuk, and E. Plotnick. The polynomial learning with errors problem and the smearing condition. *Journal of Mathematical Cryptology*, 16(1):215–232, 2022.

[14] R. Bacher. Constructions of some perfect integral lattices with minimum 4. *J. Théor. Nombres Bordeaux*, 27(3):655–687, 2015.

[15] R. Bacher. On the number of perfect lattices. *J. Théor. Nombres Bordeaux*, 30(3):917–945, 2018.

[16] R. Baraniuk, S. Dash, and R. Neelamani. On nearly orthogonal lattice bases. *SIAM J. Discrete Math.*, 21(1):199–219, 2007.

[17] B. Barbero-Lucas, I. Blanco-Chacón, R. Durán-Díaz, R. Y. N. Nchiwo, and R. M. Sánchez-Ledesma. Cryptanalysis of PLWE based on zero-trace quadratic roots. *Accepted for publication in Journal of Mathematical Cryptology*, 2026.

[18] A. Barreal. *Lattice Codes for Physical Layer Communications*. PhD thesis, Aalto University publication series Doctoral Theses, 71/2017, 2017.

[19] A. Barreal, M. T. Damir, R. Freij-Hollanti, and C. Hollanti. An approximation of theta functions with applications to communications. *SIAM Journal on Applied Algebra and Geometry*, 4(4):471–501, 2020.

[20] A. Barreal, A. Karrila, D. A. Karpuk, and C. Hollanti. Information bounds and flatness factor approximation for fading wiretap MIMO channels. In *IEEE International Telecommunications Networks and Applications Conference*, pages 277–282, 2016.

[21] S. C. Batson. The linear transformation that relates the canonical and coefficient embeddings of ideals in cyclotomic integer rings. *Int. J. Number Theory*, 13(9):2277–2297, 2017.

[22] E. Bayer-Fluckiger. Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 168–184. Cambridge Univ. Press, Cambridge, 2002.

[23] E. Bayer-Fluckiger and G. Nebe. On the euclidean minimum of some real number fields. *J. Théor. Nombres Bordeaux*, 17(2):437–454, 2005.

[24] J.-C. Belfiore and F. Oggier. Lattice code design for the Rayleigh fading wiretap channel. In *2011 IEEE International Conference on Communications Workshops (ICC)*, pages 1–5, 2011.

[25] J.-C. Belfiore and F. E. Oggier. Secrecy gain: A wiretap lattice code design. *2010 International Symposium On Information Theory and Its Applications*, pages 174–178, 2010.

[26] J. Benaloh. Dense probabilistic encryption. In *Proceedings of the Workshop on Selected Areas in Cryptography (SAC)*, 1994.

[27] I. Blanco-Chacón. On the RLWE/PLWE equivalence for cyclotomic number fields. *Applicable Algebra in Engineering, Communication and Computing*, 33(1):53–71, 2022.

[28] I. Blanco-Chacón, B. Barbero-Lucas, R. Durán-Díaz, and R. Y. Njah Nchiwo. Trace-based cryptanalysis of cyclotomic $R_{q,0} \times R_q$-PLWE for the non-split case. *Communications in Mathematics*, 31, 2023.

[29] I. Blanco Chacón, R. Durán Díaz, and R. Martín Sánchez-Ledesma. A generalized approach to root-based attacks against PLWE. *Cryptography and Communications*, pages 1–45, 2025.

[30] I. Blanco-Chacón, A. Pedrouzo-Ulloa, R. Y. Njah Nchiwo, and B. Barbero-Lucas. Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields. *Cryptography and Communications*, pages 1–35, 2025.

[31] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer. An overview of information-theoretic security and privacy: Metrics, limits and applications. *IEEE Journal on Selected Areas in Information Theory*, 2(1):5–22, 2021.

[32] W. Bolaños, A. Haavikko, and R. M. Sánchez-Ledesma. A fast multiplication algorithm and RLWE-PLWE equivalence for the maximal real subfield of the $2^r p^s$-th cyclotomic field. *Advances in Mathematics of Communications*, 21:212–238, 2026.

[33] W. Bolaños and G. Mantilla-Soler. The trace form over cyclic number fields. *Canad. J. Math.*, pages 1–23, 2020.

[34] M. Bollauf, H.-Y. Lin, and O. Ytrehus. Secrecy gain of formally unimodular lattices from codes over the integers modulo 4. *IEEE Transactions on Information Theory*, 2024.

[35] M. F. Bollauf and H.-Y. Lin. On the maximum flatness factor over unimodular lattices. *arXiv preprint arXiv:2403.16932*, 2024.

[36] M. F. Bollauf and H.-Y. Lin. Generalized theta series of a lattice. In *2025 IEEE Information Theory Workshop (ITW)*, pages 827–832, 2025.

[37] A. Bondarenko, D. Radchenko, and M. Viazovska. Optimal asymptotic bounds for spherical designs. *Ann. of Math. (2)*, 178(2):443–452, 2013.

[38] A. Böttcher, S. Eisenbarth, L. Fukshansky, S. R. Garcia, and H. Maharaj. Spherical 2-designs and lattices from abelian groups. *Discrete Comput. Geom.*, 61(1):123–135, 2019.

[39] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. On lattices generated by finite abelian groups. *SIAM J. Discrete Math.*, 29(1):382–404, 2015.

[40] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj. Lattices from hermitian function fields. *J. Algebra*, 447:560–579, 2016.

[41] A. Böttcher, L. Fukshansky, S. R. Garcia, H. Maharaj, and D. Needell. Lattices from equiangular tight frames. *Linear Algebra Appl.*, 510:395–420, 2016.

[42] K. Boudgoust, C. Jeudy, A. Roux-Langlois, and W. Wen. On the hardness of module learning with errors with short distributions. *Journal of Cryptology*, 36(1), 2023.

[43] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

[44] Z. Brakerski and V. Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Annual cryptology conference*, pages 505–524. Springer, 2011.

[45] B. Casselman. Stability of lattices and the partition of arithmetic quotients. *Asian J. Math.*, 8:607–637, 2004.

[46] J. W. S. Cassels. On a problem of Rankin about the Epstein zeta-function. *Proc. Glasgow Math. Assoc.*, 4:73–80 (1959), 1959.

[47] W. Castryck, I. Iliashenko, and F. Vercauteren. Provably weak instances of ring-LWE revisited. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 147–167. Springer, 2016.

[48] H. Chen and L. Xu. Counterexamples to the Woods conjecture in dimensions $d \geq 24$. *J. Théor. Nombres Bordeaux*, 31(3):723–726, 2019.

[49] Y. X. Chew and F. Oggier. Well-rounded ideal lattices from totally definite quaternion algebras, 2025.
[50] D. P. Chi, J. W. Choi, J. San Kim, and T. Kim. Lattice based cryptography for beginners. *Cryptology ePrint Archive*, 2015.
[51] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan. Private information retrieval. *J. ACM*, 45(6):965–981, nov 1998.
[52] A. Chorti, C. Hollanti, J. Belfiore, and H. Poor. *Physical layer security: A paradigm shift in data confidentiality*, volume 358 of *Springer Lecture Notes in Electrical Engineering*, pages 1–15. Springer, 2016.
[53] A. Chorti, S. Tomasin, M. Baldi, S. Delbruel, and G. Karabulut Kurt (editors). 2025 working group white paper, security and privacy. `https://futurenetworks.ieee.org/roadmap/physical-layer-security-focus-group`, 2025. IEEE Focus Group on Physical Layer Security, International Networks Generations Roadmap (INGR).
[54] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. S. Viazovska. The sphere packing problem in dimension 24. *Ann. of Math. (2)*, 185(3):1017–1033, 2017.
[55] P. E. Conner and R. Perlis. *A Survey of Trace Forms of Algebraic Number Fields*. World Scientific, 1984.
[56] J. H. Conway and N. J. A. Sloane. A lattice without a basis of minimal vectors. *Mathematika*, 42(1):175–177, 1995.
[57] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups*. Springer-Verlag, Third edition, 1999.
[58] S. I. Costa, F. Oggier, A. Campello, J.-C. Belfiore, and E. Viterbo. *Lattices Applied to Coding for Reliable and Secure Communications*. Springer, 2017.
[59] R. Coulangeon. Spherical designs and zeta functions of lattices. *Int. Math. Res. Not.*, pages Art. ID 49620, 16, 2006.
[60] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Ltd, 2005.
[61] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang. A survey of post-quantum cryptography: Start of a new race. *Cryptography*, 7(3):40, 2023.
[62] M. T. Damir. *Well-Rounded Lattices and Applications to Physical Layer Security*. PhD thesis, Aalto University publication series Doctoral Theses, 160/2020, 2020.
[63] M. T. Damir and L. Fukshansky. Canonical basis twists of ideal lattices from real quadratic number fields. *Houston J. Math.*, 45(4):999–1019, 2019.
[64] M. T. Damir, O. Gnilke, L. Amorós, and C. Hollanti. Analysis of some well-rounded lattices in wiretap channels. In *IEEE Int. Workshop on Signal Process. Adv. in Wireless Commun.*, pages 1–5, 2018.
[65] M. T. Damir and D. Karpuk. Well-rounded twists of ideal lattices from real quadratic fields. *J. Number Theory*, 196:168–196, 2019.
[66] M. T. Damir, A. Karrila, L. Amoros, O. W. Gnilke, D. Karpuk, and C. Hollanti. Well-rounded lattices: towards optimal coset codes for Gaussian and fading wiretap channels. *IEEE Trans. Inform. Theory*, 67(6):3645–3663, 2021. part 2.
[67] M. T. Damir and G. Mantilla-Soler. Bases of minimal vectors in tame lattices. *Acta Arith*, 205:265–285, 2022.
[68] R. R. de Araujo and S. I. R. Costa. Well-rounded algebraic lattices in odd prime dimension. *Arch. Math. (Basel)*, 112(2):139–148, 2019.
[69] R. R. de Araujo, A. de Andrade, T. d. Nóbrega Neto, and J. Bastos. Constructions of well-rounded algebraic lattices over odd prime degree cyclic number fields. *Commun. Math.*, 33(1), 2025. Paper No. 6. 18 pp.
[70] B. N. Delone and S. S. Ryshkov. A contribution to the theory of the extrema of a multidimensional ζ-function. *Doklady Akademii Nauk*, 173(5):991–994, 1967.
[71] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6(3):363–388, 1977.
[72] A. J. Di Scala, C. Sanna, and E. Signorini. RLWE and PLWE over cyclotomic fields are not equivalent. *Applicable Algebra in Engineering, Communication and Computing*, 35(3):351–358, 2024.
[73] P. H. Diananda. Notes on two lemmas concerning the Epstein zeta-function. *Proc. Glasgow Math. Assoc.*, 6:202–204 (1964), 1964.

[74] W. Diffie and M. E. Hellman. *New Directions in Cryptography*, pages 365–390. Association for Computing Machinery, New York, NY, USA, 1 edition, 2022.
[75] I. Dinur, G. Kindler, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 99–109. IEEE, 1998.
[76] L. Ducas and A. Durmus. Ring-LWE in polynomial rings. In *International Workshop on Public Key Cryptography*, pages 34–51. Springer, 2012.
[77] R. G. L. D'Oliveira and S. E. Rouayheb. A guided walk through coded private information retrieval. *IEEE BITS the Information Theory Magazine*, 3(4):51–66, 2023.
[78] K. Eisenträger, S. Hallgren, and K. Lauter. Weak instances of PLWE. In *International Conference on Selected Areas in Cryptography*, pages 183–194. Springer, 2014.
[79] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology – CRYPTO 1984*, pages 10–18, 1985.
[80] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. Provably weak instances of Ring-LWE. In *Annual Cryptology Conference*, pages 63–92. Springer, 2015.
[81] V. Ennola. A lemma about the Epstein zeta-function. *Proc. Glasgow Math. Assoc.*, 6:198–201 (1964), 1964.
[82] V. Ennola. On a problem about the Epstein zeta-function. *Proc. Cambridge Philos. Soc.*, 60:855–875, 1964.
[83] A.-M. Ernvall-Hytönen and B. A. Sethuraman. Counterexample to the generalized Belfiore-Solé secrecy function conjecture for l-modular lattices. *IEEE Transactions on Information Theory*, 62(8):4514–4522, 2016.
[84] L. Fukshansky. Well-rounded zeta-function of planar arithmetic lattices. *Proc. Amer. Math. Soc.*, 142(2):369–380, 2014.
[85] L. Fukshansky. Stability of ideal lattices from quadratic number fields. *Ramanujan J.*, 37(2):243–256, 2015.
[86] L. Fukshansky, P. Guerzhoy, and S. Kühnlein. On sparse geometry of numbers. *Res. Math. Sci.*, 8(1), 2021. Paper No. 2. 18 pp.
[87] L. Fukshansky, P. Guerzhoy, and F. Luca. On arithmetic lattices in the plane. *Proc. Amer. Math. Soc.*, 145(4):1453–1465, 2017.
[88] L. Fukshansky, P. Guerzhoy, and T. Nielsen. Deep hole lattices and isogenies of elliptic curves. *Res. Number Theory*, 10(2), 2024. Paper No. 33. 12 pp.
[89] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices ii. *Int. J. Number Theory*, 9(1):139–154, 2013.
[90] L. Fukshansky and C. Hollanti. Euclidean lattices: theory and applications. *Commun. Math.*, 31(2):251–263, 2023.
[91] L. Fukshansky and E. Knight. On lattices generated by algebraic conjugates. in preparation.
[92] L. Fukshansky and D. Kogan. On the geometry of nearly orthogonal lattices. *Linear Algebra Appl.*, 629:112–137, 2021.
[93] L. Fukshansky and D. Kogan. Cyclic and well-rounded lattices. *Mosc. J. Comb. Number Theory*, 11(1):79–96, 2022.
[94] L. Fukshansky and H. Maharaj. Lattices from elliptic curves over finite fields. *Finite Fields Appl.*, 28:67–78, 2014.
[95] L. Fukshansky, D. Needell, J. Park, and Y. Xin. Lattices from tight frames and vertex transitive graphs. *Electron. J. Combin.*, 26(3), 2019. Paper No. 3.49. 30pp.
[96] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.
[97] L. Fukshansky and S. Robins. Frobenius problem and the covering radius of a lattice. *Discrete Comput. Geom.*, 37(3):471–483, 2007.
[98] L. Fukshansky and X. Sun. On the geometry of cyclic lattices. *Discrete Comput. Geom.*, 52(2):240–259, 2014.
[99] L. Fukshansky and X. Sun. Erratum to: On the geometry of cyclic lattices. *Discrete Comput. Geom.*, 53(4):971–972, 2015.
[100] C. Gentry. *A Fully Homomorphic Encryption Scheme*. PhD thesis, Stanford University, 2009.
[101] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.

[102] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. A. Karpuk, and C. Hollanti. Well-rounded lattices for coset coding in MIMO wiretap channels. In *Proc. IEEE International Telecommunication Networks and Applications Conference (ITNAC)*, pages 289–294, 2016.

[103] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti. Well-rounded lattices for reliability and security in Rayleigh fading SISO channels. In *Proc. IEEE Information Theory Workshop*, pages 359–363, 2016.

[104] O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 1–9, New York, NY, USA, 1998. Association for Computing Machinery.

[105] P. M. Gruber. *Convex and Discrete Geometry*. North-Holland, Publishing Co, 1987.

[106] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. Grundlehren der mathematischen Wissenschaften. 336. Springer, Berlin, 2007.

[107] T. Hales and S. Ferguson. *The Kepler conjecture. The Hales-Ferguson proof. Including papers reprinted from Discrete Comput. Geom. 36 (2006), no. 1. Edited by Jeffrey C. Lagarias*. Springer, New York, 2011.

[108] C. Hollanti, J. Lahtonen, and H.-f. Lu. Maximal orders in the design of dense space-time lattice codes. *IEEE Transactions on Information Theory*, 54(10):4493–4510, 2008.

[109] C. Hollanti, G. Mantilla-Soler, and N. Miller. Dense generic well-rounded lattices. *SIAM J. Appl. Algebra Geom.*, 9(1):154–185, 2025.

[110] L. Ji. Well-rounded equivariant deformation retracts of teichmüller spaces. *Enseign. Math.*, 60(1-2):109–129, 2014.

[111] L. Kathuria and M. Raka. On conjectures of Minkowski and Woods for n=10. In *Proc. Indian Acad. Sci. Math. Sci.*, Paper No. 45 , 2022, 2022. 132(2). 27 pp.

[112] Y. Kim. On semistability of perfect lattices. *Alabama Journal of Mathematics*, 39, 2015.

[113] B. Klartag. Lattice packing of spheres in high dimensions using a stochastically evolving ellipsoid. *arXiv:2504.05042*, 2025.

[114] S. Kühnlein. Well-rounded sublattices. *Int. J. Number Theory*, 8(5):1133–1144, 2012.

[115] E. Kushilevitz and R. Ostrovsky. Replication is not needed: single database, computationally-private information retrieval. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 364–373, 1997.

[116] F. Ladisch. Lattices of finite abelian groups. *Discrete Comput. Geom.*, 65(3):938–951, 2021.

[117] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

[118] N. H. Le, D. T. Tran, and H. T. N. Tran. Well-rounded ideal lattices of cyclic cubic and quartic fields. *Commun. Math.*, 31(2):209–250, 2023.

[119] M. Levin, U. Shapira, and B. Weiss. Closed orbits for the diagonal group and well-rounded lattices. *Groups Geom. Dyn.*, 10(4):1211–1255, 2016.

[120] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé. Semantically secure lattice codes for the Gaussian wiretap channel. *IEEE Transactions on Information Theory*, 60(10):6399–6416, 2014.

[121] L. Luzzi, R. Vehkalahti, and C. Ling. Almost universal codes for fading wiretap channels. In *IEEE Int. Symp. Inf. Theory*, 2016.

[122] L. Luzzi, R. Vehkalahti, and C. Ling. Almost universal codes for MIMO wiretap channels. *IEEE Transactions on Information Theory*, 64(11):7218–7241, 2018.

[123] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. automata, languages and programming. In I. I. Part, editor, *Lecture Notes in Comput. Sci., 4052*, pages 144–155. Springer, Berlin, 2006.

[124] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 1–23. Springer, 2010.

[125] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-LWE cryptography. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 35–54. Springer, 2013.

[126] O. Makkonen. *Algebraic methods for secure coded computing*. PhD thesis, Aalto University publication series Doctoral Theses, 195/2025, 2025.

[127] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.

[128] J. Martinet. Bases of minimal vectors in lattices. i. *Arch. Math. (Basel)*, 89(5):404–410, 2007.

[129] J. Martinet. Bases of minimal vectors in lattices. ii. *Arch. Math. (Basel)*, 89(6):541–551, 2007.
[130] J. Martinet and A. Schürmann. Bases of minimal vectors in lattices. iii. *Int. J. Number Theory*, 8(2):551–567, 2012.
[131] C. T. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.
[132] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM journal on Computing*, 30(6):2008–2035, 2001.
[133] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complexity*, 16(4):365–411, 2007.
[134] D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.
[135] N. Miller. A design criterion for the rayleigh fading wiretap channel based on ℓ^1-norm theta functions. *SIAM Journal on Applied Algebra and Geometry*, 9(3):682–706, 2025.
[136] N. Miller. On the kissing number of the cross-polytope. `https://arxiv.org/abs/2501.09245`, 2025.
[137] H. Mirghasemi and J.-C. Belfiore. Lattice code design criterion for MIMO wiretap channels. In *2015 IEEE Information Theory Workshop (ITW)*, pages 277–281, 2015.
[138] O. Musin. The kissing number in four dimensions. *Ann. of Math. (2)*, 168(1):1–32, 2008.
[139] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization. `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf`, 2016. Accessed: 2026-03-26.
[140] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization round 1 submission. `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions`, 2017. Accessed: 2026-03-26.
[141] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization round 2 submission. `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions`, 2017. Accessed: 2026-03-26.
[142] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization round 3 submission. `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions`, 2021. Accessed: 2026-03-26.
[143] National Institute of Standards and Technology (NIST). NIST announces first group of cryptographic algorithms for post-quantum cryptography standardization. `https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms`, 2022. Accessed: 2025-01-17.
[144] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization round 4 submission. `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-4-submissions`, 2022. Accessed: 2026-03-26.
[145] G. Nebe. Boris Venkov's theory of lattices and spherical designs. In *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, volume 587 of *Contemp. Math.*, pages 1–19. Amer. Math. Soc., Providence, RI, 2013.
[146] R. Y. Njah Nchiwo. *Algebraic number theory and lattice based cryptography: equivalence and cryptanalysis of RLWE and PLWE*. PhD thesis, Aalto University publication series Doctoral Theses, 147/2026, 2026.
[147] R. Y. Njah Nchiwo. Cryptanalysis of polynomial learning with errors (PLWE): A survey. *Accepted for publication in Springer "Association for Women in Mathematics Series"*, 2026.
[148] E. Nossek. Spherical designs and lattices. *Beitr. Algebra Geom.*, 55(1):25–31, 2014.
[149] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Transactions on Information Theory*, 57(8):4961–4972, 2011.
[150] F. Oggier, P. Solé, and J. Belfiore. Lattice codes for the wiretap Gaussian channel: Construction and analysis. *IEEE Transactions on Information Theory*, 62(10):5690–5708, 2016.

[151] F. Oggier and E. Viterbo. *Algebraic Number Theory and Code Design for Rayleigh Fading Channels*, volume 1(3) of *Foundations and Trends in Communications and Information Theory*. Now Publisher Inc., 2004.

[152] F. E. Oggier, J.-C. Belfiore, and E. Viterbo. Cyclic division algebras: A tool for space-time coding. *Found. Trends Commun. Inf. Theory*, 4:1–95, 2007.

[153] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. *AT&T Bell Laboratories technical journal*, 63(10):2135–2157, 1984.

[154] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT*, pages 223–238, 1999.

[155] A. Pettet and J. Souto. Minimality of the well-rounded retract. *Geom. Topol.*, 12(3):1543–1556, 2008.

[156] R. A. Rankin. A minimum problem for the Epstein zeta-function. *Proc. Glasgow Math. Assoc.*, 1:149–158, 1953.

[157] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[158] O. Regev. The learning with errors problem (invited survey). In *Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity*, pages 191–204, 2010.

[159] O. Regev, U. Shapira, and B. Weiss. Counterexamples to a conjecture of woods. *Duke Math. J.*, 166(13):2443–2446, 2017.

[160] C. Riener. On extreme forms in dimension 8. *J. Théor. Nombres Bordeaux*, 18(3):677–682, 2006.

[161] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

[162] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[163] M. Rosca, D. Stehlé, and A. Wallet. On the ring-LWE and polynomial-LWE problems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 146–173. Springer, 2018.

[164] M. Y. Rosenbloom and M. A. Tsfasman. Multiplicative lattices in global fields. *Invent. Math.*, 101:687–696, 1990.

[165] S. S. Ryškov. On the question of the final ζ-optimality of lattices that yield the densest packing of n-dimensional balls. *Sibirsk. Mat. Ž.*, 14:1065–1075, 1158, 1973.

[166] P. Sarnak and A. Strömbergsson. Minima of Epstein's zeta function and heights of flat tori. *Invent. Math.*, 165(1):115–151, 2006.

[167] A. J. D. Scala, C. Sanna, and E. Signorini. On the condition number of the vandermonde matrix of the n th cyclotomic polynomial. *Journal of Mathematical Cryptology*, 15(1):174–178, 2020.

[168] B. Sethuraman, B. Rajan, and V. Shashidhar. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Transactions on Information Theory*, 49(10):2596–2616, 2003.

[169] P. D. Seymour and T. Zaslavsky. Averaging sets: a generalization of mean values and spherical designs. *Adv. in Math.*, 52(3):213–240, 1984.

[170] M. Sha. On the lattices from elliptic curves over finite fields. *Finite Fields Appl.*, 31(2):84–107, 2015.

[171] U. Shapira and B. Weiss. Stable lattices and the diagonal group. *J. Eur. Math. Soc. (JEMS)*, 18(8):1753–1767, 2016.

[172] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[173] M. D. Sikirić, A. Schürmann, and F. Vallentin. Classification of eight-dimensional perfect forms. *Electron. Res. Announc. Amer. Math. Soc.*, 13:21–32, 2007.

[174] S. L. Sobolev. Formulas for mechanical cubatures in n-dimensional space. *Dokl. Akad. Nauk SSSR*, 137:527–530, 1961.

[175] O. Solan. Stable and well-rounded lattices in diagonal orbits. *Israel J. Math.*, 234(2):501–519, 2019.

[176] A. Srinivasan. A complete classification of well-rounded real quadratic ideal lattices. *J. Number Theory*, 207:349–355, 2020.

[177] M. A. Tsfasman and S. G. Vladut. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, 1991.
[178] P. van Emde Boas. Another np-complete problem and the complexity of computing short vectors in a lattice. *Tecnical Report, Department of Mathmatics, University of Amsterdam*, 1981.
[179] W. P. J. van Woerden. An upper bound on the number of perfect quadratic forms. *Adv. Math.*, 365, 2020. 107031, 12 pp.
[180] S. Vatedka, N. Kashyap, and A. Thangaraj. Secure compute-and-forward in a bidirectional relay. *IEEE Transactions on Information Theory*, 61(5):2531–2556, 2015.
[181] R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto. On the densest mimo lattices from cyclic division algebras. *IEEE Transactions on Information Theory*, 55(8):3751–3780, 2009.
[182] B. Venkov. Réseaux et designs sphériques. In *Réseaux euclidiens, designs sphériques et formes modulaires*, volume 37 of *Monogr. Enseign. Math.*, pages 10–86. Enseignement Math., Geneva, 2001.
[183] M. S. Viazovska. The sphere packing problem in dimension 8. *Ann. of Math. (2)*, 185(3):991–1015, 2017.
[184] A. C. Woods. Covering six space with spheres. *J. Number Theory*, 4(2):157–180, 1972.
[185] A. D. Wyner. The wiretap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711, USA
Email address: lenny@cmc.edu

Department of Mathematics and Systems Analysis, Aalto University, P.O. Box 11100, FI-00076 Aalto, Finland
Email address: camilla.hollanti@aalto.fi, rahinatou.njahepousenchiwo@aalto.fi