On the Ring-LWE and Polynomial-LWE Problems

Miruna Rosca[1,2], Damien Stehlé[1], and Alexandre Wallet[1]

[1] ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), France
[2] Bitdefender, Romania

Abstract. The Ring Learning With Errors problem (RLWE) comes in various forms. Vanilla RLWE is the decision dual-RLWE variant, consisting in distinguishing from uniform a distribution depending on a secret belonging to the dual $\mathcal{O}_K^\vee$ of the ring of integers $\mathcal{O}_K$ of a specified number field K. In primal-RLWE, the secret instead belongs to $\mathcal{O}_K$. Both decision dual-RLWE and primal-RLWE enjoy search counterparts. Also widely used is (search/decision) Polynomial Learning With Errors (PLWE), which is not defined using a ring of integers $\mathcal{O}_K$ of a number field K but a polynomial ring $\mathbb{Z}[x]/f$ for a monic irreducible $f \in \mathbb{Z}[x]$. We show that there exist reductions between all of these six problems that incur limited parameter losses. More precisely: we prove that the (decision/search) dual to primal reduction from Lyubashevsky *et al.* [EUROCRYPT 2010] and Peikert [SCN 2016] can be implemented with a small error rate growth for all rings (the resulting reduction is non-uniform polynomial time); we extend it to polynomial-time reductions between (decision/search) primal RLWE and PLWE that work for a family of polynomials f that is exponentially large as a function of $\deg f$ (the resulting reduction is also non-uniform polynomial time); and we exploit the recent technique from Peikert *et al.* [STOC 2017] to obtain a search to decision reduction for RLWE for arbitrary number fields. The reductions incur error rate increases that depend on intrinsic quantities related to K and f.

1 Introduction

Different shades of RLWE. Ring Learning With Errors (RLWE) was introduced by Lyubashevsky *et al.* in [LPR10], as a means of speeding up cryptographic constructions based on the Learning With Errors problem (LWE) [Reg09]. Let K be a number field, $\mathcal{O}_K$ its ring of integers and $q \geq 2$ a rational integer. The search variant of RLWE with parameters K and q consists in recovering a secret $s \in \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$ with $\mathcal{O}_K^\vee$ denoting the dual of $\mathcal{O}_K$, from arbitrarily many samples $(a_i, a_i \cdot s + e_i)$. Here each a_i is uniformly sampled in $\mathcal{O}_K / q\mathcal{O}_K$ and each e_i is a small random element of $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R}$. The noise term e_i is sampled such that its Minkowski embedding vector follows a Gaussian distribution with a small covariance matrix (relative to $q\mathcal{O}_K^\vee$). The decision variant consists in distinguishing arbitrarily many such pairs for a common s chosen uniformly in $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$, from uniform samples in $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K^\vee$. More formal definitions are provided in Section 2, but these suffice for describing our contributions.

Lyubashevsky *et al.* backed in [LPR10] the conjectured hardness of RLWE with a quantum polynomial-time reduction from the (worst-case) Approximate Shortest Vector Problem (ApproxSIVP) restricted to the class of Euclidean lattices corresponding to ideals of $\mathcal{O}_K$, with geometry inherited from the Minkowski embeddings. They showed its usefulness by describing a public-key encryption with quasi-optimal efficiency: the bit-sizes of the keys and the run-times of all involved algorithms are quasi-linear in the security parameter. A central technical contribution was a reduction from search RLWE to decision RLWE, when K is cyclotomic, and decision RLWE for cyclotomic fields is now pervasive in lattice-based cryptography, including in practice [ADPS16,BDK$^+$18,DLL$^+$18]. The search-to-decision reduction from [LPR10] was later extended to the case of general Galois rings in [EHL14,CLS15].

Prior to RLWE, Stehlé *et al.* [SSTX09] introduced what is now referred to as Polynomial Ring Learning With Errors (PLWE), for cyclotomic polynomials of degree a power of 2. PLWE is parametrized by a monic irreducible $f \in \mathbb{Z}[x]$ and an integer $q \geq 2$, and consists in recovering a secret $s \in \mathbb{Z}_q[x]/f$ from arbitrarily many samples $(a_i, a_i \cdot s + e_i)$ where each a_i is uniformly sampled in $\mathbb{Z}_q[x]/f$ and each e_i is a small random element of $\mathbb{R}[x]/f$. The decision variant consists in distinguishing arbitrarily many such samples for a common s sampled uniformly in $\mathbb{Z}_q[x]/f$, from uniform samples. Here the noise term e_i is sampled such that its coefficient vector follows a Gaussian distribution with a small covariance matrix. Stehlé *et al.* gave a reduction from the restriction of ApproxSIVP to the class of lattices corresponding to ideals of $\mathbb{Z}[x]/f$, to search PLWE, for f a power-of-2 cyclotomic polynomial.

Finally, a variant of RLWE with $s \in \mathcal{O}_K/q\mathcal{O}_K$ rather than $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ was also considered (see, e.g., [DD12] among others), to avoid the complication of having to deal with the dual $\mathcal{O}_K^\vee$ of $\mathcal{O}_K$. In the rest of this paper, we will refer to the latter as primal-RLWE and to standard RLWE as dual-RLWE.

The case of cyclotomics. Even though [LPR10] defined RLWE for arbitrary number fields, the problem was mostly studied in the literature for K cyclotomic. This specialization had three justifications:

- it leads to very efficient cryptographic primitives, in particular if q totally splits over K;

- the hardness result from [LPR10] holds for cyclotomics;
- no particular weakness was known for these fields.

Among cyclotomics, those of order a power of 2 are a popular choice. In the case of a field K defined by the cyclotomic polynomial f, we have that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for α a root of f. Further, in the case of power-of-2 cyclotomics, mapping the coefficient vector of a polynomial in $\mathbb{Z}[x]/f$ to its Minkowski embedding is a scaled isometry. This makes primal-RLWE and PLWE collapse into a single problem. Still in the case of power-of-2 cyclotomics, the dual $\mathcal{O}_K^\vee$ is a scaling of $\mathcal{O}_K$, implying that dual and primal-RLWE are equivalent. Apart from the monogenicity property, these facts do not hold for all cyclotomics. Nevertheless, Ducas and Durmus [DD12] showed it is still possible to reduce dual-RLWE to primal-RLWE.

Looking at other fields. The RLWE hardness proof holds with respect to a fixed field: the reduction in [LPR10] maps ApproxSIVP for lattices corresponding to $\mathcal{O}_K$-ideals with small approximation factors, to decision/search dual-RLWE on K. Apart from the very specific case of field extensions [GHPS12], hardness on K seems unrelated to hardness on another field K'. One may then wonder if RLWE is easier for some fields. The attacks presented in [EHL14,ELOS15,CLS15,CLS16] were used to identify weak generating polynomials f of a number field K, but they only work for error distributions with small width relative to the geometry of the corresponding ring [CIV16b,CIV16a,Pei16]. At this occasion, the relationships between the RLWE and PLWE variants were more closely investigated.

Building upon [CGS14,CDPR16], Cramer *et al.* [CDW17] gave a quantum polynomial-time ApproxSIVP algorithm for ideals of $\mathcal{O}_K$ when K is a cyclotomic field of prime-power conductor, when the ApproxSIVP approximation factor is $2^{\widetilde{O}(\sqrt{\deg K})}$. For general lattices, the best known algorithm [SE94] runs in time $2^{\widetilde{O}(\sqrt{n})}$ for such an approximation factor, where n is the lattice dimension (here $n = \deg K$). We note that the result from [CGS14,CDPR16] was partly extended in [BBdV$^+$17] to principal ideals generated by a short element in a completely different family of fields. These results show that all fields are not equal in terms of ApproxSIVP hardness (unless they turn out to be all weak!). So far, there is no such result for RLWE.

On the constructive front, Bernstein *et al.* [BCLvV16] showed that some non-cyclotomic polynomials f also enjoy practical arithmetic over $\mathbb{Z}_q[x]/f$ and lead to efficient cryptographic design (though the concrete scheme relies on the presumed hardness of another problem than RLWE).

Hedging against the weak field risk. Two recent works propose complementary approaches to hedge against the risk of a weakness of RLWE for specific fields. First, in [PRSD17], Peikert *et. al* give a new (quantum) reduction from ApproxSIVP for $\mathcal{O}_K$-ideals to decision dual-RLWE for the corresponding field K. All fields support a (quantum) reduction from ApproxSIVP, and hence, from this respect, one is not restricted to cyclotomics. Second, following an analogous result by Lyubashevsky for the Small Integer Solution problem [Lyu16], Roşca *et al.* [RSSS17] introduced the Middle-Product LWE problem and showed that it is at least as hard as PLWE for any f in an exponentially large family of f's (as a function of their degree). Neither result is fully satisfactory. In the first case, it could be that ApproxSIVP is easy for lattices corresponding to ideals of $\mathcal{O}_K$ for any K: this would make the result vacuous. In the second case, the result of [RSSS17] focuses on PLWE rather than the more studied RLWE problem.

Our results. The focus on the RLWE hardness for non-cyclotomic fields makes the discrepancies between the RLWE and PLWE variants more critical. In this article, we show that the six problems considered above — dual-RLWE, primal-RLWE and PLWE, all in both decision and search forms — reduce to one another in polynomial time with limited error rate increases, for huge classes of rings. More precisely, these reductions are obtained with the following three results.

- We show that for every field K, it is possible to implement the reduction from decision (resp. search) dual-RLWE to decision (resp. search) primal-RLWE from [LPR10, Le. 2.15] and [Pei16, Se. 2.3.2], with a limited error growth. Note that there exists a trivial converse reduction from primal-RLWE to dual-RLWE.
- We show that the reduction mentioned above can be extended to a reduction from decision (resp. search) primal-RLWE in K to decision (resp. search) PLWE for f, where K is the field generated by the polynomial f. The analysis is significantly more involved. It requires the introduction of the so-called conductor ideal, to handle the transformation from the ideal $\mathcal{O}_K$ to the order $\mathbb{Z}[x]/f$, and upper bounds on the condition number of the map that sends the coefficient embeddings to the Minkowski embeddings, to show that the noise increases are limited. Our conditioning upper bound is polynomial in n only for limited (but still huge) classes of polynomials that include those of the form $x^n + x \cdot P(x) - a$, with $\deg P < n/2$ and a prime that is $\geq 25 \cdot \|P\|_1^2$ and $\leq \mathrm{poly}(n)$. A trivial converse reduction goes through for the same f's.

- We exploit the recent technique from [PRSD17] to obtain a search to decision reduction for dual-RLWE.

Concretely, the error rate increases are polynomial in $n = \deg K$, the root discriminant $|\Delta_K|^{1/n}$ and, for the reduction to PLWE, in the root algebraic norm $\mathcal{N}(\mathcal{C}_{\mathbb{Z}[\alpha]})^{1/n}$ of the conductor ideal $\mathcal{C}_{\mathbb{Z}[\alpha]}$ of $\mathbb{Z}[\alpha]$, where α is a root of f defining K. We note that in many cases of interest, all these quantities are polynomially bounded in n. To enjoy these limited error rate growths, the first two reductions require knowledge of specific data related to K, namely, a short element (with respect to the Minkowski embeddings) in the different ideal $(\mathcal{O}_K^\vee)^{-1}$ and a short element in $\mathcal{C}_{\mathbb{Z}[\alpha]}$. In general, these are hard to compute.

Techniques. The first reduction is derived from [LPR10, Le. 2.15] and [Pei16, Se. 2.3.2]: if it satisfies some arithmetic properties, a multiplication by an element $t \in \mathcal{O}_K$ induces an $\mathcal{O}_K$-module isomorphism from $\mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$ to $\mathcal{O}_K/q\mathcal{O}_K$. For the reduction to be meaningful, we need t to have small Minkowski embeddings. We prove the existence of such a small t satisfying the appropriate arithmetic conditions, by generalizing the inclusion-exclusion technique developed in [SS13] to study the key generation algorithm of the NTRU signature scheme [HHPW10].

The Lyubashevsky *et al.* bijection works with $\mathcal{O}_K^\vee$ and $\mathcal{O}_K$ replaced by arbitrary ideals of K, but this does not provide a bijection from $\mathcal{O}_K/q\mathcal{O}_K$ to $\mathbb{Z}[\alpha]/q\mathbb{Z}[\alpha]$, as $\mathbb{Z}[\alpha]$ may only be an order of $\mathcal{O}_K$ (and not necessarily an ideal). We circumvent this difficulty by using the conductor ideal of $\mathbb{Z}[\alpha]$. Intuitively, the conductor ideal describes the relationship between $\mathcal{O}_K$ and $\mathbb{Z}[\alpha]$. As far as we are aware, this is the first time the conductor ideal is used in the RLWE context. This bijection and the existence of an appropriate multiplier t as above provide a (non-uniform) reduction from primal-RLWE to a variant of PLWE for which the noise terms have small Minkowski embeddings (instead of small polynomial coefficients).

We show that for many number fields, the linear map between polynomial coefficients and Minkowski embeddings has a condition number that is polynomially bounded in n, i.e., the map has bounded distortion and behaves not too noticeably differently from a scaling. This implies that the latter reduction is also a reduction from primal-RLWE to standard PLWE for these rings. We were able to show condition number bounds that are polynomial in n only for restricted families of polynomials f, yet exponentially large as n increases. These include in particular those of the form mentioned above. Note that the primality condition on the constant coefficient is used only to ensure that f is irreducible and hence defines a number field. For these f's, we use Rouché's theorem to prove that the roots are close to the scaled n-th roots of unity $(a^{1/n} \cdot \alpha_n^k)_{0 \leq k < n}$, and then that f "behaves" as $x^n - a$ in terms of geometric distortion.

Our search-to-decision reduction for dual-RLWE relies on techniques developed in [PRSD17]. In that article, Peikert *et al.* consider the following 'oracle hidden center' problem (OHCP). In this problem, we are given access to an oracle $\mathcal{O}$ taking as inputs a vector $\vec{z} \in \mathbb{R}^k$ and a scalar $t \in \mathbb{R}^{\geq 0}$, and outputting a bit. The probability that the oracle outputs 1 (over its internal randomness) is assumed to depend only on $\exp(t) \cdot \|\vec{z} - \vec{x}\|$, for some vector $\vec{x}$. The goal is to recover $\mathcal{O}$'s center $\vec{x}$. On the one hand, Peikert *et al.* give a polynomial-time algorithm for this problem, assuming the oracle is 'well-behaved' ([PRSD17, Prop. 4.4]). On the other hand, they show how to map a Bounded Distance Decoding (BDD) instance to such an OHCP instance if they have access to Gaussian samples in the dual of the BDD lattice, where the engine of the oracle is the decision dual-RLWE oracle ([PRSD17, Se. 6.1]). We construct the OHCP instance from the decision RLWE oracle in a different manner. We use our input search dual-RLWE samples and take small Gaussian combinations of them. By re-randomizing the secret and adding some noise, we can obtain arbitrarily many dual-RLWE samples. Subtracting from the input samples well-chosen z_i's in $K_{\mathbb{R}}$ and setting the standard deviation of the Gaussian combination appropriately leads to a valid OHCP instance. The main technical hurdle is to show that a Gaussian combination of elements of $\mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$ is close to uniform. For this, we generalize a ring Leftover Hash Lemma proved for specific pairs $(\mathcal{O}_K, q)$ in [SS11].

Related works. The reductions studied in this work can be combined with those from ApproxSIVP for $\mathcal{O}_K$-ideals to dual-RLWE [LPR10,PRSD17]. Recently, Albrecht and Deo [AD17] built upon [BLP+13] to obtain a reduction from Module-LWE to RLWE. This can be both combined with our reductions and the quantum reductions from ApproxSIVP for $\mathcal{O}_K$-modules to Module-LWE[3] [LS15,PRSD17]. Downstream, the reductions can be combined with the reduction from PLWE to Middle-Product LWE from [RSSS17]. The latter was showed to involve an error rate growth that is linearly bounded by the so-called the expansion factor of f: it turns out that those f's for which we could bound the condition number of the Minkowski map by a polynomial function of $\deg f$ also have polynomially bounded expansion factor. These reductions and those considered in the present work are pictorially described in Figure 1.

[3] The reduction from [LS15] is limited to cyclotomic fields, but [PRSD17] readily extends to module lattices.

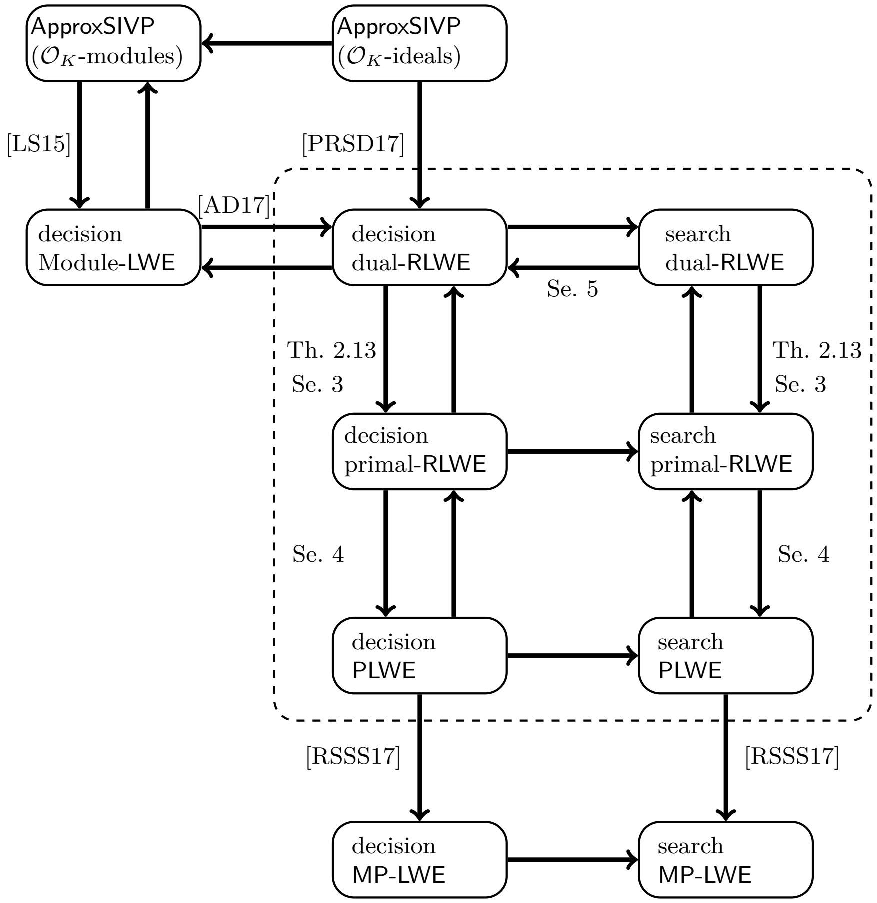

Fig. 1. Relationships between variants of RLWE and PLWE. The dotted box contains the problems studied in this work. Each arrow may hide a noise rate degradation (and module rank - modulus magnitude transfer in the case of [AD17]). The top to bottom arrows in the dotted box correspond to non-uniform reductions. The reductions involving PLWE are analyzed for limited family of defining polynomials. The arrows without references correspond to trivial reductions.

The ideal-changing scaling element t and the distortion of the Minkowski map were closely studied in [CIV16b,CIV16a,Pei16] for a few precise polynomials and fields. We use the same objects, but provide bounds that work for all (or many) fields.

Impact. As it is standard for the hardness foundations of lattice-based cryptography, our reductions *should not* be considered for setting practical parameters. They should rather be viewed as a strong evidence that the six problems under scope are essentially equivalent and do not suffer from a design flaw (unless they all do). We hope they will prove useful towards understanding the plausibility of weak fields for RLWE.

Our first result shows that there exists a way of reducing dual-RLWE to primal-RLWE while controlling the noise growth. Even though the reduction is non-uniform, it gives evidence that these problems are qualitatively equivalent. Our second result shows that RLWE and PLWE are essentially equivalent for a large class of polynomials/fields. In particular, the transformation map between the Minkowski embeddings and the coefficient embeddings has a bounded distortion. Finally, our search to decision fills an important gap. On the one hand, it precludes the possibility that search RLWE could be harder than decision RLWE. On the other hand, it gives further evidence of the decision RLWE hardness. In [PRSD17], the authors give a reduction from ApproxSIVP for $\mathcal{O}_K$-ideals to decision RLWE. But in the current state of affairs, ApproxSIVP for this special class of lattices seems easier than RLWE, at least for some parameters. Indeed, Cramer *et al.* [CDW17] gave quantum algorithms that outperform generic lattice algorithms for some range of approximation factors in the context of ideal lattices. On the opposite, RLWE is qualitatively equivalent to ApproxSIVP for $\mathcal{O}_K$-modules ([LS15,AD17]).

As the studied problems reduce to one another, one may then wonder which one to use for cryptographic design. Using dual-RLWE requires knowledge of $\mathcal{O}_K$, which is notoriously hard to compute for an arbitrary field K. This may look as an incentive to use the corresponding PLWE problem instead, as it does not require the knowledge of $\mathcal{O}_K$. Yet, for it to be useful in cryptographic design, one must be able to decode the noise from its representative modulo a scaled version of the lattice corresponding to $\mathbb{Z}[\alpha]$. This seems to require the knowledge of a good basis of that lattice, which may not be easy to obtain either, depending on the considered polynomial f.

Notations. If D is a distribution, we write $x \hookleftarrow D$ to say that we sample x from D. If D_1, D_2 are continuous distributions over the same measurable set $\varOmega$, we let $\varDelta(D_1, D_2) = \int_\varOmega |D_1(x) - D_2(x)| \mathrm{d}x$ denote their statistical distance. Similarly, we let $R(D_1 \| D_2) = \int_\varOmega D_1(x)^2/D_2(x) \mathrm{d}x$ denote their Rényi divergence. If E is a set of finite measure, we let $U(E)$ denote the uniform distribution over E. For a matrix $V = (v_{ij})$, we let $\|V\| = \sqrt{\sum_{1 \leq i,j \leq n} |v_{ij}|^2}$ denote its Frobenius norm.

2 Preliminaries

In this section, we give the necessary background in algebraic number theory, recall properties of Euclidean lattices, and state the precise definitions of the RLWE variants we will consider.

2.1 Some algebraic number theory

In Appendix A, we recall some notions of algebraic number theory that are standard in lattice-based cryptography. We recall here less usual notions such as orders and conductor ideals. Useful references for the latter include [Ste17,Cona].

Rings and ideals in number fields. In this article, we call any subring of K a number ring. For a number ring R, an (integral) R-ideal is an additive subgroup $I \subseteq R$ which is closed by multiplication in R, i.e., such that $IR = I$. A more compact definition is to say that I is an R-module. If $a_1, \ldots, a_k$ are elements in R, we let $\langle a_1, \ldots, a_k \rangle = a_1 R + \ldots + a_k R$ and call it the ideal generated by the a_i's. The product of two ideals I, J is the ideal generated by all elements xy with $x \in I$ and $y \in J$. The sum, product and intersection of two R-ideals are again R-ideals.

Two integral R-ideals I, J are said to be coprime if $I + J = R$, and, in this case, we have $I \cap J = IJ$. Any non-zero ideal in a number ring has finite index, i.e., the quotient ring R/I is always finite when I is a non-zero R-ideal. An R-ideal $\mathfrak{p}$ is said to be prime if whenever $\mathfrak{p} = IJ$ for some R-ideals I, J, then either $I = \mathfrak{p}$ or $J = \mathfrak{p}$. In a number ring, any prime ideal $\mathfrak{p}$ is maximal [Ste17, p. 19], i.e., R is the only R-ideal containing it. It also means that the quotient ring $R/\mathfrak{p}$ is a finite field. It is well-known that any $\mathcal{O}_K$-ideal admits a unique factorization into prime $\mathcal{O}_K$-ideals, i.e., it can be written $I = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$ with all $\mathfrak{p}_i$'s distinct prime ideals. It fails to hold in general number rings and orders, but we describe later in Lemma 2.1 how the result can be extended in certain cases.

A fractional R-ideal I is an R-module such that $xI \subseteq R$ for some $x \in K^\times$. An integral ideal is a fractional ideal, and so are the sum, the product and the intersection of two fractional ideals. A fractional R-ideal I is said to be invertible if there exists a fractional R-ideal J such that $IJ = R$. In this case, the (unique) inverse is the integral ideal $I^{-1} = \{x \in K : xI \subseteq R\}$. Any $\mathcal{O}_K$-ideal is invertible, but it is again false for a general number ring.

The algebraic norm of a non-zero integral R-ideal I is defined as $\mathcal{N}_R(I) = |R/I|$, and we will omit the subscript when $R = \mathcal{O}_K$. It satisfies $\mathcal{N}_R(IJ) = \mathcal{N}_R(I)\mathcal{N}_R(J)$ for every R-ideals I, J.

The dual of a fractional R-ideal I is $I^\vee = \{\alpha \in K : \mathrm{Tr}(\alpha I) \subseteq \mathbb{Z}\}$, which is also a fractional R-ideal. We always have $II^\vee = R^\vee$, so that $I^\vee = I^{-1}R^\vee$ when I is invertible. We also have $I^{\vee\vee} = I$ for any R-ideal I.

A particularly interesting dual is $\mathcal{O}_K^\vee$, whose inverse $(\mathcal{O}_K^\vee)^{-1}$ is called the different ideal. The different ideal is an integral ideal, whose norm $\Delta_K = \mathcal{N}((\mathcal{O}_K^\vee)^{-1})$ is called the discriminant of the number field. We note that, for every f defining K, the field discriminant Δ_K is a factor of the discriminant of f. The latter is denoted Δ_f and is defined as $\Delta_f = \prod_{i\neq j}(\alpha_i - \alpha_j)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f. This provides an upper bound on Δ_K in terms of the defining polynomial f.

Orders in number fields. An order $\mathcal{O}$ in K is a number ring which is a finite index subring of $\mathcal{O}_K$. In particular, the ring of integers $\mathcal{O}_K$ is the maximal order in K. Number rings such as $\mathbb{Z}[\alpha]$, with α a root of a defining polynomial f, are of particular interest. The conductor of an order $\mathcal{O}$ is defined as the set $\mathcal{C}_\mathcal{O} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}$. It is contained in $\mathcal{O}$, and it is both an $\mathcal{O}$-ideal and an $\mathcal{O}_K$-ideal: it is in fact the largest ideal with this property. It is never empty, as it contains the index $[\mathcal{O}_K : \mathcal{O}]$.

If it is coprime with the conductor, an ideal in $\mathcal{O}_K$ can be naturally considered as an ideal in $\mathcal{O}$, and reciprocally. This is made precise in the following lemma.

Lemma 2.1 ([Cona, Th. 3.8]). *Let $\mathcal{O}$ be an order in K.*

1. *Let I be an $\mathcal{O}_K$-ideal coprime to $\mathcal{C}_\mathcal{O}$. Then $I \cap \mathcal{O}$ is an $\mathcal{O}$-ideal coprime to $\mathcal{C}_\mathcal{O}$ and the natural map $\mathcal{O}/I\cap\mathcal{O} \longrightarrow \mathcal{O}_K/I$ is a ring isomorphism.*
2. *Let J be an $\mathcal{O}$-ideal coprime to $\mathcal{C}_\mathcal{O}$. Then $J\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal coprime to $\mathcal{C}_\mathcal{O}$ and the natural map $\mathcal{O}/J \longrightarrow \mathcal{O}_K/J\mathcal{O}_K$ is a ring isomorphism.*
3. *The set of $\mathcal{O}_K$-ideals coprime to $\mathcal{C}_\mathcal{O}$ and the set of $\mathcal{O}$-ideals coprime to $\mathcal{C}_\mathcal{O}$ are in multiplicative bijection by $I \longmapsto I \cap \mathcal{O}$ and $J \longmapsto J\mathcal{O}_K$.*

The above description does not tell how to "invert" the isomorphisms. This can be done by a combination of the following lemmas and passing through the conductor, as we will show in the next section.

Lemma 2.2. *Let $\mathcal{O}$ be an order in K and I an $\mathcal{O}_K$-ideal coprime to the conductor $\mathcal{C}_\mathcal{O}$. Then the inclusions $\mathcal{C}_\mathcal{O} \subseteq \mathcal{O}$ and $\mathcal{C}_\mathcal{O} \subseteq \mathcal{O}_K$ induce isomorphisms $\mathcal{C}_\mathcal{O}/I \cap \mathcal{C}_\mathcal{O} \simeq \mathcal{O}/I \cap \mathcal{O}$ and $\mathcal{C}_\mathcal{O}/I \cap \mathcal{C}_\mathcal{O} \simeq \mathcal{O}_K/I$.*

Proof. By assumption we have $\mathcal{C}_\mathcal{O} + I = \mathcal{O}_K$, so that the homomorphism $\mathcal{C}_\mathcal{O} \to \mathcal{O}_K/I$ is surjective. By Lemma 2.1, the set $I \cap \mathcal{O}$ is an $\mathcal{O}$-ideal coprime to $\mathcal{C}_\mathcal{O}$ so that $\mathcal{C}_\mathcal{O} + I \cap \mathcal{O} = \mathcal{O}$. This implies that the homomorphism $\mathcal{C}_\mathcal{O} \to \mathcal{O}/I \cap \mathcal{O}$ is surjective too. Both homomorphisms have kernel $I \cap \mathcal{C}_\mathcal{O}$. □

Lemma 2.3 ([Cona, Cor. 3.10]). *Let $\mathcal{O}$ be an order in K and $\beta \in \mathcal{O}$ such that $\beta\mathcal{O}_K$ is coprime to $\mathcal{C}_{\mathcal{O}}$. Then $\beta\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$.*

Quotients of ideals. We will use the following result.

Lemma 2.4 ([LPR10, Le. 2.14]). *Let I and J two $\mathcal{O}_K$-ideals. Let $t \in I$ such that the ideals $t \cdot I^{-1}$ and J are coprime and let $\mathcal{M}$ be any fractional $\mathcal{O}_K$-ideal. Then the function $\theta_t : \mathcal{M} \to \mathcal{M}$ defined as $\theta_t(x) = t \cdot x$ induces an $\mathcal{O}_K$-module isomorphism from $\mathcal{M}/J\mathcal{M}$ to $I\mathcal{M}/IJ\mathcal{M}$.*

The authors of [LPR10] also gave an explicit way to obtain a suitable t by solving a set of conditions stemming from the Chinese Remainder Theorem. However, this construction does not give good control on the magnitudes of the Minkowski embeddings of t.

2.2 Lattices

For the remainder of this article, a lattice is defined as a full-rank discrete additive subgroup of an $\mathbb{R}$-vector space V which is a Cartesian power H^m (for $m \geq 1$) of $H := \{\vec{x} \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : \forall i \leq s_2 : x_{s_1+s_2+i} = \overline{x_{s_1+i}}\}$. This space H is sometimes called the "canonical" space and its definition is recalled in Appendix A. A given lattice $\mathcal{L}$ can be thought as the set of $\mathbb{Z}$-linear combinations $(\vec{b}_i)_i$ of some linearly independent vectors of V. These vectors are said to form a lattice basis, and we define the lattice determinant as $\det \mathcal{L} = (\det(\langle \vec{b}_i, \vec{b}_j \rangle)_{i,j})^{1/2}$ (it does not depend on the choice of the basis of $\mathcal{L}$). For $v \in V$, let $\|v\| = (\sum_{i \leq \dim V} |v_i|^2)^{1/2}$ denote the standard Hermitian norm on V and $\|v\|_\infty = \max_{i \leq \dim V} |v_i|$ denote the infinity norm. The minimum $\lambda_1(\mathcal{L})$ is the Hermitian norm of a shortest non-zero element in $\mathcal{L}$. We define $\lambda_1^\infty(\mathcal{L})$ similarly. If $\mathcal{L}$ is a lattice, then we define its dual as $\mathcal{L}^* = \{\vec{y} \in V : \vec{y}^T\mathcal{L} \subseteq \mathbb{Z}\}$.

Ideal lattices. While it is possible to associate lattices with fractional ideals of a number ring, we will not need it. Any fractional $\mathcal{O}_K$-ideal I is a free $\mathbb{Z}$-module of rank $n = \deg(K)$, i.e., it can be written as $\mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n$ for some u_i's in K. Its canonical embedding $\sigma(I)$ is a lattice of dimension n in the $\mathbb{R}$-vector space $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$. Such a lattice is called an ideal lattice (for $\mathcal{O}_K$). For the sake of readability, we will abuse notations and often identify I and $\sigma(I)$. It is possible to look at the coefficient embedding of such lattices as well, but we will not need it in this work. The lattice corresponding to $I^\vee$ is $\overline{I^*}$. The discriminant of K satisfies $\varDelta_K = (\det \mathcal{O}_K)^2$. In the following lemma, the upper bounds follow from Minkowski's theorem whereas the lower bounds are a consequence of the algebraic structure underlying ideal lattices.

Lemma 2.5 (Adapted from [PR07, Se. 6.1]). *Let K be a number field of degree n. For any fractional $\mathcal{O}_K$-ideal I, we have:*

$$\begin{aligned} \sqrt{n} \cdot \mathcal{N}(I)^{1/n} &\leq \lambda_1(I) \leq \sqrt{n} \cdot (\mathcal{N}(I)\sqrt{\Delta_K})^{1/n}, \\ \mathcal{N}(I)^{1/n} &\leq \lambda_1^{\infty}(I) \leq (\mathcal{N}(I)\sqrt{\Delta_K})^{1/n}. \end{aligned}$$

Gaussians. It is standard practice in the RLWE setting to consider Gaussian distributions with diagonal covariance matrices. In this work, we will be interested in the behavior of samples after linear transformations that are not necessarily diagonal. As the resulting covariance matrix may not be diagonal, we adopt a more general framework. Let $\mathbf{\Sigma} \succ 0$, i.e., a symmetric positive definite matrix. We define the Gaussian function on $\mathbb{R}^n$ of covariance matrix $\mathbf{\Sigma}$ as $\rho_{\mathbf{\Sigma}}(\mathbf{x}) := \exp(-\pi \cdot \mathbf{x}^T \mathbf{\Sigma}^{-1} \mathbf{x})$ for every vector $\mathbf{x} \in \mathbb{R}^n$. The Gaussian distribution $D_{\mathbf{\Sigma}}$ is the probability distribution whose density is proportional to $\rho_{\mathbf{\Sigma}}$. When $\mathbf{\Sigma} = \operatorname{diag}(r_i^2)_i$ for some $\vec{r} \in \mathbb{R}^n$, we write $\rho_{\vec{r}}$ and $D_{\vec{r}}$, respectively.

Let $(\vec{e}_i)_{i \leq n}$ be the canonical basis of $\mathbb{C}^n$. We define $\vec{h}_i = \vec{e}_i$ for $i \leq s_1$, and $\vec{h}_{s_1+i} = (\vec{e}_{s_1+i} + \vec{e}_{s_1+s_2+i})/\sqrt{2}$ and $\vec{h}_{s_1+s_2+i} = (\vec{e}_{s_1+i} - \vec{e}_{s_1+s_2+i})/\sqrt{-2}$ for $i \leq s_2$. The $\vec{h}_i$'s form an orthonormal $\mathbb{R}$-basis of H. We define the Gaussian distribution $D^H_{\mathbf{\Sigma}}$ as the distribution obtained by sampling $x \hookleftarrow D_{\mathbf{\Sigma}}$ and returning $\sum_i x_i \vec{h}_i$. We will repeatedly use the observation that if $\vec{x}$ is sampled from $D^H_{\mathbf{\Sigma}}$ and t belongs to $K_{\mathbb{R}}$, then $t \cdot \vec{x}$ is distributed as $D^H_{\mathbf{\Sigma}'}$ with $\mathbf{\Sigma}' = \operatorname{diag}(|\sigma_i(t)|) \cdot \mathbf{\Sigma} \cdot \operatorname{diag}(|\sigma_i(t)|)$.

For a lattice $\mathcal{L}$ over $V = H^m$ (for some $m \geq 1$) and a coset $\vec{c} \in V/\mathcal{L}$, we let $D_{\mathcal{L}+\vec{c},r}$ denote the discretization of $D^H_{r\mathbf{I}}$ over $\mathcal{L} + \vec{c}$ (we omit the subscript for $D_{\mathcal{L}+\vec{c},r}$ as all our lattices are over Cartesian powers of H). For $\varepsilon > 0$, we define the smoothing parameter $\eta_\varepsilon(\mathcal{L})$ as the smallest $r > 0$ such that $\rho_{(1/r)\mathbf{I}}(\mathcal{L}^* \setminus \vec{0}) \leq \varepsilon$. We have the following upper bounds.

Lemma 2.6 ([MR04, Le. 3.3]). *For any lattice $\mathcal{L}$ over H^m and $\varepsilon \in (0,1)$, we have $\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\log(2mn(1+1/\varepsilon))/\pi}/\lambda_1^{\infty}(\mathcal{L}^*)$.*

Lemma 2.7 (Adapted from [PR07, Le. 6.5]). *For any $\mathcal{O}_K$-ideal I and $\varepsilon \in (0,1)$, we have $\eta_\varepsilon(I) \leq \sqrt{\log(2n(1+1/\varepsilon))/(\pi n)} \cdot (\mathcal{N}(I)\Delta_K)^{1/n}$.*

The following are standard applications of the smoothing parameter.

Lemma 2.8 ([GPV08, Cor. 2.8]). *Let $\mathcal{L}' \subseteq \mathcal{L}$ be full-rank lattices, $\varepsilon \in (0,1/2)$ and $r \geq \eta_\varepsilon(\mathcal{L}')$. Then $\Delta(D_{\mathcal{L},r} \bmod \mathcal{L}', U(\mathcal{L}/\mathcal{L}')) \leq 2\varepsilon$.*

Lemma 2.9 ([PR06, Le. 2.11]). *Let $\mathcal{L}$ be an n-dimensional lattice, $\varepsilon \in (0,1/3)$ and $r \geq 4\eta_\varepsilon(\mathcal{L})$. Then $D_{\mathcal{L},r}(\vec{0}) \leq 2^{-2n+1}$.*

Lemma 2.10 (Adapted from [MR04, Le. 4.4]). *Let $\mathcal{L}$ be an n-dimensional lattice, $\varepsilon \in (0, 1/3)$ and $r \geq \eta_\varepsilon(\mathcal{L})$. Then $\Pr_{\vec{x} \hookleftarrow D_{\mathcal{L},r}}[\|\vec{x}\| \geq 2r\sqrt{n}] \leq 2^{-2n}$.*

2.3 Computational problems

We now formally define the computational problems we will study.

Definition 2.11 (RLWE and PLWE distributions). *Let K a degree n number field defined by f, $\mathcal{O}_K$ its ring of integers, $\mathbf{\Sigma} \succ 0$ and $q \geq 2$.*

For $s \in \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$, we define the dual-RLWE distribution $\mathcal{A}_{s,\mathbf{\Sigma}}^\vee$ as the distribution over $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K^\vee$ obtained by sampling $a \hookleftarrow U(\mathcal{O}_K/q\mathcal{O}_K)$, $e \hookleftarrow D_{\mathbf{\Sigma}}^H$ and returning the pair $(a, a \cdot s + e)$.

For $s \in \mathcal{O}_K/q\mathcal{O}_K$, we define the primal-RLWE distribution $\mathcal{A}_{s,\mathbf{\Sigma}}$ as the distribution over $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K$ obtained by sampling $a \hookleftarrow U(\mathcal{O}_K/q\mathcal{O}_K)$, $e \hookleftarrow D_{\mathbf{\Sigma}}^H$ and returning the pair $(a, a \cdot s + e)$.

For $s \in \mathbb{Z}_q[x]/f$, we define the PLWE distribution $\mathcal{B}_{s,\mathbf{\Sigma}}$ as the distribution over $\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f$ obtained by sampling $a \hookleftarrow U(\mathbb{Z}_q[x]/f)$, $e \hookleftarrow D_{\mathbf{\Sigma}}$ and returning the pair $(a, a \cdot s + e)$ (with $\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$).

In the definition above, we identified the support H of $D_{\mathbf{\Sigma}}^H$ with $K_\mathbb{R}$, and the support $\mathbb{R}^n$ of $D_{\mathbf{\Sigma}}$ with $\mathbb{R}[x]/f$. Note that sampling from $\mathcal{A}_{s,\mathbf{\Sigma}}^\vee$ and $\mathcal{A}_{s,\mathbf{\Sigma}}$ seems to require the knowledge of a basis of $\mathcal{O}_K$. It is not known to be computable in polynomial-time from a defining polynomial f of an arbitrary K. In this article, we assume that a basis of $\mathcal{O}_K$ is known.

Definition 2.12 (The RLWE and PLWE problems). *We use the same notations as above. Further, we let $\mathcal{E}_\succ$ be a subset of $\Sigma \succ 0$ and $D_\succ$ be a distribution over $\Sigma \succ 0$.*

Search dual-RLWE$_{q,\mathcal{E}_\succ}$ (resp. primal-RLWE and PLWE) consists in finding s from a sampler from $\mathcal{A}_{s,\mathbf{\Sigma}}^\vee$ (resp. $\mathcal{A}_{s,\mathbf{\Sigma}}$ and $\mathcal{B}_{s,\mathbf{\Sigma}}$), where $s \in \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ (resp. $s \in \mathcal{O}_K/q\mathcal{O}_K$ and $s \in \mathbb{Z}_q[x]/f$) and $\mathbf{\Sigma} \in \mathcal{E}_\succ$ are arbitrary.

Decision dual-RLWE$_{q,D_\succ}$ (resp. primal-RLWE and PLWE) consists in distinguishing between a sampler from $\mathcal{A}_{s,\mathbf{\Sigma}}^\vee$ (resp. $\mathcal{A}_{s,\mathbf{\Sigma}}$ and $\mathcal{B}_{s,\mathbf{\Sigma}}$) and a uniform sampler over $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K^\vee$ (resp. $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K$ and $\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f$), with non-negligible probability over $s \hookleftarrow \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ (resp. $s \in \mathcal{O}_K/q\mathcal{O}_K$ and $s \in \mathbb{Z}_q[x]/f$) and $\mathbf{\Sigma} \hookleftarrow D_\succ$.

The problems above are in fact defined for sequences of number fields of growing degrees n such that the bit-size of the problem description grows at most polynomially in n. The run-times, success probabilities and distinguishing advantages of the algorithms solving the problems are considered asymptotically as functions of n.

The following reduction from dual-RLWE to primal-RLWE is a consequence of Lemma 2.4. A proof is given in Appendix B.

Theorem 2.13 (Adapted from [Pei16, Se. 2.3.2]). *Let $\mathbf{\Sigma} \succ 0$ and $s \in \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$. Let $t \in (\mathcal{O}_K^\vee)^{-1}$ such that $t(\mathcal{O}_K^\vee) + q\mathcal{O}_K = \mathcal{O}_K$. Then the map $(a,b) \mapsto (a, t \cdot b)$ transforms $\mathcal{A}^\vee_{s,\mathbf{\Sigma}}$ to $\mathcal{A}_{t\cdot s,\mathbf{\Sigma}'}$ and $U(\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K^\vee)$ into $U(\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K)$, with $\mathbf{\Sigma}' = \operatorname{diag}(|\sigma_i(t)|) \cdot \mathbf{\Sigma} \cdot \operatorname{diag}(|\sigma_i(t)|)$. The natural inclusion $\mathcal{O}_K \to \mathcal{O}_K^\vee$ induces a map that transforms $U(\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K)$ to $U(\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K^\vee)$, and $\mathcal{A}_{s,\mathbf{\Sigma}}$ to $\mathcal{A}^\vee_{s,\mathbf{\Sigma}}$.*

We will consider variants of the decision problems for which the distinguishing must occur for all $s \in \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ (resp. $s \in \mathcal{O}_K/q\mathcal{O}_K$ and $s \in \mathbb{Z}_q[x]/f$) and all $\mathbf{\Sigma} \succ 0$ rather than with non-negligible probability over s. We call this variant worst-case decision dual-RLWE (resp. primal-RLWE and PLWE). Under some conditions on $D_\succ$ and $\mathcal{E}_\succ$, these variants are computationally equivalent.

Lemma 2.14 (Adapted from [LPR10, Se. 5.2]). *We use the same notations as above. If $\Pr_{\mathbf{\Sigma} \hookleftarrow D_\succ}[\mathbf{\Sigma} \notin \mathcal{E}_\succ] \leq 2^{-n}$, then decision dual-$\mathsf{RLWE}_{q,D_\succ}$ (resp. primal-RLWE and PLWE) reduces to worst-case decision dual-$\mathsf{RLWE}_{q,\mathcal{E}_\succ}$ (resp. primal-RLWE and PLWE).*

Assume further that $D_\succ$ can be sampled from in polynomial-time. If $\max_{\mathbf{\Sigma}\in\mathcal{E}_\succ} R(D_\succ \| D_\succ + \mathbf{\Sigma}) \leq \operatorname{poly}(n)$, then worst-case decision dual-$\mathsf{RLWE}_{q,\mathcal{E}_\succ}$ (resp. primal-RLWE and PLWE) reduces to decision dual-$\mathsf{RLWE}_{q,D_\succ}$ (resp. primal-RLWE and PLWE).

Note that it is permissible to use the Rényi divergence here even though we are considering decision problems. Indeed, the argument is applied to the random choice of the noise distribution and not to the distinguishing advantage. The same argument has been previously used in [LPR10, Se. 5.2].

Proof. The first statement is direct. We prove the second statement only for dual-RLWE, as the proofs for primal-RLWE and PLWE are direct adaptations. Assume we are given a sampler that outputs (a_i, b_i) with $a_i \hookleftarrow U(\mathcal{O}_K/q\mathcal{O}_K)$ and b_i either uniform in $K_\mathbb{R}/q\mathcal{O}_K^\vee$ or of the form $b_i = a_i s + e_i$ with $s \in \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ and $e_i \hookleftarrow D^H_{\mathbf{\Sigma}}$. The reduction proceeds by sampling $s' \hookleftarrow U(\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee)$ and $\mathbf{\Sigma}' \hookleftarrow D_\succ$, and mapping all input (a_i, b_i)'s to $(a'_i, b'_i) = (a_i, b_i + a_i s' + e'_i)$ with $e'_i \hookleftarrow D^H_{\mathbf{\Sigma}'}$. This transformation maps the uniform distribution to itself, and $\mathcal{A}^{\vee}_{s,\mathbf{\Sigma}}$ to $\mathcal{A}^{\vee}_{s+s',\mathbf{\Sigma}''}$ with $\mathbf{\Sigma}''_{ij} = \mathbf{\Sigma}_{ij} + \mathbf{\Sigma}'_{ij}$ for all i, j. If the success probability (success being enjoying a non-negligible distinguishing advantage) over the error parameter sampled from $D_{\succ}$ is non-negligible, then so is it for the error parameter sampled $D_{\succ} + \mathbf{\Sigma}$, as, by assumption, the Rényi divergence $R(D_{\succ} \| D_{\succ} + \mathbf{\Sigma})$ is polynomially bounded. □

Many choices of $D_{\succ}$ and $\mathcal{E}_{\succ}$ satisfy the conditions of Lemma 2.14. The following is inspired from [LPR10, Se. 5.2]. We define the distribution $\mathcal{E}_{\succ}$ as follows, for an arbitrary r: Let $s_{ij} = r^2(1 + nx_{ij})$ for all $i > j$, $s_{ii} = r^2(1 + n^3 x_{ii})$ for all i and $s_{ij} = s_{ji}$ for all $i < j$, where the x_{ij}'s are independent samples from the $\Gamma(2, 1)$ distribution (of density function $x \mapsto x \exp(-x)$); the output matrix is $(s_{ij})_{ij}$. Note that it is symmetric and strictly diagonally dominant (and hence $\succ 0$) with probability $1 - 2^{-\Omega(n)}$. Then the set of all $\Sigma \succ 0$ with coefficients of magnitudes $\leq r^2 n^4$ satisfies the first condition of Lemma 2.14, and the set of all $\Sigma \succ 0$ with coefficients of magnitudes $\leq r^2$ satisfies the second condition of Lemma 2.14. We can hence switch from one variant to the other while incurring an error rate increase that is $\leq \mathrm{poly}(n)$.

3 Controlling noise growth in dual to primal reduction

The reduction of Theorem 2.13 is built upon the existence of t as in Lemma 2.4. While this existence is guaranteed constructively by [LPR10], the size is not controlled by the construction. Another t that satisfies the conditions is $t = f'(\alpha)$, where f' is the derivative of f defining $K = \mathbb{Q}[\alpha]$. Indeed, from [Conb, Rem. 4.5], we know that $f'(\alpha) \in (\mathcal{O}_K^{\vee})^{-1}$. However, the noise growth incurred by multiplication by $f'(\alpha)$ may be rather large in general: we have $N(f'(\alpha)) = \Delta_f = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \mathcal{N}((\mathcal{O}_K^{\vee})^{-1})$.

In this section, we give a probabilistic proof that adequate t's with controlled size can be found by Gaussian sampling.

Let I and J be integral ideals of $\mathcal{O}_K$. Theorem 3.1 below states that a Gaussian sample t in I is such that $t \cdot I^{-1} + J = \mathcal{O}_K$ with non-negligible probability. The main technical hurdle is to show that the sample is not trapped in IJ' with J' a non-trivial factor of J. We handle this probability in different ways depending on the algebraic norm of J', extending an idea used in [SS13, Se. 4].

- For small-norm factors J' of J, the Gaussian folded modulo IJ' is essentially uniform over I/IJ', by Lemma 2.8. This requires the standard deviation parameter s to be above the smoothing parameter of IJ'. We use the smoothing parameter bound from Lemma 2.7.

- For large-norm factors J', we argue that the non-zero points of IJ' are very unlikely to be hit, thanks to the Gaussian tail bound given in Lemma 2.10 and the fact that the lattice minimum of IJ' is large, by Lemma 2.5.
- For middle-norm factors J', neither of the arguments above applies. Instead, we bound the probability that t belongs to IJ' by the probability that t belongs to IJ'', where J'' is a non-trivial factor of J', and use the first argument above. The factor J'' must be significantly denser than J' so that we have smoothing. But it should also be significantly sparser than $\mathcal{O}_K$ so that the upper bound is not too large.

Setting the standard deviation parameter of the discrete Gaussian so that at least one of the three arguments above applies is non-trivial. In particular, this highly depends on how the ideal J factors into primes (whether the pieces are numerous, balanced, unbalanced, etc). The choice we make below works in all cases while still providing a reasonably readable proof and still being sufficient for our needs, from an asymptotic perspective. In many cases, better choices can be made. If J is prime, we can take a very small s and use only the second argument. If all factors of J are small, there is good enough ‘granularity’ in the factorization to use the third argument, and again s can be chosen very small.

Theorem 3.1. *Let I and J be integral $\mathcal{O}_K$-ideals, and write $J = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ for some prime ideals $\mathfrak{p}_i$. We sort the $\mathfrak{p}_i$'s by non-decreasing algebraic norms. Assume that we can take $\delta \in [\frac{4n+\log_2 \Delta_K}{\log_2 \mathcal{N}(J)}, 1]$.*[4] *We define:*

$$s = \begin{cases} \left(\mathcal{N}(J)^{1/2}\mathcal{N}(I)\Delta_K\right)^{1/n} & \text{if} \quad \mathcal{N}(\mathfrak{p}_k) \geq \mathcal{N}(J)^{1/2+\delta}, \\ \left(\mathcal{N}(J)^{1/2+2\delta}\mathcal{N}(I)\Delta_K\right)^{1/n} & \text{else.} \end{cases}$$

Then we have

$$\Pr_{t \hookleftarrow D_{I,s}}[tI^{-1} + J = \mathcal{O}_K] \geq 1 - \frac{k}{\mathcal{N}(\mathfrak{p}_1)} - 2^{-n+4}.$$

Proof. We bound the probability P of the negation, from above. We have

$$P = \Pr_{t \hookleftarrow D_{I,s}}[t \in \bigcup_{i\in[k]} I\mathfrak{p}_i] = \sum_{S\subseteq[k], S\neq\emptyset} (-1)^{|S|+1} \cdot \Pr_{t \hookleftarrow D_{I,s}}[t \in I \cdot \prod_{i\in S} \mathfrak{p}_i].$$

[4] The parameter δ should be thought as near 0. It can actually be chosen such if $\mathcal{N}(J)$ is sufficiently large.

We rewrite it as $P = P_1 + P_2$ with

$$\begin{aligned} P_1 &= \sum_{S \subseteq [k], S \neq \emptyset} (-1)^{|S|+1} \frac{1}{\prod_{i \in S} \mathcal{N}(\mathfrak{p}_i)} = 1 - \prod_{i \in [k]} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p}_i)}\right), \\ P_2 &= \sum_{S \subseteq [k], S \neq \emptyset} (-1)^{|S|+1} \left(\Pr_{t \hookleftarrow D_{I,s}} [t \in I \cdot \prod_{i \in S} \mathfrak{p}_i] - \prod_{i \in S} \frac{1}{\mathcal{N}(\mathfrak{p}_i)} \right). \end{aligned}$$

We have $P_1 \leq 1 - (1 - 1/\mathcal{N}(\mathfrak{p}_1))^k \leq k/\mathcal{N}(\mathfrak{p}_1)$. Our task is now to bound P_2.

Assume first that $\mathcal{N}(\mathfrak{p}_k) \geq \mathcal{N}(J)^{1/2+\delta}$. This implies that $\prod_{i \in S} \mathcal{N}(\mathfrak{p}_i) \leq \mathcal{N}(J)^{1/2-\delta}$ for all $S \subseteq [k]$ not containing k. By Lemma 2.7, we have $s \geq \eta_\varepsilon(I \prod_{i \in S} \mathfrak{p}_i)$ for all such S's, with $\varepsilon = 2^{-2n}$. We "smooth" out those ideals, i.e., we use Lemma 2.8 to obtain, for all $S \subseteq [k] \setminus \{k\}$:

$$\left| \Pr_{t \hookleftarrow D_{I,s}} [t \in I \cdot \prod_{i \in S} \mathfrak{p}_i] - \prod_{i \in S} \frac{1}{\mathcal{N}(\mathfrak{p}_i)} \right| \leq 2\varepsilon.$$

Now if S is a subset containing k, then we have $\mathcal{N}(\prod_{i \in S} \mathfrak{p}_i) \geq \mathcal{N}(J)^{1/2+\delta}$. By Lemma 2.5, we have $\lambda_1(I \prod_{i \in S} \mathfrak{p}_i) \geq \sqrt{n} \cdot \mathcal{N}(I)^{1/n} \mathcal{N}(J)^{(1/2+\delta)/n}$. On the other hand, by Lemma 2.10, we have $\Pr_{t \hookleftarrow D_{I,s}}[\|t\| \geq 2s\sqrt{n}] \leq 2^{-2n}$. Thanks to our choice of s, the assumption on δ and Lemma 2.9, we obtain

$$\Pr_{t \hookleftarrow D_{I,s}} [t \in I \prod_{i \in S} \mathfrak{p}_i] \leq \Pr_{t \hookleftarrow D_{I,s}} [t = 0] + 2^{-2n} \leq 2^{-2n+2}.$$

This allows us to bound P_2 as follows:

$$P_2 \leq 2^k \cdot \left(\varepsilon + 2^{-2n+2} + \mathcal{N}(J)^{-(1/2+\delta)} \right).$$

By assumption on δ, we have $\mathcal{N}(J) \geq 2^{2n}$ and $P_2 \leq 2^{-n+3}$. This completes the proof for the large $\mathcal{N}(\mathfrak{p}_k)$ case.

Now, assume that $\mathcal{N}(\mathfrak{p}_k) < \mathcal{N}(J)^{1/2+2\delta}$. Then, as above, the definition of s implies that, for any $S \subseteq [k]$ with $\mathcal{N}(\prod_{i \in S} \mathfrak{p}_i) \leq \mathcal{N}(J)^{1/2+\delta}$, we have $|\Pr[t \in I \prod_{i \in S} \mathfrak{p}_i] - 1/\prod_{i \in S} \mathcal{N}(\mathfrak{p}_i)| \leq 2^{-2n+1}$. Also as above, if we have $\mathcal{N}(\prod_{i \in S} \mathfrak{p}_i) \geq \mathcal{N}(J)^{1/2+3\delta}$, then $\lambda_1(I \prod_{i \in S} \mathfrak{p}_i)$ is too large for a non-zero element of $I \prod_{i \in S} \mathfrak{p}_i$ to be hit with significant probability. Assume finally that

$$\mathcal{N}(J)^{1/2+2\delta} \leq \mathcal{N}(\prod_{i \in S} \mathfrak{p}_i) \leq \mathcal{N}(J)^{1/2+3\delta}.$$

As $\mathcal{N}(\mathfrak{p}_k) < \mathcal{N}(J)^{1/2+\delta}$, there exists $S' \subseteq S$ such that

$$\mathcal{N}(J)^{\delta} \leq \mathcal{N}(\prod_{i \in S'} \mathfrak{p}_i) \leq \mathcal{N}(J)^{1/2+2\delta}.$$

By inclusion, we have that $\Pr[t \in I \prod_{i \in S} \mathfrak{p}_i] \leq \Pr[t \in I \prod_{i \in S'} \mathfrak{p}_i]$. Now, as the norm of $\prod_{i \in S'} \mathfrak{p}_i$ is small enough, we can use the smoothing argument above to claim that

$$\Pr_{t \hookleftarrow D_{I,s}}[t \in I \prod_{i \in S'} \mathfrak{p}_i] \leq 2^{-2n+1} + \frac{1}{\mathcal{N}(\prod_{i \in S'} \mathfrak{p}_i)} \leq 2^{-2n+1} + \frac{1}{\mathcal{N}(J)^{\delta}}.$$

By assumption on δ, the latter is $\leq 2^{-n+2}$. Collecting terms allows to complete the proof. □

The next corollary shows that the needed t can be found with non-negligible probability.

Corollary 3.2. *Let I be an integral $\mathcal{O}_K$-ideal. Let $q \geq \max(2n, 2^{16} \cdot \Delta_K^{8/n})$ be a prime rational integer and $\mathfrak{p}_k$ a prime factor of $q\mathcal{O}_K$ with largest norm. We define:*

$$s = \begin{cases} q^{1/2} \cdot (\mathcal{N}(I)\Delta_K)^{1/n} & \textit{if} \quad \mathcal{N}(\mathfrak{p}_k) \geq q^{(5/8) \cdot n}, \\ q^{3/4} \cdot (\mathcal{N}(I)\Delta_K)^{1/n} & \textit{else}. \end{cases}$$

Then, for sufficiently large n, we have

$$\Pr_{t \hookleftarrow D_{I,s}}[tI^{-1} + q\mathcal{O}_K = \mathcal{O}_K] \geq 1/2.$$

Proof. The result follows from applying Theorem 3.1 with $J = q\mathcal{O}_K$ and $\delta = 1/8$. The first lower bound on q ensures that $k/\mathcal{N}(\mathfrak{p}_1) \leq 1/2$, where $k \leq n$ denotes the number of prime factors of $q\mathcal{O}_K$ and $\mathfrak{p}_1$ denotes a factor with smallest algebraic norm. The second lower bound on q ensures that we can indeed set $\delta = 1/8$. □

We insist again on the fact that the required lower bounds on s can be much improved under specific assumptions on the factorization of q. For example, one could choose a q such that all the factors of $q\mathcal{O}_K$ have large norms, by sampling q randomly and checking its primality and the factorization of the defining polynomial f modulo q. In that case, the factors $q^{1/2}$ and $q^{3/4}$ can be decreased drastically.

We note that if the noise increase incurred by a reduction from an LWE-type problem to another is bounded as $n_1^c \cdot q_2^c$ for some $c_1 < 1$ and some $c_2 > 0$, then one may set the working modulus q so that the starting LWE problem has a sufficient amount of noise to not be trivially easy to solve, and the ending LWE problem has not enough noise to be information-theoretically impossible to solve (else the reduction would be vacuous). Indeed, it suffices to set q sufficiently larger than $n^{c_1/(1-c_2)}$.

4 From primal-RLWE to PLWE

The goal of this section is to describe a reduction from primal-RLWE to PLWE. As an intermediate step, we first consider a reduction from primal-RLWE to a variant PLWE^σ of PLWE where the noise is small with respect to the Minkowski embedding rather than the coefficient embedding. Then, we assess the noise distortion when looking at its Minkowski embedding versus its coefficient embedding.

If $K = \mathbb{Q}[x]/f$ for some $f = \prod_{j\leq n}(x - \alpha_j)$, the associated Vandermonde matrix V_f has jth row $(1, \alpha_j, \ldots, \alpha_j^{n-1})$ and corresponds to the linear map between the coefficient and Minkowski embedding spaces (see Appendix A). Thus a good approximation of the distortion is given by the condition number $\mathrm{Cond}(V_f) = s_n/s_1$, where the s_i's refer to the largest/smallest singular values of V_f. As we also have $\mathrm{Cond}(V_f) = \|V_f\| \cdot \|V_f^{-1}\|$, these matrix norms also quantify how much V_f distorts the space. For a restricted, yet exponentially large, family of polynomials defining number fields, we show that both $\|V_f\|$ and $\|V_f^{-1}\|$ are polynomially bounded.

To do this, we start from $f_{n,a} = x^n - a$ whose distortion is easily computable. Then we add a "small perturbation" to this polynomial. Intuitively, the roots of the resulting polynomial should not move much, so that the norms of the "perturbed" Vandermonde matrices should be essentially the same. We formalize this intuition in Section 4.2 and locate the roots of the perturbed polynomial using Rouché's theorem.

Mapping a sample of PLWE^σ to a sample of the corresponding PLWE simply consists in changing the geometry of the noise distribution. A noise distribution with covariance matrix $\mathbf{\Sigma}$ in the Minkowski embedding corresponds to a noise distribution of covariance matrice $(V_f^{-1})^T\mathbf{\Sigma}V_f^{-1}$ in the coefficient space. The converse is also true, replacing V_f^{-1} by V_f. Moreover, the noise growths incurred by the reductions remain limited whenever $\|V_f\|$ and $\|V_f^{-1}\|$ are small.

Overall, reductions between primal-RLWE to PLWE can be obtained by combining Theorems 4.2 and 4.7 below (with Lemma 2.14 to randomize the noise distributions).

4.1 Reducing primal-RLWE to PLWE^σ

We keep the notations of the previous section, and let $\mathbb{Z}[x]/(f) = \mathcal{O}$.

Definition 4.1 (The PLWE^σ problem). *Let also $\mathbf{\Sigma}$ be a positive definite matrix, and $q \geq 2$. For $s \in \mathcal{O}/q\mathcal{O}$, we define the* PLWE^σ *distribu-*

tion $\mathcal{B}^{\sigma}_{s,\mathbf{\Sigma}}$ as the distribution over $\mathcal{O}/q\mathcal{O} \times K_{\mathbb{R}}/q\mathcal{O}$ obtained by sampling $a \hookleftarrow U(\mathcal{O}/q\mathcal{O})$, $e \hookleftarrow D^{H}_{\mathbf{\Sigma}}$ and returning the pair $(a, a \cdot s + e)$

Let $D_{\succ}$ be a distribution over $\Sigma \succ 0$. Decision PLWE^{σ} consists in distinguishing between a sampler from $\mathcal{B}^{\sigma}_{s,\mathbf{\Sigma}}$ and a uniform sampler over $\mathcal{O}/q\mathcal{O} \times K_{\mathbb{R}}/q\mathcal{O}$, with non-negligible probability over $s \hookleftarrow \mathcal{O}/q\mathcal{O}$ and $\mathbf{\Sigma} \hookleftarrow D_{\succ}$.

Theorem 4.2. *Assume that $q\mathcal{O}_K + \mathcal{C}_{\mathcal{O}} = \mathcal{O}_K$. Let $\mathbf{\Sigma}$ be a positive definite matrix and $s \in \mathcal{O}_K/q\mathcal{O}_K$. Let $t \in \mathcal{C}_{\mathcal{O}}$ such that $t\mathcal{C}_{\mathcal{O}}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$. Then the map $(a, b) \mapsto (t \cdot a, t^2 \cdot b)$ transforms $U(\mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/q\mathcal{O}_K)$ to $U(\mathcal{O}/q\mathcal{O} \times K_{\mathbb{R}}/q\mathcal{O})$ and $\mathcal{A}_{s,\mathbf{\Sigma}}$ to $\mathcal{B}^{\sigma}_{t \cdot s,\mathbf{\Sigma}'}$, where the new covariance is $\mathbf{\Sigma}' = \mathrm{diag}(|\sigma(t_i)|^2) \cdot \mathbf{\Sigma} \cdot \mathrm{diag}(|\sigma_i(t)|^2)$.*

Let $\mathcal{B}^{\sigma}_{s,\mathbf{\Sigma}}$ be a PLWE^{σ} distribution. The natural inclusion $\mathcal{O} \to \mathcal{O}_K$ induces a map that transforms $U(\mathcal{O}/q\mathcal{O} \times K_{\mathbb{R}}/q\mathcal{O})$ to $U(\mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/q\mathcal{O}_K)$ and $\mathcal{B}^{\sigma}_{s,\mathbf{\Sigma}}$ to $\mathcal{A}_{s,\mathbf{\Sigma}}$.

Proof. Let $(a, b = a \cdot s + e)$ be distributed as $\mathcal{A}_{s,\mathbf{\Sigma}}$. Let $a' = t \cdot a$ and $b' = t^2 \cdot b = a' \cdot (t \cdot s) + e'$, with $e' = t^2 \cdot e$. Then a' is uniformly distributed in $\mathcal{C}_{\mathcal{O}}/q\mathcal{C}_{\mathcal{O}}$ by applying Lemma 2.4 for $I = \mathcal{C}_{\mathcal{O}}$, $J = q\mathcal{O}_K$ and $\mathcal{M} = \mathcal{O}_K$. It is also uniformly distributed in $\mathcal{O}/q\mathcal{O}$ by combining Lemma 2.2 and Lemma 2.3. The noise follows the claimed distribution, see the observation in Section 2.2. The fact that $t \cdot s \in \mathcal{O}/q\mathcal{O}$ completes the proof that $\mathcal{A}_{s,\mathbf{\Sigma}}$ is mapped to $\mathcal{B}^{\sigma}_{t \cdot s,\mathbf{\Sigma}'}$.

Now, let (a, b) be uniform in $\mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/q\mathcal{O}_K$. We already know that a' is uniformly distributed in $\mathcal{O}/q\mathcal{O}$. Let us now consider the distribution of b'. Thanks to the assumption on $q\mathcal{O}_K$, we also have $t^2\mathcal{C}_{\mathcal{O}}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$. Therefore, by Lemma 2.4, multiplication by t^2 induces an isomorphism $\mathcal{O}_K/q\mathcal{O}_K \simeq \mathcal{C}_{\mathcal{O}}/q\mathcal{C}_{\mathcal{O}}$, and hence, by Lemmas 2.2 and 2.3, an isomorphism $\mathcal{O}_K/q\mathcal{O}_K \simeq \mathcal{O}/q\mathcal{O}$. This gives the first reduction.

We now turn to the converse reduction. By coprimality and Lemmas 2.2 and 2.4, we have $|\mathcal{O}/q\mathcal{O}| = |\mathcal{O}_K/q\mathcal{O}_K|$. This implies that any (a, b) uniform in $\mathcal{O}/q\mathcal{O} \times K_{\mathbb{R}}/q\mathcal{O}$ is also uniform in $\mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/q\mathcal{O}_K$. The inclusion $\mathcal{O} \subseteq \mathcal{O}_K$ allows to conclude. □

As Theorem 2.13, Theorem 4.2 relies on a the existence of a good multiplier. Writing $K = \mathbb{Q}[x]/(f) = \mathbb{Q}[\alpha]$ and $\mathcal{O} = \mathbb{Z}[\alpha]$, the element $f'(\alpha)$ again satisfies the constraints. Indeed, we know that $\mathcal{O}^{\vee} = \frac{1}{f'(\alpha)}\mathcal{O}$ (see [Conb, Th. 3.7]), and we have the inclusion $\mathcal{O}_K \subseteq \mathcal{O}^{\vee}$. Multiplying by $f'(\alpha)$, we obtain $f'(\alpha)\mathcal{O}_K \subseteq \mathcal{O}$. By definition, this means that $f'(\alpha) \in \mathcal{C}_{\mathcal{O}}$, as claimed. While a large $f'(\alpha)$ would mean a large noise growth in the primal-RLWE to PLWE^{σ} reduction, we described in Section 3 how to find a smaller adequate multiplier if needed.

We have $\mathcal{N}(f'(\alpha)) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K$, and, from [Ste17, p.48], the prime factors of $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ are exactly those of $\mathcal{N}(\mathcal{C}_{\mathcal{O}})$. Provided the valuations are not too high, there should be smaller elements in $\mathcal{C}_{\mathcal{O}}$ than $f'(\alpha)$. We provide in Appendix D concrete examples of number fields with defining polynomials f such that the norm of $f'(\alpha)$ is considerably larger than both the norms of $\mathcal{C}_{\mathcal{O}}$ and $(\mathcal{O}_K^{\vee})^{-1}$.

4.2 Distortion between embeddings

To bound the norms of a Vandermonde matrix associated to a polynomial and its inverse, we study the magnitude of the roots and their pairwise distances. It is known that $\|V\|^2 = \mathrm{Tr}(V^* V)$, where $*$ denotes the transpose-conjugate operator. For Vandermonde matrices, this gives

$$\|V_f\|^2 = \sum_{j\in[n]} \sum_{k\in[n]} |\alpha_j|^{2(k-1)}, \tag{1}$$

which can be handled when the magnitudes of the α_j's are known. The entries of $V_f^{-1} = (w_{ij})$ have well-known expressions as:

$$w_{ij} = (-1)^{n-i} \frac{e_{n-i}(\overrightarrow{\alpha}^j)}{\prod\limits_{k\neq j} (\alpha_j - \alpha_k)}, \tag{2}$$

where $e_0 = 1$, e_j for $j > 0$ stands for the elementary symmetric polynomial of total degree j in $n-1$ variables, and $\overrightarrow{\alpha}^j = (\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n)$, the vector of all roots but α_j. We have the following useful relations with the symmetric functions E_i of all the roots (for all j):

$$\begin{cases} E_1(\vec{\alpha}) = & \alpha_j + e_1(\overrightarrow{\alpha}^j), \\ E_i(\vec{\alpha}) = & \alpha_j e_{i-1}(\overrightarrow{\alpha}^j) + e_i(\overrightarrow{\alpha}^j) \text{ for } 2 \leq i \leq n-1, \\ E_n(\vec{\alpha}) = & \alpha_j e_{n-1}(\overrightarrow{\alpha}^j). \end{cases} \tag{3}$$

Combining (3) with Vieta's formulas, bounds on the magnitudes of the roots leads to bounds on the numerators of the w_{ij}'s. The denominators encode the separation of the roots, and deriving a precise lower bound turns out to be the main difficulty. By differentiating $f(x) = \prod_{j\in[n]}(x - \alpha_j)$, we note that $\prod_{k\neq j} |\alpha_j - \alpha_k| = |f'(\alpha_j)|$.

A FAMILY OF POLYNOMIALS WITH EASILY COMPUTABLE DISTORTION. We first introduce a family of polynomials for which $\|V_f\|$ and $\|V_f^{-1}\|$ are both simple to estimate. For $n \geq 2$ and $a \geq 1$, we define $f_{n,a} = x^n - a$.

The roots can be written[5] as $\alpha_j = a^{1/n} \mathrm{e}^{2\mathrm{i}\pi \frac{j}{n}}$, for $0 \leq j < n$. As these are scalings of the roots of unity, both their magnitude and separation are well-understood. With (1), we obtain $\|V_{f_{n,a}}\| \leq na^{\frac{n-1}{n}} \leq na$.

For any j, we readily compute $|f'_{n,a}(\alpha_j)| = na^{\frac{n-1}{n}}$. Using (3), we observe that $|e_i(\overrightarrow{\alpha}^j)| = |\alpha_j|^i$ for $1 \leq i < n$. We obtain that the row norm of $V_{f_{n,a}}^{-1}$ is given by its first row as

$$\sum_{j \in [n]} |w_{1j}| = \frac{1}{na^{\frac{n-1}{n}}} \cdot \sum_{j \in [n]} |\alpha_j|^{n-1} = 1,$$

from which it follows that $\|V_{f_{n,a}}^{-1}\| \leq \sqrt{n}$.

Small perturbations of $f_{n,a}$. Let $P(x) = \sum_{1 \leq j \leq \rho \cdot n} p_j x^j$ for some constant $\rho \in (0,1)$, where the p_j's are a priori complex numbers. Locating the roots of $g_{n,a} = f_{n,a} + P$ is our first step towards estimating $\|V_{g_{n,a}}\|$ and $\|V_{g_{n,a}}^{-1}\|$. We will use the following version of Rouché's theorem.

Theorem 4.3 (Rouché, adapted from [Con95, p.125-126]). *Let f, P be complex polynomials, and let D be a disk in the complex plane. If for any z on the boundary ∂D we have $|P(z)| < |f(z)|$, then f and $f + P$ have the same number of zeros inside D, where each zero is counted as many times as its multiplicity.*

The lemma below allows to determine sufficient conditions on the parameters such that the assumptions of Theorem 4.3 hold. We consider small disks $D_k = D(\alpha_k, 1/n)$ of radius $1/n$ around the roots $\alpha_1, \ldots, \alpha_n$ of $f_{n,a}$, and we let ∂D_k denote their respective boundaries. We let $\|P\|_1 = \sum_j |p_j|$ denote the 1-norm of P.

Lemma 4.4. *We have, for all $k \leq n$ and $z \in \partial D_k$:*

$$|P(z)| \leq (a\mathrm{e})^{\rho} \cdot \|P\|_1 \quad \textit{and} \quad |f_{n,a}(z)| \geq a \left(1 - \cos(a^{-1/n}) - \frac{2\mathrm{e}^{a^{-1/n}}}{na^{2/n}} \right).$$

Proof. Write $z = \alpha_k + \frac{\mathrm{e}^{\mathrm{i}t}}{n}$ for some $t \in [0, 2\pi)$. We have $|z| \leq a^{1/n} + 1/n$, and hence $|z|^{\rho n} \leq a^{\rho} \left(1 + \frac{1}{na^{1/n}}\right)^{\rho n}$. The first claim follows from the inequality $|P(z)| \leq \max(1, |z|^{\rho n}) \cdot \|P\|_1$.

Next, we have $|f_{n,a}(z)| = a|(1 + \frac{\mathrm{e}^{\mathrm{i}t'}}{na^{1/n}})^n - 1|$, where $t' = t - 2k\pi/n$. W.l.o.g., we assume that $k = 0$. Let Log denote the complex logarithm,

[5] For the rest of this section, 'i' will refer to the imaginary unit.

defined on $\mathbb{C} \setminus \mathbb{R}^-$. Since the power series $\sum_{k\geq 1}(-1)^{k-1}u^k/k$ converges to $\mathrm{Log}(1+u)$ on the unit disk, we have $\mathrm{Log}(1+\frac{\mathrm{e}^{\mathrm{i}t}}{na^{1/n}}) = \frac{\mathrm{e}^{\mathrm{i}t}}{na^{1/n}} + \delta$, for some δ satisfying $|\delta| \leq |u| \cdot \sum_{k\geq 1} |u|^k/(k+1) \leq |u|^2$ for $u = \frac{\mathrm{e}^{\mathrm{i}t}}{na^{1/n}}$ (note that it has modulus $\leq 1/n \leq 1/2$). Similarly, we can write $\exp(n\delta) = 1 + \varepsilon$ for some ε satisfying $|\varepsilon| \leq 2n|\delta| \leq 2/(na^{2/n})$. We hence have:

$$|f_{n,a}(z)| = a \cdot |A \cdot (1+\varepsilon) - 1| \geq a \cdot ||A-1| - |\varepsilon \cdot A||\,,$$

with $A = \exp(\mathrm{e}^{it}a^{-1/n})$. Elementary calculus (see Appendix B) leads to the inequalities $|A-1| > 1-\cos(a^{-1/n})$ and $|A| \leq \mathrm{e}^{a^{-1/n}}$ for all $t \in [0, 2\pi)$. The second claim follows. □

We note that when $a = 2^{o(n)}$ and n is sufficiently large, then the lower bound on $|f_{n,a}(z)|$ may be replaced by $|f_{n,a}(z)| > a/3$. To use Rouché's theorem, it is then enough that a, ρ and $\|P\|_1$ satisfy $a > (3\mathrm{e}^\rho \|P\|_1)^{\frac{1}{1-\rho}}$. We can now derive upper bounds on the norms of $V_{g_{n,a}}$ and its inverse.

Lemma 4.5. *For any* $a > (\|P\|_1 \cdot C^{-1} \cdot \mathrm{e}^\rho)^{\frac{1}{1-\rho}}$ *with* $C = |1-\cos(a^{-1/n}) - \frac{2\mathrm{e}^{a^{-1/n}}}{na^{2/n}}|$, *we have:*

$$\|V_{g_{n,a}}\| \leq an\mathrm{e} \quad \textit{and} \quad \|V_{g_{n,a}}^{-1}\| \leq n^{5/2}(\|P\|_1 + 1)a^{1/n}\mathrm{e}^2.$$

Proof. Let $\alpha_j = a^{1/n}\mathrm{e}^{2\mathrm{i}\pi j/n}$ be the roots of $f_{n,a}$ (for $0 \leq j < n$). Thanks to the assumptions and Lemma 4.4, Theorem 4.3 allows us to locate the roots $(\beta_j)_{0\leq j<n}$ of $g_{n,a}$ within distance $1/n$ from the α_j's. Up to renumbering, we have $|\alpha_j - \beta_j| \leq 1/n$ for all j. In particular, this implies that $|\beta_j| \leq a^{1/n} + 1/n$ for all j. The first claim follows from (1).

Another consequence is that any power less than n of any $|\beta_j|$ is $\leq a\mathrm{e}$. We start the estimation of $\|V_{g_{n,a}}^{-1}\|$ by considering the numerators in (2). Let $k_0 = 1 + \lfloor n(1-\rho) \rfloor$. For any $k < k_0$, we know that $E_k(\vec{\beta}) = 0$. Using (3), we obtain $|e_k(\overline{\vec{\beta}}^{j})| = |\beta_j|^k \leq a\mathrm{e}$ for $k < k_0$ and that $e_{k_0-1}(\overline{\vec{\beta}}^{j}) = (-1)^{k_0-1}\beta_j^{k_0-1}$. Then (3) gives $E_{k_0}(\vec{\beta}) = (-1)^{k_0}p_{n-k_0} = (-1)^{k_0-1}\beta_j^{k_0} + e_{k_0}(\overline{\vec{\beta}}^{j})$, which implies that $|e_{k_0}(\overline{\vec{\beta}}^{j})| \leq |\beta_j|^{k_0} + |p_{n-k_0}|$. By induction, we obtain, for all $k < n - k_0$:

$$\begin{aligned}|e_{k_0+k}(\overline{\vec{\beta}}^{j})| &\leq |p_{n-k_0-k}| + |p_{n-k_0-k+1}\beta_j| + \cdots + |p_{n-k_0}\beta_j^k| + |\beta_j|^{k_0+k} \\ &\leq (\|P\|_1 + 1)\max(1, |\beta_j|^n),\end{aligned}$$

so that $|e_k(\overline{\vec{\beta}}^{j})| \leq (\|P\|_1 + 1)a\mathrm{e}$ for $k \geq 1$.

We now derive a lower bound on the denominators in (2). The separation of the β_j's is close to that of the α_j's. Concretely: $|\beta_j - \beta_k| \geq |\alpha_j - \alpha_k| - 2/n$ for all j, k. Therefore, we have $\prod_{k \neq j} |\beta_j - \beta_k| \geq \prod_{k \neq j}(|\alpha_j - \alpha_k| - 2/n)$. Using the identity $|\alpha_j - \alpha_k| = 2a^{1/n} \sin(|k-j|\pi/n)$ and elementary calculus (see Appendix B), we obtain $\prod_{k \neq j} |\beta_j - \beta_k| \geq a^{\frac{n-1}{n}}/(n\mathrm{e})$. Thus any coefficient w_{ij} of $V_{g_{n,a}}^{-1}$ satisfies $|w_{ij}| \leq n(\|P\|_1 + 1)a^{1/n}\mathrm{e}^2$. The claim follows from equivalence between the row and Frobenius norms. □

We now assume that the p_j's and a are integers. The following lemma states that, for a prime and sufficiently large, the polynomial $g_{n,a}$ is irreducible, and thus defines a number field.

Lemma 4.6. *Assume that P is an integer polynomial. For any prime $a > \|P\|_1 + 1$, the polynomial $g_{n,a}$ is irreducible over $\mathbb{Q}$.*

Proof. Let β be a root of $g_{n,a}$. Then we have $a = |\beta^n + P(\beta)| \leq |\beta|^n + \|P\|_1 \max(1, |\beta|^n)$. The assumption on a implies that $|\beta| > 1$. In other words, all the roots of $g_{n,a}$ have a magnitude > 1. Now, assume by contradiction that $g_{n,a} = h_1 h_2$ for some rational polynomials h_1, h_2. Since $g_{n,a}$ is monic, it is primitive and we can choose h_1, h_2 as integer polynomials. The product of their constant coefficients is then the prime a. Hence the constant coefficient of h_1 or h_2 is ± 1, which contradicts the fact that the roots of $g_{n,a}$ have magnitude > 1. □

Overall, we have proved the following result.

Theorem 4.7. *Let $\rho \in (0,1)$ and $p_j \in \mathbb{Z}$ for $1 \leq j \leq \rho \cdot n$. Then for $a \geq (3\mathrm{e}^{\rho}\|P\|_1)^{1/(1-\rho)}$ smaller than $2^{o(n)}$ and prime, and n sufficiently large, the polynomial $g_{n,a} = x^n + \sum_{1 \leq j \leq \rho \cdot n} p_j x^j + a$ is irreducible over $\mathbb{Q}$ and satisfies:*

$$\|V_{g_{n,a}}\| \leq an\mathrm{e} \quad \textit{and} \quad \|V_{g_{n,a}}^{-1}\| \leq n^{5/2}(\|P\|_1 + 1)a^{1/n}\mathrm{e}^2.$$

In particular, if a and $\|P\|_1$ are polynomial in n, then both $\|V_{g_{n,a}}\|$ and $\|V_{g_{n,a}}^{-1}\|$ are polynomial in n.

In Appendix C, we give another family of well-behaved polynomials.

5 Search to decision dual-RLWE

The reduction relies on the recent technique of [PRSD17]. To leverage it, we use a generalized Leftover Hash Lemma over rings. The proof generalizes a technique used in [SS11] to the case where the irreducible factors of the defining polynomial (of K) reduced modulo q do not share the same degree. Alternatively, a generalization of the regularity lemma from [LPR13, Se. 7] to arbitrary number fields could be used. Such a generalization may go through and improve our results a little.

5.1 A ring-based Leftover Hash Lemma

Let $m \geq 2$. We identify any rank m $\mathcal{O}_K$-module $M \subseteq K^m$ with the lattice $\sigma(M) \subseteq H^m$. For such modules, the dual may be defined as

$$\widehat{M} = \{\mathbf{t} \in K^m \, : \, \forall \mathbf{x} \in M, \mathrm{Tr}(\langle \mathbf{t}, \mathbf{x} \rangle) \in \mathbb{Z}\}.$$

Here $\langle \cdot, \cdot \rangle$ is the K-bilinear map defined by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{m} x_i y_i$. We have $\sigma(\widehat{M}) = \overline{\sigma(M)^*}$ in H^m. For some $q \geq 2$ and a fixed $\mathbf{a} \in (\mathcal{O}_K / q\mathcal{O}_K)^m$, we focus on the modules:

$$L(\mathbf{a}) = \frac{\mathbf{a}}{q} \mathcal{O}_K^\vee + (\mathcal{O}_K^\vee)^m \quad \text{and} \quad \mathbf{a}^\perp = \{\mathbf{t} \in \mathcal{O}_K^m \; : \; \langle \mathbf{t}, \mathbf{a} \rangle = 0 \bmod q\mathcal{O}_K\}.$$

To prove our Leftover Hash Lemma variant, the main argument relies on an estimation of $\lambda_1^\infty(\widehat{\mathbf{a}^\perp})$, which is obtained by combining the following two lemmas. The first one was stated in [LS15, Se. 5] without a proof, for the case of cyclotomic fields (this restriction is unnecessary). For the sake of completeness, we give a proof in Appendix B.

Lemma 5.1. *Let $q \geq 2$ and $\mathbf{a} \in (\mathcal{O}_K / q\mathcal{O}_K)^m$. Then we have $\widehat{\mathbf{a}^\perp} = L(\mathbf{a})$.*

We now obtain a probabilistic lower bound on $\lambda_1^\infty(\widehat{\mathbf{a}^\perp}) = \lambda_1^\infty(L(\mathbf{a}))$. In full generality, it should depend on the ramification of the selected prime integer q, i.e., the exponents appearing in the factorization of $q\mathcal{O}_K$ in prime ideals. It is a classical fact that the ramified prime integers are exactly the primes dividing the discriminant of the field, so that there are only finitely many such q's. Moreover, it is always possible to use modulus switching techniques ([BLP$^+$13,LS15]) if q ramifies. Therefore, we consider only the non-ramified case.

Lemma 5.2. *Let $q \geq 2$ a prime that does not divide Δ_K. For any $m \geq 2$ and $\delta > 0$, and except with a probability $\leq 2^{3n(m+1)} q^{-mn\delta}$ over the uniform choice of $\vec{a} \in ((\mathcal{O}_K / q\mathcal{O}_K)^\times)^m$, we have:*

$$\lambda_1^\infty(L(\mathbf{a})) \geq \Delta_K^{-1/n} \cdot q^{-\frac{1}{m} - \delta}.$$

Proof. Thanks to the assumption on q, we can write $q\mathcal{O}_K = \mathfrak{p}_1 \ldots \mathfrak{p}_k$ for distinct prime ideals $\mathfrak{p}_i$. By Lemma 2.4 and the Chinese Remainder Theorem, we have $\mathcal{O}_K^\vee / q\mathcal{O}_K^\vee \simeq \mathcal{O}_K / q\mathcal{O}_K \simeq \bigoplus_{i=1}^{k} \mathbb{F}_{q^{d_i}}$, where $q^{d_i} = \mathcal{N}(\mathfrak{p}_i)$.

Let $\mathbf{a} = (a_1, \ldots, a_m)$ sampled uniformly in $((\mathcal{O}_K/q\mathcal{O}_K)^\times)^m$. Fix some bound $B > 0$ and let p_B be the probability that $qL(\mathbf{a}) = \mathbf{a}\mathcal{O}_K^\vee + q(\mathcal{O}_K^\vee)^m$ contains a $\mathbf{t} = (t_1, \ldots, t_m)$ such that $0 < \|\mathbf{t}\|_\infty < B$. Our goal is to bound p_B from above. By the union bound, we have that

$$p_B \le \sum_{s \in \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee} \sum_{\substack{\mathbf{t} \in (\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee)^m \\ 0 < \|\mathbf{t}\|_\infty < B}} p(\mathbf{t}, s),$$

with $p(\mathbf{t}, s) = \Pr_{\mathbf{a}}[\forall\, j, t_j = a_j s \bmod q\mathcal{O}_K^\vee]$ for any s and $\vec{t}$ over $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$. By independance of the a_j's, we can write $p(\mathbf{t}, s) = \prod_{j \in [m]} p(t_j, s)$ with $p(t_j, s) = \Pr_{a_j}[t_j = a_j s \bmod q\mathcal{O}_K^\vee]$. As $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ and $\mathcal{O}_K/q\mathcal{O}_K$ are isomorphic, estimating this probability amounts to studying the solutions in $(\mathcal{O}_K/q\mathcal{O}_K)^\times$ of the equation $t = as \bmod q\mathcal{O}_K$, for all $t, s \in \mathcal{O}_K/q\mathcal{O}_K$.

Note that if there is an i such that $t = 0 \bmod \mathfrak{p}_i$ and $s \neq 0 \bmod \mathfrak{p}_i$, or vice-versa, then there is no solution, so that $p(t, s) = 0$. Now, assume that s and t are 0 modulo the same $\mathfrak{p}_i$'s. Let $S \subseteq [k]$ denote the set of their indices, and let d_S be such that $q^{d_S} = \mathcal{N}(\prod_{i \in S} \mathfrak{p}_i)$. On the one hand, for all $i \in [k] \setminus S$, both t and s are invertible modulo $\mathfrak{p}_i$ so there is exactly one solution modulo those i's. On the other hand, for all $i \in S$, all the elements of $\mathbb{F}_{q^{d_i}}^\times$ are solutions. This gives $\prod_{i \in S}(q^{d_i} - 1)$ possibilities out of the $\prod_i (q^{d_i} - 1)$ elements of $(\mathcal{O}_K/q\mathcal{O}_K)^\times$. Overall, we obtain that $p(t, s) = \prod_{i \in [k] \setminus S}(q^{d_i} - 1)^{-1}$. Hence, for $\mathbf{t}$ with coordinates t_j such that s and all t_j's are 0 modulo the same $\mathfrak{p}_i$'s, we have:

$$p(\mathbf{t}, s) = q^{-m(n - d_S)} \prod_{i \in [k] \setminus S} (1 - \frac{1}{q^{d_i}})^{-m} \le q^{-m(n - d_S)} \cdot 2^{mk},$$

the last inequality coming from the fact that $1 - 1/q^{d_i} \ge 1/2$ for all i.

Let τ denote the isomorphism mapping $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ to $\mathcal{O}_K/q\mathcal{O}_K$. The probability to bound is now

$$p_B \le 2^{mk} \cdot \sum_{S \subseteq [k]} \sum_{\substack{\tau(s) \in \mathcal{O}_K/q\mathcal{O}_K \\ \forall i \in S : \mathfrak{p}_i \,|\, \tau(s)}} \sum_{\substack{\tau(\mathbf{t}) \in (\mathcal{O}_K/q\mathcal{O}_K)^m \\ 0 < \|\mathbf{t}\|_\infty < B \\ \forall\, j, \forall i \in S : \mathfrak{p}_i \,|\, \tau(t_j)}} q^{-m(n - d_S)}.$$

For any $r > 0$, we let $\mathcal{B}(r)$ denote the (open) ball in H of center 0 and radius r, with respect to the infinity norm. Such a ball has a volume $\mathrm{Vol}(\mathcal{B}(r)) = (2r)^n$. For any $S \subseteq [k]$, we define $N(B, S) = |\mathcal{B}(B) \cap \mathcal{L}(\tau^{-1}(\prod_{i \in S} \mathfrak{p}_i))| - 1$. Since there are 2^k subsets in $[k]$ and $q^{n - d_S}$ elements $\tau(s) \in \mathcal{O}_K/q\mathcal{O}_K$ such that $\mathfrak{p}_i | s$ for all $i \in S$, we have

$$p_B \leq 2^{k(m+1)} \cdot \max_{S \subseteq [k]} \frac{N(B,S)^m}{q^{(n-d_S)(m-1)}}. \tag{4}$$

We now give an upper bound for $N(B,S)$, from which we will obtain the result. Let $I_S = \prod_{i \in S} \mathfrak{p}_i$ and $\lambda_S = \lambda_1^\infty(\tau^{-1}(I_S))$. Observe that any two distinct balls of radius $\lambda_S/2$ and centered around elements of $\mathcal{B}(B) \cap \mathcal{L}(\tau^{-1}(I_S))$ do not intersect. Moreover, all of them are contained in $\mathcal{B}(B+\lambda_S/2)$. This implies that

$$N(B,S) \leq \frac{\mathrm{Vol}(\mathcal{B}(B+\lambda_S/2))}{\mathrm{Vol}(\mathcal{B}(\lambda_S/2))} = \left(\frac{2B}{\lambda_S}+1\right)^n.$$

It remains to give a lower bound on λ_S. As $\tau^{-1}(I_S) = I_S\mathcal{O}_K^\vee$, we have $\mathcal{N}(\tau^{-1}(I_S)) = q^{d_S}/\Delta_K$. With Lemma 2.5, this gives $\Delta_K^{-1/n}q^{d_S/n} \leq \lambda_S$. If we set $B = \Delta_K^{-1/n}q^\beta$, then $n\beta < d_S$ leads to $N(B,S) = 0$ and $n\beta \geq d_S$ implies the upper bound $N(B,S) \leq 2^{2n}q^{n\beta-d_S}$. With (4), this gives

$$p_B \leq 2^{(m+1)(k+2n)} \cdot \max_{\substack{S \subseteq [k] \\ d_S \leq n\beta}} q^{m(\beta-1)n+(n-d_S)}.$$

The maximum is reached for $d_S = 0$ (i.e., when $S = \emptyset$). In this case, the exponent of q is $-mn\delta$ for $\beta = 1 - \frac{1}{m} - \delta$. We obtain that $\lambda_1^\infty(qL(\mathbf{a})) \geq \Delta_K^{-1/n}q^{1-\frac{1}{m}-\delta}$ except with probability $\leq 2^{3n(m+1)}q^{-mn\delta}$. □

We are now ready to state the variant of the Leftover Hash Lemma.

Theorem 5.3. *Let $q \geq 2$ prime that does not divide Δ_K. Let $\delta > 0, \varepsilon \in (0,1/2)$ and $m \geq 2$. For a given $\mathbf{a}$ in $((\mathcal{O}_K/q\mathcal{O}_K)^\times)^m$, let $U_{\boldsymbol{a}}$ be the distribution of $\sum_{i \leq m} t_i a_i$ where the vector $\boldsymbol{t} = (t_1, \ldots, t_m)$ is sampled from $D_{\mathcal{O}_K,s}$ with $s \geq \sqrt{\log(2mn(1+1/\varepsilon))/\pi} \cdot \Delta_K^{1/n}q^{1/m+\delta}$. Then, except for $\leq 2^{3n(m+1)}q^{-mn\delta}$ of $\mathbf{a}$'s, the distance to uniformity of $U_\mathbf{a}$ is $\leq 2\varepsilon$.*

Proof. First we note that the map $\mathbf{t} \mapsto \sum_{i \leq m} t_i a_i$ is a well-defined surjective $\mathcal{O}_K$-module homomorphism from $\mathcal{O}_K^m$ to $\mathcal{O}_K/q\mathcal{O}_K$, with kernel $\mathbf{a}^\perp$. The distance to uniformity of $U_\mathbf{a}$ is hence the same as the distance to uniformity of $\mathbf{t} \bmod \mathbf{a}^\perp$. By Lemma 2.8, the claim follows whenever $s \geq \eta_\varepsilon(\mathbf{a}^\perp)$. By Lemma 2.6, t it suffices to find an appropriate lower bound on $\lambda_1^\infty(L(\mathbf{a}))$. Lemma 5.2 allows to complete the proof. □

Corollary 5.4 (Leftover Hash lemma). *If $\mathbf{t}$ is sampled from $D_{\mathcal{O}_K,s}$ with $s \geq \sqrt{\log(2mn(1+1/\epsilon))/\pi} \cdot \Delta_K^{1/n}q^{1/m+\delta}$, and the a_i's are sampled* *from $U((\mathcal{O}_K/q\mathcal{O}_K)^\times)$, then:*

$$\varDelta\ \left[\Big(a_1,\dots,a_m,\sum_{i\le m} t_i a_i\Big), U\Big(((\mathcal{O}_K/q\mathcal{O}_K)^\times)^m \times \mathcal{O}_K/q\mathcal{O}_K\Big)\right]$$
$$\le 2\varepsilon + 2^{3n(m+1)} \cdot q^{-mn\delta}.$$

5.2 Search RLWE to decision RLWE

We now give the reduction from search to decision. As all proofs can be done similarly, we focus on the dual-RLWE version of the problems. For the sake of simplicity, we consider only the case of diagonal covariance matrices. The proof readily extends to general covariance matrices. To obtain the reduction, we need to generate suitable new samples from a starting set of samples from search dual-RLWE.

The lemma below is adapted from [LS15, Le. 4.15]. We will use it to analyze the error distribution we get when generating new samples.

Lemma 5.5. *Let $\alpha > 0$, $\mathcal{L}$ a rank-m $\mathcal{O}_K$-module, $\varepsilon \in (0, 1/2)$, a vector $\mathbf{t} \in D_{\mathcal{L}+\mathbf{c},\mathbf{r}}$ for some $\boldsymbol{c} \in H^m$, and $e' \in K_{\mathbb{R}}$ chosen according to D^H_α. If $r_i \ge \eta_\varepsilon(\mathcal{L})$ and $\frac{\alpha}{\delta_i} \ge \eta_\varepsilon(\mathcal{L})$ for all i, then $\varDelta(\langle \mathbf{t}, \mathbf{e}\rangle + e', D^H_{\mathbf{x}}) \le 4\varepsilon$ with $x_i = \sqrt{(r_i\delta_i)^2 + \alpha^2}$ and $\delta_i = (\sum_{k\in[m]} |\sigma_i(e_k)|^2)^{1/2}$ for all i.*

We can now give a reduction from search dual-RLWE to worst-case decision dual-RLWE. It may be combined with the worst-case decision dual-RLWE to decision dual-RLWE from Lemma 2.14.

Theorem 5.6. *Let $\boldsymbol{r} \in (\mathbb{R}^{\ge 0})^n$ be such that $r_i = r_{i+s_2}$ for any $i > s_1$ and $r_i \le r$ for some $r > 0$. Let $d = \sqrt{n}\cdot \varDelta_K^{1/n} q^{1/m+1/n}$, and consider $\varSigma = \{\boldsymbol{r'} : r'_i \le \sqrt{d^2 \cdot r^2 \cdot m + d^2}\}$. Then there exists a probabilistic polynomial-time reduction from search dual-RLWE_{q,D_r} with $m \le q/(2n)$ input samples to worst-case decision dual-$\mathsf{RLWE}_{q,\varSigma}$.*

Proof. We have m samples $(a_i, b_i = a_i s + e_i) \in \mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/q\mathcal{O}_K^\vee$ from the dual-RLWE distribution $\mathcal{A}^\vee_{s,\mathbf{r}}$, for a uniform $s \in \mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ that we want to find. This is equivalent to finding the error term $\mathbf{e} = (e_1, \dots, e_m)$. By assumption on m, the a_i's are all invertible with non-negligible probability. If it is not the case, the reduction aborts. From now on, we hence assume that they are uniformly distributed in $(\mathcal{O}_K/q\mathcal{O}_K)^\times$.

We use the same technique as in [PRSD17], in that we find the ith embeddings $\sigma_i(e_1), \dots, \sigma_i(e_m)$ of the error terms by constructing an m-dimensional instance of the Oracle Hidden Center Problem (OHCP). The only difference consists in the way we create the samples that we give to the decision oracle. The reduction uses the dual-RLWE decision oracle to build the oracles $\mathcal{O}_i : \mathbb{R}^m \times \mathbb{R}^{\geq 0} \to \{0,1\}$ for $i \leq s_1$ and $\mathcal{O}_i : \mathbb{C}^m \times \mathbb{R}^{\geq 0} \to \{0,1\}$ for $s_1 < i \leq s_1 + s_2$.

For $i \leq s_1$, we define $k_i : \mathbb{R} \to K_{\mathbb{R}}$ as $k_i(x) = \sigma^{-1}(x \cdot \mathbf{v}_i)$ and for $s_1 < i \leq s_1 + s_2$, we define $k_i : \mathbb{C} \to K_{\mathbb{R}}$ as $k_i(x) = \sigma^{-1}(x \cdot \mathbf{v}_i + \overline{x} \cdot \mathbf{v}_{i+s_2})$, where the $\mathbf{v}_i$'s form the canonical basis of H.

On input $(z_1, \ldots, z_m, \alpha)$, oracle $\mathcal{O}_i$ will output 1 with probability depending on $\exp(\alpha)\|\mathbf{e} - \overline{\mathbf{z}}\|$, where $\overline{\mathbf{z}} = (k_i(z_1), \ldots, k_i(z_m))$. It works as follows. It first chooses a uniform $s' \in \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$. On input $(z_1, \ldots, z_m, \alpha)$, it samples $\mathbf{t} = (t_1, \ldots, t_m) \in \mathcal{O}_K^m$ Gaussian with parameter $\exp(\alpha) \cdot \sqrt{n} \cdot \varDelta_K^{1/n} q^{1/m+1/n}$ and some e' from D_d. The oracle then creates $(a', b') = (\langle \mathbf{t}, \mathbf{a} \rangle, \langle \mathbf{t}, \mathbf{b} - \bar{\mathbf{z}} \rangle + a's' + e')$, where $\mathbf{b} = (b_1, \ldots, b_m)$.

By Corollary 5.4, the distribution of $(\mathbf{a}, \langle \mathbf{t}, \mathbf{a} \rangle)$ is exponentially close to $U(((\mathcal{O}_K/q\mathcal{O}_K)^\times)^m \times \mathcal{O}_K/q\mathcal{O}_K)$. Since $b_j = a_j s + e_j$ for all j, we get $b' = a'(s + s') + \langle \mathbf{t}, \mathbf{e} - \bar{\mathbf{z}} \rangle + e'$, so oracle $\mathcal{O}_i$ creates RLWE samples for a uniformly distributed $s + s'$, provided the error term follows a suitable distribution. We let $\delta_\ell = (\sum_{j \in [m]} \sigma_\ell(e_j - k_i(z_j))|^2)^{1/2}$ for $\ell \leq n$. In particular, we have $\delta_i = \|\sigma_i(e_1) - z_1, \ldots, \sigma_i(e_m) - z_m\|$. Let us now study the distribution of the error term $\langle \mathbf{t}, \mathbf{e} - \overline{\mathbf{z}} \rangle + e'$. We can see that once the value of $\langle \mathbf{t}, \mathbf{a} \rangle = c$ and the a_i's are known, one can write $\mathbf{t} = (ca_1^{-1}, 0, \ldots, 0) + (-a_1^{-1} \sum_{i \geq 2} t_i a_i, t_2, \ldots, t_m)$, where the second vector belongs to $\mathbf{a}^\perp$. This means that the actual support of $\mathbf{t}$ is a shift of the $\mathbf{a}^\perp$ lattice by the vector $(ca_1^{-1}, 0, \ldots, 0)$. Using Lemma 5.5, we get that the distribution of the error is $D_{\mathbf{x}}^H$ where $x_j = \sqrt{\exp^2(\alpha) \cdot d^2 \cdot \delta_j^2 + d^2}$.

Let $\mathcal{S}_{i,(z_1,\ldots,z_m,\alpha)}$ be the samples obtained by applying the procedure above many times. Oracle $\mathcal{O}_i$ calls the dual-RLWE decision oracle with these and outputs 1 if and only if the latter accepts. With non-negligible probability over the choice of the initial errors, the distribution of the samples we get when we call the oracle $\mathcal{O}_i$ on $(\mathbf{0}, 0)$ belongs to the set $\varSigma$. One can now show that using the same technique as in [PRSD17], it is possible to recover good approximations of the vector $(\sigma_i(e_1), \ldots, \sigma_i(e_m))$. By substracting them from the initial search samples, rounding and then taking the inverses of the a_i's, we obtain s. □

Acknowledgments. We thank Karim Belabas, Guillaume Hanrot, Alice Pellet--Mary, Bruno Salvy and Elias Tsigaridas for helpful discussions. This work has been supported in part by ERC Starting Grant ERC-2013-StG-335086-LATTAC, by the European Union PROMETHEUS project

(Horizon 2020 Research and Innovation Program, grant 780701) and by BPI-France in the context of the national project RISQ (P141580).

References

[AD17] M. R. Albrecht and A. Deo. Large modulus Ring-LWE $\geq$ Module-LWE. In *ASIACRYPT*, 2017.

[ADPS16] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In *USENIX*, 2016.

[BBdV^{+}17] J. Bauch, D. J. Bernstein, H. de Valence, T. Lange, and C. van Vredendaal. Short generators without quantum computers: The case of multiquadratics. In *EUROCRYPT*, 2017.

[BCLvV16] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. NTRU Prime, 2016. `http://eprint.iacr.org/2016/461`.

[BDK^{+}18] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé. CRYSTALS - Kyber: a CCA-secure module-lattice-based KEM. In *EuroS&P*, 2018.

[BLP^{+}13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In *STOC*, 2013.

[BM04] Y. Bugeaud and M. Mignotte. On the distance between roots of integer polynomials. *Proceedings of Edinburgh Mathematical Society*, 47:553–556, 2004.

[BM10] Y. Bugeaud and M. Mignotte. Polynomial root separation. *International Journal of Number Theory*, 6:587–602, 2010.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT*, 2016.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. Short Stickelberger class relations and application to Ideal-SVP. In *EUROCRYPT*, 2017.

[CGS14] P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale. ETSI 2nd quantum-safe crypto workshop, 2014. `http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`, 2014.

[CIV16a] W. Castryck, I. Iliashenko, and F. Vercauteren. On the tightness of the error bound in Ring-LWE. *LMS J Comput Math*, 2016.

[CIV16b] W. Castryck, I. Iliashenko, and F. Vercauteren. Provably weak instances of Ring-LWE revisited. In *EUROCRYPT*, 2016.

[CLS15] H. Chen, K. Lauter, and K. E. Stange. Attacks on search RLWE. 2015. To appear in SIAM Journal on Applied Algebra and Geometry (SIAGA).

[CLS16] H. Chen, K. Lauter, and K. E. Stange. Vulnerable Galois RLWE families and improved attacks. In *Proc. of SAC*. Springer, 2016.

[Cona] K. Conrad. The conductor ideal. `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/conductor.pdf`.

[Conb] K. Conrad. The different ideal. Available at `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf`.

[Con95] J. B. Conway. *Functions of one complex variable*. 1995.

[DD12] L. Ducas and A. Durmus. Ring-LWE in polynomial rings. In *PKC*, 2012.

[DLL^{+}18] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS - Dilithium: digital signatures from module lattices. In *TCHES*, 2018.

[EHL14] K. Eisenträger, S. Hallgren, and K. Lauter. Weak instances of PLWE. In *SAC*, 2014.

[ELOS15] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. Provably weak instances of Ring-LWE. In *CRYPTO*, 2015.

[GHPS12] C. Gentry, S. Halevi, C. Peikert, and N. P. Smart. Ring switching in BGV-style homomorphic encryption. In *SCN*, 2012.

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, 2008.

[HHPW10] J. Hoffstein, N. Howgrave-Graham, J. Pipher, and W. Whyte. Practical lattice-based cryptography: NTRUEncrypt and NTRUSign. In *The LLL Algorithm - Survey and Applications*. Springer, 2010.

[LM06] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *ICALP*, 2006.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *JACM, 2013*, 60(6):43, 2010.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for Ring-LWE cryptography. In *EUROCRYPT*, 2013.

[LS15] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptography*, 75(3):565–599, 2015.

[Lyu16] V. Lyubashevsky. Digital signatures based on the hardness of ideal lattice problems in all rings. In *ASIACRYPT*, 2016.

[Mig00] M. Mignotte. Bounds for the roots of lacunary polynomials. *Journal of Symbolic Computation*, 30(3):325 – 327, 2000.

[MR04] D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measure. In *Proc. of FOCS*, pages 371–381. IEEE, 2004.

[Pei16] C. Peikert. How not to instantiate Ring-LWE. In *SCN*, 2016.

[PR06] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *TCC*, 2006.

[PR07] C. Peikert and A. Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *STOC*, 2007.

[PRSD17] C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of Ring-LWE for any ring and modulus. In *STOC*, 2017.

[Reg09] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[RSSS17] M. Roşca, A. Sakzad, D. Stehlé, and R. Steinfeld. Middle-product learning with errors. In *CRYPTO*, 2017.

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

[SS11] D. Stehlé and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *EUROCRYPT*, 2011.

[SS13] D. Stehlé and R. Steinfeld. Making NTRUEncrypt and NTRUSign as secure standard worst-case problems over ideal lattices, 2013. `http://perso.ens-lyon.fr/damien.stehle/NTRU.html`.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *ASIACRYPT*, 2009.

[Ste17] P. Stevenhagen. Lecture notes on *number rings*. `http://websites.math.leidenuniv.nl/algebra/ant.pdf`, 2017.

A Standard background in algebraic number theory

A number field K is a finite extension of $\mathbb{Q}$, which can always be described as $\mathbb{Q}[x]/f$ for some monic irreducible polynomial $f \in \mathbb{Z}[x]$, or $\mathbb{Q}[\alpha]$ for some root α of f. Note that a given K admits several such f's. In this setup, the polynomial f is called a defining polynomial of K and the extension degree of K is $\deg f$. The set of all elements of K whose minimal polynomials have coefficients in $\mathbb{Z}$ is a ring called the ring of integers and is denoted by $\mathcal{O}_K$. It contains the subring $\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/f$ and, in general, the inclusion is strict. Examples where $\mathcal{O}_K = \mathbb{Z}[\alpha]$ include some quadratic extensions, cyclotomic fields (i.e., when α is a primitive root of the unity) and number fields with a defining polynomial f of squarefree discriminant Δ_f. To avoid confusion with elements of $\mathcal{O}_K$, elements in $\mathbb{Z}$ are called rational integers.

A number field $K = \mathbb{Q}[\alpha]$ of degree n has exactly n ring embeddings $\sigma_i : K \to \mathbb{C}$ in the complex field. If we let $\alpha_1, \ldots, \alpha_n$ be the n roots of its defining polynomial, then these embeddings are defined by $\sigma_i(\alpha) = \alpha_i$ and extended $\mathbb{Q}$-linearly. They are often called Minkowski embeddings. If the image of an embedding is contained in the real field $\mathbb{R}$ it is said to be real, else it is said to be complex. As complex roots come by pairs of conjugates, so do the complex embeddings. We let s_1 denote the number of real embeddings and s_2 the number of pairs of complex embeddings, so that $n = s_1 + 2s_2$. The embedding map is then defined as $\sigma : K \to H$ by mapping an element in K to its vector of (suitably ordered) embeddings. Note that via the embedding map, we have $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \simeq H$. Among its nice properties, the multiplicative structure of K is preserved, i.e., $\sigma(xy) = (\sigma_1(x)\sigma_1(y), \ldots, \sigma_n(x)\sigma_n(y))$. If we are given a (geometric) norm $\|\cdot\|$ on the space $\mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$, then we can consider the geometric norm of an element in K by means of the Minkowski embeddings. The (field) trace is the $\mathbb{Q}$-linear map defined as $\mathrm{Tr}(x) = \sum_{i \leq n} \sigma_i(x)$ and the (field) norm is $N(x) = \prod_{i \leq n} \sigma_i(x)$.

Another way is to use the so-called *coefficients* embedding, which amounts to viewing an element $a = \sum_{i=0}^{n} a_i x^i$ as its vector of coefficients $\vec{a} = (a_i)_{i<n}$. Different defining polynomials for $K = \mathbb{Q}[x]/f$ give different coefficient embeddings, and coefficient and Minkowski embeddings have different geometric settings. Going from the coefficient representation $\vec{a}$ of K to its Minkowski equivalent is done by the linear transformation $\sigma(a) = V_f \vec{a}$, where V_f denotes the *Vandermonde* matrix of

$f = \prod_{i=1}^{n}(x - \alpha_i)$:

$$V_f = \begin{pmatrix} 1 \; \alpha_1 \; \dots \; \alpha_1^{n-1} \\ 1 \; \alpha_2 \; \dots \; \alpha_2^{n-1} \\ \vdots \quad\; \dots \quad \vdots \\ 1 \; \alpha_n \; \dots \; \alpha_n^{n-1} \end{pmatrix}.$$

It is well-known that the square determinant of this matrix is the discriminant of f, i.e., we have $(\det V_f)^2 = \mathit{\Delta}_f = \prod_{i \neq j}(\alpha_i - \alpha_j)$. When it defines a number field, the polynomial f does not have any double root thus V_f is invertible and we have $\vec{a} = V_f^{-1}\sigma(a)$.

B Missing proofs

Proof (Th. 2.13). First, let $(a, b = a \cdot s + e)$ be distributed as $\mathcal{A}_{s,\mathbf{\Sigma}}^{\vee}$. We define $b' = t \cdot b = a \cdot (t \cdot s) + e'$, with $e' = t \cdot e$. By Lemma 2.4, multiplication by t induces an $\mathcal{O}_K$-module isomorphism $\mathcal{O}_K^{\vee}/q\mathcal{O}_K^{\vee} \simeq \mathcal{O}_K/q\mathcal{O}_K$, hence $t \cdot s \in \mathcal{O}_K/q\mathcal{O}_K$. Also, the distribution of the error term e' is $D_{\mathbf{\Sigma}'}^{H}$. As a consequence, the sample (a, b') is distributed as $\mathcal{A}_{t \cdot s, \mathbf{\Sigma}'}$. Second, if (a, b) is uniform in $\mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/q\mathcal{O}_K^{\vee}$, as multiplying by t induces an isomorphism, we have that b' is uniform in $K_{\mathbb{R}}/q\mathcal{O}_K$, independently from a. □

Proof (Le. 4.4). Define $A(t) = \exp(\mathrm{e}^{\mathrm{i}t} a^{-1/n})$ for $t \in [-\pi, \pi]$. We have

$$\begin{aligned} \arg A(-t) &= -\arg A(t) = a^{-1/n}\sin(-t), \\ |A(-t)| &= |A(t)| = \exp(a^{-1/n}\cos(t)). \end{aligned}$$

Therefore, the graph of $A(t)$ is symmetric with respect to the real axis. We can hence restrict the study of $A(t)$ to $[0, \pi]$. As $|A(t)|$ decreases for such t's, this implies that $|A(t)| \leq |A(\pi)| \leq \mathrm{e}^{a^{-1/n}}$ for all t.

Let $\Re A(t)$ and $\Im A(t)$ respectively denote the real and imaginary parts of $A(t)$. Their derivatives are $-\exp\big(a^{-1/n}\cos(t)\big)a^{-1/n} \cdot \sin\big(t + a^{-1/n}\sin(t)\big)$ and $\exp\big(a^{-1/n}\cos(t)\big)a^{-1/n} \cdot \cos\big(t + a^{-1/n}\sin(t)\big)$, respectively. The study of their signs shows that $\Re A(t)$ decreases on $[0, \pi]$, and that there exists a $t_0 \in (\pi/4, \pi/2)$ such that $\Im A(t)$ increases on $[0, t_0]$ and decreases on $[t_0, \pi]$. We have:

- when $t \in [\pi/2, \pi]$, $\Re A(t) \leq \Re A(\pi/2)$ so that $|A(t) - 1| \geq 1 - \cos(a^{-1/n})$,
- when $t \in [\pi/4, \pi/2]$, $\Im A(t) \geq \min\{\Im A(\pi/2), \Im A(\pi/4)\}$ so that $|A(t) - 1| \geq \min\{\sin(a^{-1/n}), \mathrm{e}^{\sqrt{2}/(2a^{1/n})}\sin(\frac{\sqrt{2}}{2}a^{-1/n})\} \geq 1 - \cos(a^{-1/n})$,
- when $t \in [0, \pi/4]$, $\Re A(t) \geq \Re A(\pi/4)$, so that $|A(t) - 1| > |\Re A(\pi/4) - 1| > \mathrm{e}^{\sqrt{2}/(2a^{1/n})}\cos(\frac{\sqrt{2}}{2a^{1/n}}) - 1 \geq 1 - \cos(a^{-1/n})$.

These inequalities and the symmetry imply the claimed lower bound on $|A(t)-1|$. □

Proof (Le. 4.5). Recall that $\prod_{k\neq j}|\beta_j-\beta_k| \geq \prod_{k\neq j}(|\alpha_j-\alpha_k|-2/n)$, and that $|\alpha_j-\alpha_k| = 2a^{1/n}\sin(|k-j|\pi/n)$. Standard bounds on the sine function give that $\sin(k\pi/n)\geq 2k/n$ for $1\leq k\leq n/2$, and $\sin(k\pi/n)\geq 2-2k/n$ for $n/2<k\leq n$. We derive that:

$$\prod_{k\neq j}|\beta_j-\beta_k| \geq \prod_{k\neq j}|\alpha_j-\alpha_k|\cdot \prod_{\substack{k\neq j\\ |k-j|\leq n/2}}\left(1-\frac{1}{2a^{1/n}|k-j|}\right)^2$$

$$\geq |f'_{n,a}(\alpha_j)|\cdot\exp\left(2\sum_{1\leq k'\leq n/2}\log\left(1-\frac{1}{2a^{1/n}k'}\right)\right).$$

We have $\log(1-\frac{1}{2a^{1/n}k'})\geq\frac{-1}{a^{1/n}k'}$, and from the asymptotic expression of harmonic numbers, we can write $\sum_{k'=1}^{n/2}1/k'\leq\log(n/2)+1$. We obtain:

$$\prod_{k\neq j}|\beta_j-\beta_k| \geq na^{(n-1)/n}\cdot\left(\frac{n\mathrm{e}}{2}\right)^{-2a^{-1/n}} \geq a^{(n-1)/n}/(n\mathrm{e}).$$

□

Proof (Le. 5.1). We proceed by double inclusion, starting with $L(\mathbf{a})\subseteq\widehat{\mathbf{a}^\perp}$. Let $\mathbf{x}=(x_1,\ldots,x_m)\in\mathbf{a}^\perp$ and $\mathbf{t}=(t_1,\ldots,t_m)\in L(\mathbf{a})$. By definition, there exist $s\in\mathcal{O}_K^\vee$ and $b_1,\ldots,b_m\in\mathcal{O}_K^\vee$ such that $t_i=\frac{a_i}{q}s+b_i$, for all i. Then the element $\mathrm{Tr}(\langle\mathbf{t},\mathbf{x}\rangle)=\frac{1}{q}\mathrm{Tr}(s\langle\mathbf{a},\mathbf{x}\rangle)+\sum_{i=1}^m\mathrm{Tr}(x_ib_i)$ is an integer. Indeed, by definition of $\mathbf{x}$, the product $s\langle\mathbf{a},\mathbf{x}\rangle$ belongs to $q\mathcal{O}_K^\vee$. This implies that all traces are rational integers, which completes the proof of the first inclusion.

By duality, the reverse inclusion is equivalent to $\widehat{L(\mathbf{a})}\subseteq\mathbf{a}^\perp$. Let $\mathbf{y}\in\widehat{L(\mathbf{a})}$. As $\frac{\mathbf{a}}{q}\in L(\mathbf{a})$ we obtain that $\mathrm{Tr}(\langle\mathbf{y},\mathbf{a}\rangle)\in q\mathbb{Z}$. This implies that we have $\mathrm{Tr}(\langle\mathbf{y},\mathbf{b}\rangle)\in\mathbb{Z}$ for all $\mathbf{b}\in(\mathcal{O}_K^\vee)^m$. Taking for $\mathbf{b}$ vectors with one coordinate arbitrary in $\mathcal{O}_K^\vee$ and 0 for the rest, we see that all y_i's belong to $\mathcal{O}_K^{\vee\vee}=\mathcal{O}_K$, hence $\mathbf{y}\in\mathcal{O}_K^m$. The fact that $\mathrm{Tr}(\langle\mathbf{y},\mathbf{b}\rangle)\in\mathbb{Z}$ for all $\mathbf{b}\in(\mathcal{O}_K^\vee)^m$ also implies that $\mathrm{Tr}(s\langle\frac{\mathbf{a}}{q},\mathbf{y}\rangle)$ is an integer for all $s\in\mathcal{O}_K^\vee$, so that $\langle\frac{\mathbf{a}}{q},\mathbf{y}\rangle\in\mathcal{O}_K^{\vee\vee}=\mathcal{O}_K$. Equivalently, we have $\mathbf{y}\in\mathbf{a}^\perp$. □

C Other "good" families of polynomials

We consider polynomials as $f_{n,\varepsilon_0,\varepsilon_1}=x^n+\varepsilon_1\cdot x+\varepsilon_0$ for $\varepsilon_i\in\{\pm1\}$. Notice that this class of polynomials includes the polynomials used in [BCLvV16].

Recall that $V_{f_{n,\varepsilon_0,\varepsilon_1}}$ denotes the Vandermonde matrix associated to $f_{n,\varepsilon_0,\varepsilon_1}$. We prove the following result.

Lemma C.1. *For every $n > 2$ and any $\varepsilon_0, \varepsilon_1 \in \{\pm 1\}$, we have:*

$$\|V_{f_{n,\varepsilon_0,\varepsilon_1}}\| \le 2n \quad \text{and} \quad \|V_{f_{n,\varepsilon_0,\varepsilon_1}}^{-1}\| \le 6n^{7/2}.$$

We first use a general result on lacunary polynomials to estimate the magnitudes of the roots.

Proposition C.2 ([Mig00, Thm. 1]). *For any positive integer n and $1 \le k < n-1$, let $P(x) = x^n + a_{n-k-1}x^{n-k-1} + \cdots + a_0$ be a complex polynomial, such that $a_0 \neq 0$. For any root α of P, we have*

$$|\alpha| \le (n-k)^{\frac{1}{k+1}} \cdot \max_{1 \le j \le n} |a_{n-j}|^{1/j}.$$

In our case, we see that any root α of $f_{n,\varepsilon_0,\varepsilon_1}$ is less than $2^{\frac{1}{n-1}}$. We use this observation several times below. Thanks to Equation (1), this gives that $\|V_{f_{n,\varepsilon_0,\varepsilon_1}}\| \le 2n$.

We use (2) to estimate $\|V_{f_{n,\varepsilon_0,\varepsilon_1}}^{-1}\|$. From (3), we get that $|e_i(\overrightarrow{\alpha}^j)| = |\alpha_j|^i$ for $i \le n-2$ and $j \le n$, and $|e_{n-1}(\overrightarrow{\alpha}^j)| = |\varepsilon_0 - \alpha_j \cdot e_{n-2}(\overrightarrow{\alpha}^j)| \le 3$. We now study the denominators of (2), that we can rewrite as $f'_{n,\varepsilon_0,\varepsilon_1}(\alpha_j) = \frac{\alpha_j(1-n)\varepsilon_1 - n\varepsilon_0}{\alpha_j}$. Using the triangle inequality, we have $|\alpha_j(1-n)\varepsilon_1 - n\varepsilon_0| \ge n-(n-1)\cdot 2^{\frac{1}{n-1}}$. Since the function $g(x) = (1+1/x)^x$ is strictly increasing, so is the sequence $a_n = (1 + \frac{n+1}{n^2})^{\frac{n^2}{n+1}}$. This gives that $a_n^{1-1/n^2} = (1 + \frac{n+1}{n^2})^{n-1} \ge 2$ for any $n \ge 3$. It follows that $n-(n-1)\cdot 2^{\frac{1}{n-1}} \ge 1/n^2$ for any $n \ge 3$. We conclude by observing that $|\alpha_j| < 2$ implies that $|f'(\alpha_j)| \ge \frac{1}{2n^2}$ and then $|w_{ij}| \le 6n^2$. Equivalence between row and Frobenius norms gives the claim.

In this situation, $f_{n,\varepsilon_0,\varepsilon_1}$ may not be irreducible over $\mathbb{Q}$. For example, if $n \equiv 2 \bmod 3$ and $\varepsilon_0 = \varepsilon_1 = 1$, then the primitive third roots of unity are also roots of $f_{n,1}$, hence x^2+x+1 is a factor. A similar situation occurs with $x^2 - x + 1$ if $n \equiv 2 \bmod 6$ and $\varepsilon_0 = 1, \varepsilon_1 = -1$. This does not, however, impact the estimation of the norms.

D On small elements and $f'(\alpha)$

In Section 4.1, we discussed the possibility to use $f'(\alpha)$ for reductions between dual (resp. primal) RLWE and primal-RLWE (resp. PLWE), as it is the case that $f'(\alpha) \in \mathcal{C}_{\mathcal{O}} \cap (\mathcal{O}_K^\vee)^{-1}$. The results of Section 3 are meaningful for our applications when there are smaller elements in $(\mathcal{O}_K^\vee)^{-1}$ and $\mathcal{C}_{\mathcal{O}}$ than in the ideal generated by $f'(\alpha)$. More formally, we show that there are fields K for which

$$\lambda_1((\mathcal{O}_K^\vee)^{-1}) < \lambda_1(f'(\alpha)) \quad (\text{ resp. } \lambda_1(\mathcal{C}_{\mathcal{O}}) < \lambda_1(f'(\alpha)) \text{).}$$

By Lemma 2.5, it suffices that $\Delta_f > \Delta_K^{3/2}$ (resp. $\Delta_f > \mathcal{N}_{\mathcal{O}_K}(\mathcal{C}_{\mathcal{O}})\Delta_K^{1/2}$). Below, we give a family of number fields K of degree 3 with defining polynomials f such that $f'(\alpha)$ can have an arbitrarily large algebraic norm, relatively to those of $(\mathcal{O}_K^\vee)^{-1}$ and $\mathcal{C}_{\mathcal{O}}$.

Lemma D.1. *Let $q \neq 3$ be a prime integer such that $q^2 \not\equiv 1 \bmod 9$. Let $f = x^3 - q^2$, $K = \mathbb{Q}[x]/f$ and $\mathcal{O} = \mathbb{Z}[x]/f \simeq \mathbb{Z}[\alpha]$.*

1. *We have $\mathcal{N}(f'(\alpha)) = \Delta_f = 3^3 \cdot q^4$ and $\mathcal{N}((\mathcal{O}_K^\vee)^{-1}) = \Delta_K = 3^3 \cdot q^2$.*
2. *If $\mathcal{C}_{\mathcal{O}}$ is the conductor of $\mathcal{O}$, then $\mathcal{N}_{\mathcal{O}}(\mathcal{C}_{\mathcal{O}}) = [\mathcal{O}_K : \mathcal{O}] = q$ and $\mathcal{N}_{\mathcal{O}_K}(\mathcal{C}_{\mathcal{O}}) = q^2$.*

The family of f's considered in Lemma D.1 is restrictive. Numerical experiments suggest that polynomials $f = x^p - q^2$ with p, q distinct primes and $q^2 \not\equiv 1 \bmod p^2$ give $[\mathcal{O}_K : \mathcal{O}] = \mathcal{N}_{\mathcal{O}}(\mathcal{C}_{\mathcal{O}}) = q^{\frac{p-1}{2}}$ and $\mathcal{N}_{\mathcal{O}_K}(\mathcal{C}_{\mathcal{O}}) = q^{p-1}$.

Proof. A determinant computation gives $\Delta_f = \mathrm{Res}(f, f') = 3^3 \cdot q^4$. From this factorization and the formula $\Delta_f = [\mathcal{O}_K : \mathcal{O}]^2 \cdot \Delta_K$, we can deduce that 3 and q are the only possible prime factors of $[\mathcal{O}_K : \mathcal{O}]$. It is known (see, e.g., [Ste17, p.48]) that a prime integer p divides this index if and only if there is at least one prime $\mathcal{O}$-ideal factor of $p\mathcal{O}$ which is not invertible as an $\mathcal{O}$-ideal. This property amounts to checking divisibility between polynomials (Kummer-Dedekind's theorem, [Ste17, Thm. 3.1, p.31]), and $\mathcal{O}$ is said to be *singular* over p.

We first show that $\mathcal{O}$ is not singular over 3 but is singular over q. The reduction of f modulo 3 is $x^3 - 1 = (x-1)^3$ in $\mathbb{F}_3$. Division of f by $x - 1$ gives $f = (x-1)(x^2+x+1) + 1 - q^2$, so from the assumptions on q, 3^2 does not divide the remainder $1 - q^2$. This precisely means that $\mathcal{O}$ is not singular over 3, and we deduce that 3 divides Δ_K. On the other hand, the reduction of f modulo q is x^3 in $\mathbb{F}_q$. Division of f by x gives $f = x \cdot x^2 - q^2$, so that q^2 divides the remainder: the order $\mathcal{O}$ is singular over q. In particular, the index $[\mathcal{O}_K : \mathcal{O}]$ is either q or q^2.

From the factorization of f modulo q, we also know that the ideal $\mathfrak{p}_q = \langle q, \alpha \rangle$ is the only prime in $\mathcal{O}$ containing $q\mathcal{O}$, and that it is not invertible. From [Ste17, ex. 25, p. 53], this also means that $\mathcal{C}_\mathcal{O} \subseteq \mathfrak{p}_q$, where $\mathcal{C}_\mathcal{O}$ is the (non-trivial) conductor of $\mathcal{O}$.

Using [Ste17, Cor. 3.2, p. 32], we know that $\beta := \frac{1}{q}\alpha^2$ is not in $\mathcal{O}$. One checks that the minimal polynomial of β over $\mathbb{Q}$ is $x^3 - q$, hence $\beta \in \mathcal{O}_K$. In particular, we have a ring extension $\mathcal{O} \subseteq \mathcal{O}[\beta] \subseteq \mathcal{O}_K$. Observe that $\mathbb{Z}[\beta]$ is regular above q: reducing $x^3 - q$ modulo q gives again x^3, but the remainder by division by x is now q. Now, the order $\mathcal{O}[\beta]$ is a common extension of $\mathcal{O}$ and $\mathbb{Z}[\beta]$, and from [Ste17, Le. 3.8, p. 33], ring extensions do not add new singular primes. This implies that $\mathcal{O}[\beta]$ is a Dedekind ring in $\mathcal{O}_K$. Moreover, from [Ste17, Le. 3.20, p. 39], we get that $\mathcal{O}[\beta] = \mathcal{O}_K$. We also obtain that $q\mathcal{O}_K \subseteq \mathfrak{P}_q := \langle q, \beta \rangle = \beta\mathcal{O}_K$.

We first observe that $\beta^2 - \alpha = 0$, which means that $\mathcal{O}[\beta] = \{\lambda\beta + \mu : \lambda, \mu \in \mathcal{O}\}$. We readily check that $q(\lambda\beta + \mu)$ and $\alpha(\lambda\beta + \mu)$ are elements in $\mathcal{O}$ for any $\lambda, \mu \in \mathbb{Z}[\alpha]$, so we actually have that $\mathfrak{p}_q := \langle q, \alpha \rangle \mathcal{O} = \mathcal{C}_\mathcal{O}$. This means that $\mathcal{O}/\mathfrak{p}_q \simeq \mathbb{F}_q$ or, equivalently, that $\mathcal{N}_\mathcal{O}(\mathcal{C}_\mathcal{O}) = q$. We now show that $|\mathcal{O}[\beta]/\mathcal{O}| = [\mathcal{O} : \mathcal{C}_\mathcal{O}]$, where the left cardinality is taken for the quotient of the additive groups. Now two elements $\lambda\beta + \mu, \lambda'\beta + \mu'$ are in the same class if and only if $(\lambda - \lambda')\beta$ is in $\mathcal{O}$. This amounts to asking that $\lambda - \lambda' \in \mathcal{C}_\mathcal{O}$, so that the classes of the quotient ring $\mathcal{O}/\mathcal{C}_\mathcal{O}$ are in one-to-one correspondance with the classes of the quotient group $\mathcal{O}[\beta]/\mathcal{O}$. In other words, we have $[\mathcal{O}_K : \mathcal{O}] = q$.

We now describe $\mathcal{C}_\mathcal{O}$ as an $\mathcal{O}_K$-ideal. Since $\beta^2 = \alpha$, we have $\mathcal{C}_\mathcal{O} \subsetneq \mathfrak{P}_q = \beta\mathcal{O}_K$ as $\mathcal{O}_K$-ideals. On the other hand, we have $\mathfrak{P}_q^2 = \beta^2\mathcal{O}_K = \alpha\mathcal{O}_K \subseteq \mathcal{C}_\mathcal{O}$ as $\mathcal{O}_K$-ideals. As $\mathfrak{P}_q$ is prime in $\mathcal{O}_K$, we get $\mathcal{C}_\mathcal{O} = \mathfrak{P}_q^2$. We now obtain that $\mathcal{N}_{\mathcal{O}_K}(\mathcal{C}_\mathcal{O}) = \mathcal{N}_{\mathcal{O}_K}(\mathfrak{P}_q^2) = q^2$. □

E On Vandermonde matrices and the expansion factor

In studies of polynomial variants of LWE, the so-called expansion factor is an important parameter. For example, the reduction from PLWE to MP-LWE from [RSSS17] requires that the expansion factor of the polynomial parameterizing PLWE be small. The polynomials f for which we bound $\|V_f\|$ and $\|V_f^{-1}\|$ have small expansion factors. This naturally raises the question of the relationship between the condition number $\|V_f\| \cdot \|V_f^{-1}\|$ and the expansion factor of f. Below, we show that there exist polynomials f with small expansion factors but large $\|V_f\| \cdot \|V_f^{-1}\|$.

For a polynomial $f \in \mathbb{Z}[x]$ of degree n, the expansion factor of f is defined as

$$\mathsf{EF}(f) = \max\left\{\frac{\|g \bmod f\|_\infty}{\|g\|_\infty} : g \in \mathbb{Z}[x] \setminus \{0\}, \deg g \leq 2n\right\},$$

where $\|g\|_\infty$ is the height of the g, i.e., the largest magnitude of its coefficients. It is known [LM06] that "gap" polynomials $f = x^n + h$ with $\deg h \le n/2$ and $\|h\|_\infty \le \mathrm{poly}(n)$ satisfy $\mathsf{EF}(f) \le \mathrm{poly}(n)$. We show that this family also contains polynomials f for which $\|V_f^{-1}\|$ grows exponentially with n. For this, we use results on roots separation from Bugeaud and Mignotte [BM04,BM10].

For integers $n \ge 4, 2 \le k < n/2, a \ge 2$, consider the family of polynomials given by

$$g_{n,a,k} = x^n - 2(ax-1)^k.$$

The factor 2 is used to ensure irreducibility by way of Eisenstein's criterion. Such polynomials have a "gap" in their coefficients. Considering a, k as function of n, their expansion factors are polynomially bounded if for example $a \le \mathrm{poly}(n)$ and k is constant, or if a is constant and $k \le O(\log n)$.

Besides, Bugeaud and Mignotte showed that there is a cluster of k roots exponentially close to the real $1/a$. In particular, if the other roots are not too far away from this cluster, the denominators in (2) force $\|V_f^{-1}\|$ to be exponentially large. We adapt some results of [BM10]; in particular, we locate the roots outside the cluster to be at distance at most a from the origin. This enables us to prove that $\|V_f^{-1}\|$ is exponentially large in n.

Lemma E.1 (Adapted from [BM10]). *If $(1 + 2^{1-n/k})^{n/k} < a$, then the polynomial $g_{n,k,a}$ has k roots in the disk $D(\frac{1}{a}, \frac{1}{a^{n/k}})$.*

Proof. We apply Rouché's theorem. Write $g_{n,k,a} = f + P$, where $f = -2(ax-1)^k$, and $P = x^n$ is the "perturbation." For any $z = \frac{1}{a} + \frac{\mathrm{e}^{\mathrm{i}t}}{a^{n/k}}$ on the circle, we have $|f(z)| = \frac{2}{a^{n-k}}$ and $|P(z)| \le \big(\frac{1}{a} + \frac{1}{a^{n/k}}\big)^n$, so that the assumption gives $|P(z)| < |f(z)|$. We conclude using Theorem 4.3 and the fact that f has a root of multiplicity k in the disk. □

Lemma E.2. *If $a > 4^{\frac{n+2k}{n-2k}}$, then the polynomial $g_{n,k,a}$ has all its roots in the disk $D(\frac{1}{a}, a^{\frac{n}{2(n-k)}} - \frac{1}{a^{n/k}})$.*

Proof. Write $P = -2(ax-1)^k$ and $f = x^n$. For any z on the boundary of the disk, we have $|f(z)| \ge \big(a^{\frac{n}{2(n-k)}} - \frac{1}{a} - \frac{1}{a^{n/k}}\big)^n \ge a^{\frac{n^2}{2(n-k)}} \cdot 2^{-n}$. If we write $P = \sum_i p_i x^i$, then $|p_i| = 2a^i\binom{k}{i}$ so that $\|P\|_1 = 2(a+1)^k$. We obtain

$$|P(z)| \le \max(1, |z|^k) \cdot \|P\|_1 \le 2(a+1)^k \big(a^{\frac{n}{2(n-k)}} - \frac{1}{a} - \frac{1}{a^{n/k}}\big)^k,$$

and the assumption implies that $|P(z)| < |f(z)|$ on the boundary of the disk. We conclude using Rouché's theorem (Theorem 4.3). $\square$

The term "$-\frac{1}{a^{n/k}}$" in the radius cancels in the next proof. As a consequence of these lemmata, we can show that the inverse Vandermonde associated to $g_{n,k,a}$ has several exponentially large entries.

Proposition E.1 *Let $n \geq 4, 2 \leq k < n/2, a \geq 2$ be integers such that $a > \max\left((1+2^{1-n/k})^{n/k}, 4^{\frac{n+2k}{n-2k}}\right)$. Then $\|V_{g_{n,k,a}}^{-1}\|_\infty \geq \frac{a^{n/2-n/k}}{2^{k-1}}$.*

Proof. The assumption on a allows us to apply the two lemmata above. Let $\alpha_1, \ldots, \alpha_k$ be the roots in the disk $D(\frac{1}{a}, \frac{1}{a^{n/k}})$ (their cardinality is provided by Lemma E.1). We have, for all $i \leq k$, that $\prod_{j=1, j\neq i}^{k} |\alpha_i - \alpha_j| \leq \frac{2^{k-1}}{a^{n-n/k}}$. Let $\alpha_{k+1}, \ldots, \alpha_n$ denote the other roots. From Lemma E.2 and for $i \leq k$, we see that $\max_{j>k} |\alpha_i - \alpha_j| \leq a^{\frac{n}{2(n-k)}}$ and thus $\prod_{j\neq i} |\alpha_i - \alpha_j| \leq \frac{2^{k-1}}{a^{n/2-n/k}}$. From (2), the latter inequality implies that the k first entries in the last row of $V_{g_{n,k,a}}^{-1}$ have magnitudes at least $\frac{a^{n/2-n/k}}{2^{k-1}}$. This gives us the claim. $\square$

Proposition E.1 shows how to define polynomials for which the expansion factor is small and the inverse Vandermonde has very large entries. The following is an example. Note that there is some flexibility in the choice of a and k with respect to n to achieve the desired behavior. For example, one can also fix a and look for $k \leq C \log(n)$ for a constant $C > 0$.

Corollary E.3. *For $k = 3$ and $5 \leq a \leq \mathrm{poly}(n)$, the polynomials $g_{n,3,a}$ satisfy*

$$\mathsf{EF}(g_{n,3,a}) \leq \mathrm{poly}(n) \quad \textit{and} \quad \|V_{g_{n,3,a}}^{-1}\| \geq 2^{\Omega(n)}.$$