A unified reduction from RLWE to MP-LWE

Alice Pellet-Mary[1] and Wenwen Xia[2,1⋆]

[1] Univ Bordeaux, CNRS, Inria, Bordeaux INP, IMB, UMR 5251, Talence, France
{alice.pellet-mary, wenwen.xia}@math.u-bordeaux.fr
[2] Shanghai Jiao Tong University, China

Abstract. The Middle-Product Learning With Errors (MP-LWE) problem, introduced by Roşca, Sakzad, Steinfeld, and Stehlé (Crypto 2017), is a structured variant of LWE defined independently of any specific number field K. Its hardness has been based on the hardness of Ring-LWE (RLWE) over families of number fields. Two main reductions exist, one from Roşca, Sakzad, Steinfeld, and Stehlé (Crypto'17) and Njah Nchiwo and Pellet-Mary (PKC'26), and another one due to Peikert and Pepin (Journal of Cryptology'24). Both reductions cover different families of number fields, and none of the two supersedes the other.
In this work, we propose a unified reduction from RLWE to MP-LWE parameterized by a pair of field elements $(y_a, y_s) \in K^2$, which recovers both prior reductions as concrete instantiations. Optimizing the choice of (y_a, y_s), we obtain the first reduction from RLWE to MP-LWE that holds for all number fields $K = \mathbb{Q}[X]/f(X)$ where f is a monic irreducible polynomial of a given degree and with polynomially bounded coefficients (and whose discriminant is coprime to the modulus q of the RLWE and MP-LWE problems, a constraint that also appeared in previous works). This new reduction supersedes the two previously known reductions.

Keywords: Middle-Product Learning with Errors · Ring Learning with Errors · Reductions (complexity theory)

1 Introduction

Over the past decade, structured lattices have become a foundation for efficient post-quantum cryptographic primitives. The Ring/Module Learning With Errors (RLWE/MLWE) problems [SSTX09,LPR10,BGV14,LS15] achieve significant gains in efficiency and key compactness over plain LWE by introducing algebraic structure into the underlying lattices. Concretely, these problems are defined over a number field $K = \mathbb{Q}[X]/f(X)$, where $f(X) \in \mathbb{Z}[X]$ is some monic irreducible polynomial of degree m. It was proven in [SSTX09, LPR10, LS15] that solving the RLWE/MLWE problems over a field K is no easier than finding short vectors in lattices that are modules of K. Overall, the hardness of the RLWE and MLWE problems is highly dependent on the choice of the number field K. This dependency raises a natural concern: do there exist "weak" defining polynomials

⋆ Corresponding author.

f, for which these structured LWE problems become significantly easier? While we do not have examples of number fields over which RLWE or MLWE would be significantly easier than over other fields, we are also unable to prove reductions for RLWE/MLWE from one field to another.

In response to this concern, Roşca et al. [RSSS17] introduced the Middle-Product LWE (MP-LWE) problem. Since its introduction in 2017, this problem has been used to construct multiple cryptographic primitives, such as public key encryption [RSSS17,SSZ19,BBD+19], (ring) signatures [Hir18,BDH+20,DAZ19, LSW+23], (hierarchical) IBE [LVV19,FLA23], etc. Unlike RLWE and MLWE, the MP-LWE problem is defined independently of any specific polynomial f. Its hardness was first established in [RSSS17] via a reduction from Polynomial Learning with Errors (PLWE), and the central object of that reduction is the so-called Hankel matrix $\mathbf{M}_f \in \mathbb{Z}^{m\times m}$ whose (i,j)-th entry is the constant coefficient of $x^{i+j-2} \bmod f$. The spectral norm $\|\mathbf{M}_f\|$ governs the noise growth in this reduction from PLWE to MP-LWE. A complementary reduction from (primal) RLWE to PLWE was given by Roşca et al. [RSW18], whose noise growth is captured by the inverse Vandermonde matrix $\mathbf{V}_f^{-1}$ associated with the roots of f. Composing both reductions yields a chain

$$\mathsf{RLWE} \longrightarrow \mathsf{PLWE} \longrightarrow \mathsf{MP\text{-}LWE}$$

in which the cumulative error expansion of the two steps was originally analyzed independently and bounded by the pessimistic product $\|\mathbf{M}_f\| \cdot \left\|\mathbf{V}_f^{-1}\right\|$. Roşca et al. [RSSS17,RSW18] provided an infinite family of polynomials for which the two quantities $\|\mathbf{M}_f\|$ and $\left\|\mathbf{V}_f^{-1}\right\|$ remain polynomially bounded (as a function of the degree m of f). Hence, they obtain the guarantee that for some well chosen parameters, the MP-LWE problem is at least as hard as RLWE for *all* polynomials of this infinite family.

This initial reduction was then improved in two follow-up works, whose results are complementary. In the first article, Peikert and Pepin [PP24] build on the order LWE framework of [BBPS19], and obtain a new reduction from (dual) RLWE to MP-LWE, whose total noise expansion is bounded by the spectral norm $\|\mathbf{V}_f\|$ of the Vandermonde matrix. They also provide an infinite family of polynomials for which this quantity remains polynomially bounded, and they show that this family includes the one from the original reductions [RSSS17,RSW18]. While this family of polynomials is infinite, it remains very sparse among the family of all (monic irreducible) polynomials of bounded degree and coefficients.

In the second follow-up article, Njah Nchiwo and Pellet-Mary [NP26] jointly analyzed the two steps of the chain reduction from [RSSS17,RSW18], exploiting the fact that the distortions $\mathbf{V}_f^{-1}$ and $\mathbf{M}_f$ largely compensate one another. The resulting bound $\left\|\mathbf{M}_f\mathbf{V}_f^{-1}\right\|$ is experimentally small for at least 90% of monic irreducible polynomials of fixed degree and polynomially bounded coefficients, extending the provable hardness of MP-LWE to a much broader class of polynomials. Interestingly, it was noted in [NP26] that the two bounds $\|\mathbf{V}_f\|$ (from [PP24]) and $\left\|\mathbf{M}_f\mathbf{V}_f^{-1}\right\|$ (from [NP26]) capture complementary phenom-

ena. There exists families of polynomials for which one bound remains polynomial while the other one grows exponentially quickly (with the degree of the polynomials), and vice versa. It was also noted in [NP26] that the two reductions from [RSSS17,RSW18] and from [PP24] seem quite different at a first sight. This motivates the following question:

Is it possible to combine both reductions and obtain a new reduction from RLWE *to* MP-LWE *whose noise growth remains polynomially bounded for all monic irreducible polynomials f?*

1.1 Our contributions

We introduce a unified reduction framework from RLWE to MP-LWE, that captures both previously known reductions from [RSSS17,RSW18,NP26] and [PP24]. Using our framework, we are able to obtain a new reduction from RLWE to MP-LWE that supersedes the two former reductions. More precisely, we are able to prove hardness of the MP-LWE problem from the hardness of the RLWE problem for *all* monic irreducible polynomials f of degree m with coefficients bounded by some $B = \mathrm{poly}(m)$, subject only to a coprimality condition between the discriminant of f and the modulus q.[3] As a concrete highlight, our framework covers specific families of polynomials (e.g. $f(x) = x^m - bx^{m-1} + b(ax-1)^2$, for m, a, b integers with $m \geq 4$ and $a, b \geq 2$) that simultaneously break the conditions required by both previous reductions, while still enjoying a polynomial noise growth in our setting.

In detail, we prove the following theorem:

Theorem 1.1 (Informal, see Corollary 5.4). *Let f be a monic irreducible polynomial of degree m with coefficients bounded by B in absolute value, and assume that the discriminant Δ_f of f is coprime to q. Let $K = \mathbb{Q}[X]/f(X)$, and $\alpha \in (0,1)$. Then* RLWE *in the number field K, with modulus q and error of size αq reduces in polynomial time to* MP-LWE *with modulus q and error of size $\alpha' q$ for some $\alpha' \leq \alpha \cdot 16\, m^8 B^5$.*

Experimentally, we observe that the actual noise expansion is several orders of magnitude smaller than the bound proven in the theorem.[4]

1.2 Technical overview

For simplicity in this technical overview, we focus on polynomials f for which the field $K = \mathbb{Q}[X]/f(X)$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[X]/f(X)$ (i.e., K is monogenic). Let m be the degree of f, and B be a bound on the absolute value

[3] This condition can be relaxed to a coprimality condition between the norm of the conductor ideal of the order $\mathbb{Z}[X]/f(X)$ and the modulus q, but for simplicity we only mention the discriminant of f in this introduction.

[4] The code for our experiments is available at `https://github.com/Summwer/code-unified-reduction-MP-LWE`.

of the coefficients of f. Thanks to our assumption, the ring of integers $\mathcal{O}_K$ admits a $\mathbb{Z}$-basis given by $(p_1, \ldots, p_m) := (1, X, \ldots, X^{m-1})$. This basis also defines a $\mathbb{Q}$-basis of K, and we call it the *power basis*. Another basis will play an important role in our reduction, which we call the *dual basis*, and which is defined as the dual of the power basis (for some definition of duality over a number field which is not important here). We write this dual basis $(p_1^\vee, \ldots, p_m^\vee)$. This is also a $\mathbb{Q}$-basis of K, and the $\mathbb{Z}$-span of this dual basis is known as the dual of $\mathcal{O}_K$, denoted by $\mathcal{O}_K^\vee$. This set satisfies the two following useful properties: $\mathcal{O}_K \cdot \mathcal{O}_K^\vee = \mathcal{O}_K^\vee$ and $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee \subseteq K$.

For simplicity, we will focus on the primal RLWE problem in this technical overview. Our reduction however works in a similar way for the dual RLWE problem, and all the results we mention below still hold for dual RLWE (with only some minor changes). The (primal) RLWE problem is defined as follows. For a uniformly sampled secret $s \xleftarrow{\$} \mathcal{O}_K/q\mathcal{O}_K$, given access to multiple pairs of the form (a_i, b_i) where $a_i \xleftarrow{\$} \mathcal{O}_K/q\mathcal{O}_K$ and $b_i = a_i s + e$ for some small e, recover the secret s. The smallness of e is defined using a map from K to $\mathbb{C}^m$ called the canonical embedding, whose precise definition is not useful here.

Our reduction framework from RLWE to MP-LWE is obtained via a very simple algorithm described below. This algorithm is parameterized by an element $y \in K$, it takes as input an RLWE pair (a, b), and outputs an MP-LWE pair (a', b').[5]

Parameters: $y \in K \setminus \{0\}$;
Input: $(a, b) \in \mathcal{O}_K/q\mathcal{O}_K \times \mathcal{O}_K/q\mathcal{O}_K$;

1. $a' \leftarrow$ coordinates of a in the *power* basis;
2. $b' \leftarrow$ coordinates of $y \cdot b$ in the *dual* basis;
3. **return** (a', b').

We prove that for any choice of $y \in \mathcal{O}_K^\vee$, the algorithm above transforms (primal) RLWE samples (a, b) with secret s into MP-LWE samples (a', b') with some secret s'.[6] Note that the new secret s' is not guaranteed to be uniform in $\mathbb{Z}_q^m$, but it will be rerandomized later, using standard techniques. One can verify that since $a \in \mathcal{O}_K$ and since $y \cdot b \in \mathcal{O}_K^\vee \cdot \mathcal{O}_K = \mathcal{O}_K^\vee$, then the coordinate vectors a' and b' have integer coordinates as desired.[7]

We also show that this reduction framework captures the two reductions from [RSSS17,RSW18,NP26] and [PP24]. The reduction from [PP24] is recovered by choosing $y = 1$, and the reduction from [RSSS17, RSW18, NP26] is obtained by taking $y = p_1^\vee$ (the first element of the dual basis).

It then remains to analyze the noise growth induced by this reduction for an arbitrary $y \in \mathcal{O}_K^\vee$. We perform the analysis, and we obtain that the reduction (parameterized by y) multiplies the error by a matrix of the form $\mathbf{V}_f^\top \mathbf{T}(y)$, where $\mathbf{V}_f \in \mathbb{C}^{m \times m}$ is the Vandermonde matrix associated to the roots of f as

[5] When the field is non monogenic, the reduction is actually parameterized by two elements $(y_a, y_s) \in K^2$.
[6] We abuse notation here and see the vectors (a', b') as polynomials of degree m.
[7] In the case of dual RLWE, we have $b \in \mathcal{O}_K^\vee$ and so we should take $y \in \mathcal{O}_K$ instead.

above, and $\mathbf{T}(y) \in \mathbb{C}^{m \times m}$ is a diagonal matrix whose diagonal coefficients are given by the canonical embedding of y. This implies that our reduction increases the noise rate by a multiplicative factor $\left|\left|\left|\mathbf{V}_f^\top \mathbf{T}(y)\right|\right|\right|$. Choosing $y = 1$, we show that $\left|\left|\left|\mathbf{V}_f^\top \mathbf{T}(1)\right|\right|\right| = |||\mathbf{V}_f|||$, and taking $y = p_1^\vee$, we prove that $\left|\left|\left|\mathbf{V}_f^\top \mathbf{T}(p_1^\vee)\right|\right|\right| = \left|\left|\left|\mathbf{M}_f \mathbf{V}_f^{-1}\right|\right|\right|$, confirming that our analysis for arbitrary y is as good as the two special case analyses of [PP24] and [NP26] when $y = 1$ and $y = p_1^\vee$.

Finally, we prove the existence of an element $y \in \mathcal{O}_K^\vee$ such that $\left|\left|\left|\mathbf{V}_f^\top \mathbf{T}(y)\right|\right|\right| \leq 16m^8 B^5$. To do so, we observe that proving the existence of such a y amounts to proving the existence of a sufficiently short vector in a given lattice (depending on f), and we use Minkowski's first theorem to prove the existence of such a short lattice vector. Overall, taking this y in our reduction framework, we obtain a reduction from RLWE in K to MP-LWE that increases the noise rate by a factor which is polynomial in m and B, for any choice of polynomial f (assuming that $\mathcal{O}_K = \mathbb{Z}[X]/f(X)$, see below for a discussion about the general case). Note that we proved the existence of a reduction, but making this reduction explicit is, for the moment, a computationally hard task. Indeed, the reduction needs to know y, and the only way we know to compute an optimal y is to solve a shortest vector problem in a lattice depending on f. Said differently, our reduction is non-uniform.

Let us finally comment on the non-monogenic case, i.e., when $\mathcal{O}_K$ is not equal to $\mathbb{Z}[X]/f(X)$. In this case, we introduce the order $\mathcal{O} = \mathbb{Z}[X]/f(X)$, which is contained in $\mathcal{O}_K$. This order comes with an ideal $\mathcal{C}_\mathcal{O} \subseteq \mathcal{O}_K$, called the *conductor ideal* of $\mathcal{O}$, which is such that for any $x \in \mathcal{O}_K$ and $y \in \mathcal{C}_\mathcal{O}$, the product xy is in $\mathcal{O}$. For our reduction framework, we will now need to consider a pair of elements $(y_a, y_s) \in K^2$ instead of a single element y. The element y_s will play the same role as y in our discussion above, and the element y_a will be an element of $\mathcal{C}_\mathcal{O}$ that is used to map elements of $\mathcal{O}_K$ into elements of $\mathcal{O}$ (by multiplying them with y_a). For some technical reasons, if we want that the multiplication by y_a induces a bijection from $\mathcal{O}_K/q\mathcal{O}_K$ into $\mathcal{O}/q\mathcal{O}$, we need that $y_a\mathcal{O}_K$ be coprime with $q\mathcal{O}_K$. This is the reason why we need to assume that the conductor ideal $\mathcal{C}_\mathcal{O}$ is coprime with $q\mathcal{O}_K$. A similar constraint appeared for the same reason in all previously known reductions. A sufficient and simpler condition to ensure that $\mathcal{C}_\mathcal{O}$ is coprime with $q\mathcal{O}_K$ is to require that the discriminant Δ_f of f is coprime to q. We note though that this is not a necessary condition.

Discussion and open problem. One may wonder whether the coprimality condition between $\mathcal{C}_\mathcal{O}$ and $q\mathcal{O}_K$ is an artifact of the proof or not. For a given f, the condition does seem necessary for our framework to work. However, observe that multiple polynomials f can define the same number field K (up to isomorphism). It would be interesting to see whether, for a given number field K, one can prove the existence of a "good" defining polynomial f, i.e., a polynomial with coefficients bounded by B (for some not too large B) and such that $\mathcal{C}_\mathcal{O}$ is coprime to $q\mathcal{O}_K$ for $\mathcal{O} = \mathbb{Z}[X]/f(X)$.

Another limitation of our reduction is that it is non-uniform, since computing a good element y (minimizing $\left\|\left\|\mathbf{V}_f^\top \mathbf{T}(y)\right\|\right\|$) may be costly. We view this limitation as less important than the coprimality condition. Indeed, our non-uniform reduction implies that if an attack is found against MP-LWE, then this would prove the existence of attacks against RLWE for a huge class of number fields. As far as we know, even if we were given an infinite amount of time to perform pre-computations on the number field K, this would not help solve RLWE in K. So proving the existence of (non-uniform) attacks against RLWE would already be a big surprise. Still, it would be interesting to see if the reduction can be made uniform. For example, the choice of $y = 1$ done in [PP24] makes their reduction uniform (but it covers only a smaller class of polynomials).

Finally, as we noted above, our reduction seems to behave much better in practice than our proven bounds suggest. It would be interesting to see if there exists some polynomials reaching our proven bounds, or whether these bounds can be improved to better match the experimental results.

2 Preliminaries

2.1 Notations

Let $\mathbb{R}$ denote the field of real numbers and $\mathbb{Z}$ denote the ring of integers. For an integer $q \geq 2$, let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ be the ring of integers modulo q and $\mathbb{R}_q = \mathbb{R}/q\mathbb{Z}$ be the set of real numbers modulo q.

We use bold letters to denote vectors and matrices, with upper case letters for matrices (e.g., $\mathbf{A}$) and lower case letters for vectors (e.g., $\mathbf{v}$). For a vector $\mathbf{v} = (v_1, \ldots, v_n)$, we denote by $\overleftarrow{\mathbf{v}} = (v_n, \ldots, v_1)$ the vector with reversed coordinates.

For any finite or compact set S, we let $\mathcal{U}(S)$ denote the uniform distribution over S. For a distribution $\mathcal{D}$, we write $x \leftarrow \mathcal{D}$ to indicate that x is sampled from distribution $\mathcal{D}$.

2.2 Number Field

Let $K := \mathbb{Q}(\zeta)$ be an algebraic number field, i.e., a finite-dimensional field extension of the rationals $\mathbb{Q}$. For any number field K, there exists a monic irreducible polynomial $f \in \mathbb{Z}[X]$ such that K is isomorphic to $\mathbb{Q}[X]/f(X)$. The degree of f is called the degree of K, and we will write it m throughout the article. We denote by Δ_K the absolute value of the discriminant of the field K. We write $K_\mathbb{R}$ the set $K \otimes_\mathbb{Q} \mathbb{R}$, which is isomorphic to $\mathbb{R}[X]/f(X)$ for f as above.

Embeddings. An embedding of a number field K to the complex field $\mathbb{C}$ is an homomorphism of fields $\sigma : K \to \mathbb{C}$. A field K of degree m admits m distinct embeddings from K to $\mathbb{C}$, which we will denote $\sigma_1, \ldots, \sigma_m$. These embedding can be extended to the set $K_\mathbb{R}$, and we keep the same notation for simplicity. We denote by $\tau(x)$ the canonical embedding which maps $K_\mathbb{R}$ into $\mathbb{C}^m$ as

$$\begin{aligned} \tau : K_\mathbb{R} &\to \mathbb{C}^m, \\ x &\mapsto (\sigma_1(x), \ldots, \sigma_m(x))^\top. \end{aligned}$$

We also define $\mathbf{T}(x) = \mathrm{diag}(\sigma_1(x), \dots, \sigma_m(x)) \in \mathbb{R}^{m\times m}$. Let Tr and $\mathcal{N}$ denote the trace and algebraic norm from $K_\mathbb{R}$ to $\mathbb{R}$. For any $x \in K_\mathbb{R}$, we have $\mathrm{Tr}(x) = \sum_{i=1}^m \sigma_i(x)$ and $\mathcal{N}(x) = \prod_{i=1}^m \sigma_i(x)$.

Power and dual bases. In this article, we will only consider number fields of the form $K = \mathbb{Q}[X]/f(X)$ for some monic irreducible polynomial f of degree m. Note that different polynomials $f_1 \neq f_2$ may lead to isomorphic fields $K_1 = \mathbb{Q}[X]/f_1(X) \simeq K_2 = \mathbb{Q}[X]/f_2(X)$. For many properties, we would like to consider K_1 and K_2 as the same objects, however, some of the properties we consider will depend on the choice of the defining polynomial f, so we will always make the defining polynomial f explicit.

The set $(1, X, X^2, \dots, X^{m-1})$ forms a $\mathbb{Q}$-basis of the field K. We will call this special basis the *power basis* of K. In order to simplify notations later on, we will denote by $p_i = X^{i-1}$ for $1 \leq i \leq m$ the elements of this basis. There exists also a dual basis to this power basis. More precisely, there exists elements $p_1^\vee, \dots, p_m^\vee \in K$ such that, for all i, j, $\mathrm{Tr}(p_i p_j^\vee) = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta function (see, e.g., [Con09b, Theorem 3.7] for an explicit description of such dual basis in the special case where $(p_i)_i$ is a power basis). The set $(p_1^\vee, \dots, p_m^\vee)$ also forms a $\mathbb{Q}$-basis of K, which we will call the *dual basis* of K.

For any element $a \in K_\mathbb{R}$, we will denote by $\pi(a) \in \mathbb{R}^m$ the vector of the coefficients of a in the power basis $(p_1, \dots, p_m)$, i.e.,

$$\begin{aligned} \pi : \quad & K_\mathbb{R} \to \mathbb{R}^m \\ & \sum_i a_i p_i \mapsto (a_1, \dots, a_m)^\top. \end{aligned} \tag{1}$$

And we will denote by $\pi^\vee(a) \in \mathbb{R}^m$ the vector of the coefficients of a in the dual basis $(p_1^\vee, \dots, p_m^\vee)$, i.e.,

$$\begin{aligned} \pi^\vee : \quad & K_\mathbb{R} \to \mathbb{R}^m \\ & \sum_i a_i p_i^\vee \mapsto (a_1, \dots, a_m)^\top. \end{aligned} \tag{2}$$

Note that if $a \in K$, then both $\pi(a)$ and $\pi^\vee(a)$ are in $\mathbb{Q}^m$.

Lemma 2.1. *For any $a \in K_\mathbb{R}$ with degree m and any $1 \leq i \leq m$, it holds that*

$$(\pi(a))_i = \mathrm{Tr}(a \cdot p_i^\vee) \tag{3}$$

$$\text{and} \quad (\pi^\vee(a))_i = \mathrm{Tr}(a \cdot p_i). \tag{4}$$

Proof. To prove the first equality, let us write $\pi(a) = (a_1, \dots, a_m)$ the coordinates of a in the power basis. Then, we may compute

$$\mathrm{Tr}(p_i^\vee \cdot a) = \mathrm{Tr}(p_i^\vee \cdot \sum_{k=1}^m a_k p_k) = \sum_{k=1}^m a_k \cdot \mathrm{Tr}(p_i^\vee \cdot p_k) = a_i = (\pi(a))_i,$$

where in the second equality we used the $\mathbb{R}$-linearity of the trace map (observe that $a_k \in \mathbb{R}$), and in the third equality we used the fact that $\mathrm{Tr}(p_i^\vee \cdot p_k) = \delta_{i,k}$.

The second equality of the lemma is obtained in a similar way by inverting p_i and $p_i^\vee$, and considering the coordinates of a in the dual basis. □

For any $a \in K_\mathbb{R}$, one can relate the canonical embedding $\tau(a)$ of a to its coordinates in the power and dual bases $\pi(a)$ and $\pi^\vee(a)$, thanks to the Vandermonde matrix associated to f.

Definition 2.2 (Vandermonde matrix). *Let $f \in \mathbb{C}[x]$ be a polynomial of degree m with complex roots $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$, the Vandermonde matrix associated to the polynomial f is defined as*

$$\mathbf{V}_f = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_m \end{bmatrix} = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \cdots & \alpha_m^{m-1} \end{bmatrix}.$$

Lemma 2.3. *Let $K = \mathbb{Q}[X]/f(x)$. For any $a \in K_\mathbb{R}$, it holds that*

$$\tau(a) = \mathbf{V}_f \cdot \pi(a) = \mathbf{V}_f^{-\top} \cdot \pi^\vee(a).$$

Proof. Let us write $a = \sum_{i=1}^m a_i p_i$, so that $\pi(a) = (a_1, \cdots, a_m)^\top$. Suppose the complex roots of f are $\alpha_1, \cdots, \alpha_m$. By definition of τ, we have

$$\begin{aligned} \tau(a) &= (\sigma_1(a), \ldots, \sigma_m(a))^\top \\ &= (\sum_{i=1}^m a_i \alpha_1^{i-1}, \ldots, \sum_{i=1}^m a_i \alpha_m^{i-1})^\top = \mathbf{V}_f \cdot \pi(a), \end{aligned}$$

since $\sigma_i(a) = a(\alpha_i)$.

To obtain the second equality, let us define $\mathbf{G} = \mathbf{V}_f^\top \mathbf{V}_f$, the Gram matrix associated to $\mathbf{V}_f$. Observe that $\mathbf{G}_{ij} = (\mathbf{V}_f^\top \mathbf{V}_f)_{ij} = \sum_{k=1}^m \sigma_k(p_i)\sigma_k(p_j) = \mathrm{Tr}(p_i p_j)$. From Lemma 2.1, the coordinates of a in the dual basis are $\pi^\vee(a) = (\mathrm{Tr}(a \cdot p_1), \cdots, \mathrm{Tr}(a \cdot p_m))^\top = \mathbf{G} \cdot \pi(a)$. Overall, we obtain $\mathbf{V}_f^{-\top} \cdot \pi^\vee(a) = \mathbf{V}_f^{-\top} \cdot \mathbf{G} \cdot \pi(a) = \mathbf{V}_f^{-\top} \cdot (\mathbf{V}_f^\top \mathbf{V}_f) \cdot \pi(a) = \mathbf{V}_f \cdot \pi(a)$ as desired. □

Orders. We denote by $\mathcal{O}_K$ the ring of integers of K. An order $\mathcal{O}$ of K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ whose $\mathbb{Z}$-rank is maximal. In particular, $\mathcal{O}_K$ is an order, which is called the maximal order, since every order $\mathcal{O}$ of K satisfies $\mathcal{O} \subseteq \mathcal{O}_K$.

For any order $\mathcal{O} \subseteq K$, its dual $\mathcal{O}^\vee$ is defined as $\mathcal{O}^\vee = \{x \in K : \mathrm{Tr}(x \cdot \mathcal{O}) \subseteq \mathbb{Z}\}$. In this article, the only non-maximal order we will consider is $\mathcal{O} = \mathbb{Z}[X]/f(X)$. This order is interesting for us because the power basis $\{p_i\}_i$ (where $p_i = X^{i-1}$) is precisely a $\mathbb{Z}$-basis of $\mathcal{O}$. In particular, for any $a \in K_\mathbb{R}$, we have that $\pi(a) \in \mathbb{Z}^m$ if and only if $a \in \mathcal{O}$. Likewise, the dual basis $\{p_i^\vee\}_i$ is a $\mathbb{Z}$-basis of the dual $\mathcal{O}^\vee$ of $\mathcal{O}$ (see, e.g., [Con09b, Theorem 3.4]). In particular, for any $a \in K_\mathbb{R}$, we have that $\pi^\vee(a) \in \mathbb{Z}^m$ if and only if $a \in \mathcal{O}^\vee$.

A field K is said to be *monogenic* if there exists an element $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. When this is the case, we have that $K = \mathbb{Q}(\alpha) \simeq \mathbb{Q}[X]/f(X)$

and $\mathcal{O}_K = \mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/f(X)$, where $f \in \mathbb{Z}[x]$ is the minimal polynomial of α. In this article, when we consider monogenic number fields, they will always be of the form $K = \mathbb{Q}[X]/f(X)$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[X]/f(X)$. In other words, the fields and ring of integers are not simply isomorphic to a polynomial ring of the desired shape, they are actually equal to these polynomial rings.

Ideals. An integral ideal is a subset $I \subseteq \mathcal{O}_K$ that is stable by addition and multiplication by any element of $\mathcal{O}_K$. A fractional ideal is a subset $I \subset K$ such that there exists $\alpha \in K$ for which $\alpha \cdot I$ is an integral ideal. Non-zero fractional ideals of $\mathcal{O}_K$ form a multiplicative group. In particular, each non-zero ideal has an inverse. Given two integral ideals I and J, we say that J divides I if $I \subseteq J$. We say that I is coprime to J if $I + J = \mathcal{O}_K$. The algebraic norm $\mathcal{N}(I)$ of an integral ideal $I \subseteq \mathcal{O}_K$ is equal to the index of I in $\mathcal{O}_K$, i.e., the cardinality of $\mathcal{O}_K/I$. For a fractional ideal I, if $\alpha \in K$ is such that $\alpha \cdot I$ is an integral ideal, we define the algebraic norm of I by $\mathcal{N}(I) = |\mathcal{N}(\alpha)|^{-1} \cdot \mathcal{N}(\alpha I)$. This does not depend on the choice of α. The algebraic norm of ideals is multiplicative, i.e., $\mathcal{N}(I \cdot J) = \mathcal{N}(I) \cdot \mathcal{N}(J)$.

The dual $\mathcal{O}_K^\vee$ of $\mathcal{O}_K$ is a fractional ideal, so it is in particular stable by multiplication by elements of $\mathcal{O}_K$. This ideal contains $\mathcal{O}_K$, i.e., $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$, and satisfies $\mathcal{N}(\mathcal{O}_K^\vee) = \Delta_K^{-1}$ (see, e.g., [Con09b, Theorem 4.8]).

Let $\mathcal{O}$ be any order of K. The conductor ideal of $\mathcal{O}$ is the set $\mathcal{C}_\mathcal{O} = \{x \in K \,|\, x\mathcal{O}_K \subseteq \mathcal{O}\}$. This is a fractional $\mathcal{O}_K$-ideal and we have the inclusion $\mathcal{C}_\mathcal{O} \subseteq \mathcal{O}$ (since $1 \in \mathcal{O}_K$). For more results about the conductor ideal of an order, we refer the reader to Conrad's lecture notes [Con09a]. By definition of the conductor ideal, it holds that for any $x \in \mathcal{O}_K$ and any $y \in \mathcal{C}_\mathcal{O}$, the product $x \cdot y$ lies in $\mathcal{O}$. We will use this property in our reduction in order to map elements of $\mathcal{O}_K$ to the (possibly sparser) order $\mathcal{O} = \mathbb{Z}[X]/f(X)$.

Denote Δ_f the absolute value of the discriminant of f, i.e., the absolute value of the resultant of f with its derivative f'. For $\mathcal{O} = \mathbb{Z}[X]/f(X)$, we know that $\Delta_f = \mathcal{N}(\mathcal{C}_\mathcal{O}) \cdot \Delta_K$ (see, e.g., [Sut16, Th. 12.22]). Finally, let us observe that if the coefficients of f are bounded in absolute value by some bound $B > 0$, then, for $\mathcal{O} = \mathbb{Z}[X]/f(X)$, it holds that

$$\Delta_K \leq \Delta_K \cdot \mathcal{N}(\mathcal{C}_\mathcal{O}) \leq (mB)^{2m}, \tag{5}$$

where the second inequality is obtained thanks to the inequality $|\mathrm{Res}(f, f')| \leq (\|f\| \cdot \|f'\|)^m$, with $\|f\|$ denoting the euclidean norm of f when seen as a vector.

The following observation will be useful for our reduction.

Lemma 2.4. *Let $K = \mathbb{Q}[X]/f(X)$ and $\mathcal{O} = \mathbb{Z}[X]/f(X)$, and let I be either $\mathcal{O}_K$ or $\mathcal{O}_K^\vee$. For $a \in \mathcal{C}_\mathcal{O}$ and $b \in I^\vee$, then $a \cdot b \in I^\vee$.*

Proof. Note that I is either $\mathcal{O}_K$ or $\mathcal{O}_K^\vee$. In both cases, this is a (fractional) ideal, so it is stable by multiplication by an element of $\mathcal{O}_K$. Using the fact that $\mathcal{C}_\mathcal{O} \subseteq \mathcal{O}_K$ concludes the proof. □

Finally, we recall a lemma that will allow us to prove the existence of small elements in an ideal, subject to some coprimality condition. This lemma was

originally proven in [BBPS19, Lemma 2.36]. The version we recall below is a slight adaptation (with explicit constant) that was proven in [NP26].

Lemma 2.5 (Lemma 2.9 in [NP26]). *Let K be a number field of degree m, $\mathcal{O}_K$ denote its ring of integers, $q \geq 8m$ be a prime integer, and let J be any fractional ideal of K. Then there exists a non-zero element $t \in J$ such that the ideal tJ^{-1} is coprime to $q\mathcal{O}_K$, satisfying the bound:*

$$\|\tau(t)\| \leq 8m^2 \cdot \Delta_K^{2/m} \cdot \mathcal{N}(J)^{1/m}.$$

2.3 Polynomials and structured matrices

Polynomials. For a ring R and an integer $k > 0$, we denote by $R^{<k}[x]$ the set of polynomials of degree $< k$ with coefficients in R. In this article, we will often need to switch between vectors in $\mathbb{R}^k$ and polynomials of degree $k-1$. We will do so by using the following function φ (note that we abuse notation and use the same φ for all values of k):

$$\begin{aligned} \varphi : \mathbb{R}^k &\to \mathbb{R}^{<k}[x] \\ (a_0, \ldots, a_{k-1})^\top &\mapsto \sum_{i=0}^{k-1} a_i \cdot x^i. \end{aligned} \tag{6}$$

In our reduction, similarly to what is done in [RSSS17], we will extend some uniform polynomial into another uniform polynomial of larger degree. We will do so using the following lemma, which follows almost immediately from [Lyu16, Lem. 2.10].

Lemma 2.6. *Let $q \geq 2$, $m \geq 1$, and $k \geq 0$ be integers. Let $f \in \mathbb{Z}[x]$ be some (fixed) monic polynomial of degree m. Let $a \leftarrow \mathcal{U}(\mathbb{Z}_q^{<m}[x])$ and $r \leftarrow \mathcal{U}(\mathbb{Z}_q^{<k}[x])$. Then $a + f \cdot r$ is uniformly distributed in $\mathbb{Z}_q^{<m+k}[x]$.*

Proof. Applying [Lyu16, Lem. 2.10] to the product $f \cdot r$ (and using the fact that f is monic) tells us that the coefficients of $f \cdot r$ corresponding to the terms $x^m, x^{m+1}, \ldots, x^{m+k-1}$ are jointly uniformly distributed modulo q. For the coefficients corresponding to the terms 1, x, …, x^{m-1}, they are of the form $a_i + (f \cdot r)_i$ with a_i uniformly distributed in $\mathbb{Z}_q$ (and independent of all other random variables). So these coefficients are uniform and jointly independent too. □

To carefully control the error expansion of our reduction, we will restrict our attention to a specific family of defining polynomials with bounded coefficients, as defined below.

Definition 2.7 (Polynomials with bounded coefficients). *Let $m \in \mathbb{Z}_{>0}$ be an integer and $B > 0$ be a real number. We denote by $\mathrm{Pol}_{m,B}$ the set of all*

monic irreducible polynomials of degree m whose coefficients are in $[-B, B]$. In other words,

$$\mathrm{Pol}_{m,B} := \left\{ f = x^m + \sum_{i=0}^{m-1} f_i x^i \,\middle|\, f \text{ irreducible}, f_i \in \mathbb{Z}, |f_i| \leq B \right\}.$$

For some results, we will additionally require some coprimality condition for the polynomials, as defined below.

Definition 2.8 (Polynomials with bounded coefficients and coprimality condition). *Let $m \in \mathbb{Z}_{>0}$ be an integer and $B > 0$ be a real number. Let $q \geq 2$ be an integer. We denote by $\mathrm{Pol}_{m,B,q}$ the set of all polynomials $f \in \mathrm{Pol}_{m,B}$ such that for $K = \mathbb{Q}[X]/f(X)$ and $\mathcal{O} = \mathbb{Z}[X]/f(X)$, it holds that $\mathcal{C}_\mathcal{O}$ is coprime to the ideal $q\mathcal{O}_K$.*

Definition 2.8 above may seem a bit obscure. The lemma below provides a simpler set that is included in $\mathrm{Pol}_{m,B,q}$. Our reduction will hold for any polynomial $f \in \mathrm{Pol}_{m,B,q}$, so in particular for any polynomial f from this simpler set.

Lemma 2.9. *For any $m > 0$ integer, $B > 0$ real number and $q \geq 2$ a prime integer, it holds that*

$$\{f \in \mathrm{Pol}_{m,B} \,|\, q \text{ does not divide } \Delta_f\} \subseteq \mathrm{Pol}_{m,B,q}.$$

Proof. This follows from the equation $\Delta_f = \mathcal{N}(\mathcal{C}_\mathcal{O}) \cdot \Delta_K$ (see above). Since q is prime and does not divide Δ_f, then in particular q is coprime to $\mathcal{N}(\mathcal{C}_\mathcal{O})$. This implies that $q\mathcal{O}_K$ is coprime to $\mathcal{C}_\mathcal{O}$ as needed. □

To assess the expansion of errors and the geometric properties of polynomials, we utilize the Mahler measure.

Definition 2.10 (Mahler measure). *Let $f \in \mathbb{C}[X]$ be a polynomial of degree m, let $a \in \mathbb{C}$ be its leading coefficient, and let $\alpha_1, \cdots, \alpha_m$ be its complex roots. In other words, f factorizes over $\mathbb{C}$ as $f(x) = a\prod_{i=1}^{m}(x - \alpha_i)$. The Malher measure of f is defined as*

$$\mathcal{M}(f) = |a| \cdot \prod_{i=1}^{m} \max(1, |\alpha_i|).$$

Lemma 2.11 (See, e.g., [Mah64, Equation (1)]). *For any polynomial $f = \sum_i f_i x^i \in \mathbb{C}[X]$, it holds that*

$$\mathcal{M}(f) \leq \sum_i |f_i|.$$

In particular, for $f \in \mathrm{Pol}_{m,B}$, we have $\mathcal{M}(f) \leq 1 + mB$.

The middle product of two polynomials is the operation that extracts a central segment of coefficients from a standard polynomial product.

Definition 2.12 (Middle Product). *Let d_a, d_b, d, k be integers such that $d_a + d_b - 1 = d + 2k$. The middle-product $\odot_d : R^{<d_a}[x] \times R^{<d_b}[x] \to R^{<d}[x]$ is the map:*

$$(a, b) \mapsto a \odot_d b = \left\lfloor \frac{(a \cdot b) \bmod x^{k+d}}{x^k} \right\rfloor .$$

We use the same notation $\odot_d$ for every d_a, d_b, k that satisfy the equation $d_a + d_b - 1 = d + 2k$.

Special matrices. In the following, we introduce several special matrices that will be essential for the definitions and proofs presented throughout this paper.

Definition 2.13 ($\mathsf{Toep}^{k,n}(a)$). *For any $k, n > 0$ and $a \in \mathbb{R}^{<n}[x]$. We let $\mathsf{Toep}^{k,n}(a)$ denote the matrix in $\mathbb{R}^{k \times (n+k-1)}$ whose i-th row is given by the coefficients of $x^{i-1} \cdot a$.*

Definition 2.14 ($\mathsf{Rot}^k_f(a)$). *Let $f \in \mathbb{R}[x]$ be a polynomial of degree m. For any $k > 0$ and any $a \in \mathbb{R}[x]$, we let $\mathsf{Rot}^k_f(a)$ denote the matrix in $\mathbb{R}^{k \times m}$ whose i-th row is given by the coefficients of the polynomial $(x^{i-1} \cdot a) \bmod f$. When $k = m$, we simply write $\mathsf{Rot}_f(a)$.*

We extend the notation to any $a \in K = \mathbb{Q}[X]/f(X)$, by taking the unique representative of a in $\mathbb{Q}[x]$ of degree $< m$, that is $\varphi(\pi(a))$.

Remark 2.15. We copied this definition of $\mathsf{Rot}^k_f(a)$ from [RSSS17, Definition 2.2], in order to make it easier to reuse some lemmas from [RSSS17]. Note that this definition uses row convention, which is slightly unconventional. In particular $\mathsf{Rot}_f(a)$ does not correspond to the multiplication by a in coefficient embedding, i.e., it does not hold that $\mathsf{Rot}_f(a) \cdot \pi(x) = \pi(a \cdot x)$ for all $x \in K$.

We state below two useful lemmas from [RSSS17]. Recall that for a vector $\mathbf{v} = (v_1, \ldots, v_n)$, we use the notation $\overleftarrow{\mathbf{v}} = (v_n, \ldots, v_1)$ for the reverse vector.

Lemma 2.16 (Lemma 2.6. in [RSSS17]). *For any $k, n > 0$ and any $a \in \mathbb{R}^{<n}[x]$, we have $\mathsf{Rot}^k_f(a) = \mathsf{Toep}^{k,n}(a) \cdot \mathsf{Rot}^{n+k-1}_f(1)$.*

Lemma 2.17 (Lemma 3.2 in [RSSS17]). *Let $k, n > 0$ be integers. Let $a \in \mathbb{R}^{<n}[x]$, $s \in \mathbb{R}^{<n+k-1}[x]$, then:*

$$a \odot_k s = \varphi\left(\overleftarrow{\mathsf{Toep}^{k,n}(a) \cdot \overleftarrow{\varphi^{-1}(s)}}\right).$$

Matrix norms. For $\mathbf{M} \in \mathbb{R}^{n \times m}$ a matrix, we denote by $|||\mathbf{M}|||$ the matrix norm induced by the euclidean norm (also known as the spectral norm of M), and by $\|\mathbf{M}\|_{\max} = \max_{i,j} |\mathbf{M}_{i,j}|$ the maximum of the coefficients of $\mathbf{M}$. It holds that

$$\|\mathbf{M}\|_{\max} \leq |||\mathbf{M}||| \leq \sqrt{nm} \cdot \|\mathbf{M}\|_{\max}. \tag{7}$$

2.4 Probabilities.

Transferring the uniform distribution. In our reduction, we will use transformation maps, that send some (compact) sets to some other (compact) sets, and we will use the fact that these transformations preserve the uniform distribution. Below are some lemmas that will be used for this.

Lemma 2.18. *Let $K = \mathbb{Q}[X]/f(X)$ and $\mathcal{O} = \mathbb{Z}[X]/f(X)$. Let I be either $\mathcal{O}_K$ or $\mathcal{O}_K^\vee$, let $q > 0$ be an integer, and let $y \in I^\vee \setminus \{0\}$. Then the map*

$$\begin{aligned} \theta_y : K_\mathbb{R}/qI &\to K_\mathbb{R}/q\mathcal{O}^\vee \\ z &\mapsto z \cdot y \end{aligned}$$

is well defined, and it sends the uniform distribution over $K_\mathbb{R}/qI$ to the uniform distribution over $K_\mathbb{R}/q\mathcal{O}^\vee$.

Proof. Let us prove first that the map is well defined. The map θ_y is well defined from $K_\mathbb{R}$ to $K_\mathbb{R}$, where it is even an isomorphism (of $\mathbb{R}$-vector spaces) since $y \in I^\vee \setminus \{0\} \subset K \setminus \{0\}$ is invertible. In order to prove that the map is well defined when we quotient by qI on the left and $q\mathcal{O}^\vee$ on the right, it suffices to prove that the image of qI by θ_y is contained in $q\mathcal{O}^\vee$. This holds because for any $z \in I$, we have $\theta_y(qz) = q \cdot (y \cdot z)$ and $y \cdot z \in I \cdot I^\vee = \mathcal{O}_K \cdot \mathcal{O}_K^\vee = \mathcal{O}_K^\vee$ (recall that $\mathcal{O}_K^\vee$ is an ideal). To conclude, note that $\mathcal{O} \subseteq \mathcal{O}_K$, and so $\mathcal{O}_K^\vee \subseteq \mathcal{O}^\vee$ since duality reverse inclusions. From this we conclude that $\theta_y(qz) \in q\mathcal{O}^\vee$ as desired.

Let us now consider the image of the uniform distribution via θ_y. Since θ_y is an isomorphism of $\mathbb{R}$-vector space, it sends in particular the distribution $\mathcal{U}(K_\mathbb{R}/qI)$ to the distribution $\mathcal{U}(K_\mathbb{R}/\theta_y(qI))$. We have seen just above that $\theta_y(qI) \subseteq q\mathcal{O}^\vee$. Moreover, both $\theta_y(qI)$ and $q\mathcal{O}^\vee$ are full rank lattices in the $\mathbb{R}$-vector space $K_\mathbb{R}$. So reducing modulo $q\mathcal{O}^\vee$ sends $\mathcal{U}(K_\mathbb{R}/\theta_y(qI))$ to $\mathcal{U}(K_\mathbb{R}/q\mathcal{O}^\vee)$. Combining both steps, we conclude that θ_y sends $\mathcal{U}(K_\mathbb{R}/qI)$ to $\mathcal{U}(K_\mathbb{R}/q\mathcal{O}^\vee)$ as desired. □

The following lemma, which was already used in [RSW18], states that the uniform distribution over $\mathcal{O}_K/q\mathcal{O}_K$ can be sent to the uniform distribution over $\mathcal{O}/q\mathcal{O}$.

Lemma 2.19 (Consequence of [RSW18, Th. 4.2]). *Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order, $q \geq 2$ be an integer and assume that $\mathcal{C}_\mathcal{O} + q\mathcal{O}_K = \mathcal{O}_K$. 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 $a \mapsto t \cdot a$ transforms $\mathcal{U}(\mathcal{O}_K/q\mathcal{O}_K)$ into $\mathcal{U}(\mathcal{O}/q\mathcal{O})$.*

Finally, we conclude with two lemmas that will allow us to transform elements of $K_\mathbb{R}$ into polynomials with real coefficients (and preserve uniformity over the desired sets).

Lemma 2.20. *For any integer $q \geq 2$, the function $\varphi \circ \pi^\vee$ sends the uniform distribution over $K_\mathbb{R}/q\mathcal{O}^\vee$ to the uniform distribution over $\mathbb{R}_q^{<m}[x]$.*

Proof. The map $\varphi \circ \pi^\vee$ induces an $\mathbb{R}$-linear bijection from $K_\mathbb{R}$ to $\mathbb{R}^{<m}[x]$. Moreover, we have seen that for any $a \in K_\mathbb{R}$, the vector $\pi^\vee(a)$ is in $\mathbb{Z}^m$ iff $a \in \mathcal{O}^\vee$. So we conclude that $\varphi \circ \pi^\vee(q\mathcal{O}^\vee) = q\mathbb{Z}^{<m}[x]$. This implies that $\varphi \circ \pi^\vee$ induces an $\mathbb{R}$-linear bijection from $K_\mathbb{R}/(q\mathcal{O}^\vee)$ to $(\mathbb{R}/q\mathbb{Z})^{<m}[x]$, and this preserves the uniform distribution. □

Lemma 2.21. *For any integer $q \geq 2$, the function $\varphi \circ \pi$ sends the uniform distribution over $\mathcal{O}/q\mathcal{O}$ to the uniform distribution over $\mathbb{Z}_q^{<m}[x]$.*

Proof. Since $(p_i)_i$ is a $\mathbb{Z}$-basis of $\mathcal{O}$, then the map $\varphi \circ \pi$ induces a bijection from $\mathcal{O}$ to $\mathbb{Z}^{<m}[x]$. Moreover, it holds that $\varphi \circ \pi(q\mathcal{O}) = q\mathbb{Z}^{<m}[x]$, so the map $\varphi \circ \pi$ is a bijection from $\mathcal{O}/q\mathcal{O}$ to $\mathbb{Z}_q^{<m}[x]$. Since these sets are finite, this bijection preserves the uniform distribution as desired. □

Gaussian distribution. We give the definition of the continuous Gaussian distribution, which will be the main distribution used thorough the article.

Definition 2.22. *Let $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ be a positive definite matrix. Define the* Gaussian function *$\rho_{\mathbf{\Sigma}} : \mathbb{R}^n \to \mathbb{R}$ by $\rho_{\mathbf{\Sigma}}(x) := e^{-\pi \cdot \mathbf{x}\mathbf{\Sigma}^{-1}\mathbf{x}^\top}$, for any $\mathbf{x} \in \mathbb{R}^n$. The probability distribution on $\mathbb{R}^n$ whose density is proportional to $\rho_{\mathbf{\Sigma}}$ is called the* Gaussian distribution *and is denoted by $D_{\mathbf{\Sigma}}$. In the special case $\mathbf{\Sigma} = \sigma_0^2\mathbf{I}_n$ (with $\sigma_0 > 0$ and $\mathbf{I}_n$ the identity matrix), we simplify the notation and write ρ_{σ_0} and D_{σ_0} in place of $\rho_{\mathbf{\Sigma}}$ and $D_{\mathbf{\Sigma}}$, respectively.*

2.5 Variants of LWE

We now define the primal/dual RLWE problems, as well as the MP-LWE problem. In this article, we will only consider the decision version of these problems.

The Ring Learning with Errors Problem. We give a single definition, encompassing both primal and dual RLWE.

Definition 2.23 (primal-RLWE/dual-RLWE). *Let K be a number field of degree m, let $q \geq 2$ be an integer, and let χ be a probability distribution on $\tau(K_\mathbb{R}) \subset \mathbb{C}^m$. Let I be either $\mathcal{O}_K$ or $\mathcal{O}_K^\vee$ (in both cases, I is a fractional ideal).*

Let $s \in I/qI$. The RLWE *distribution $\mathcal{D}^{\mathsf{RLWE}}_{K,q,\chi}(s)$ with parameters K, q, χ and s is the distribution obtained by sampling $a \leftarrow \mathcal{U}(\mathcal{O}_K/q\mathcal{O}_K)$ and $e \in K_\mathbb{R}$ such that $\tau(e) \sim \chi$ and outputting $(a, b) \in \mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/qI$ where $b = as+e \mod q$.*

The decision primal-$\mathsf{RLWE}_{K,q,\chi}$ (resp. decision dual-$\mathsf{RLWE}_{K,q,\chi}$) problem with parameters K, q and χ takes $I = \mathcal{O}_K$ (resp. $I = \mathcal{O}_K^\vee$) and consists in distinguishing between a sampler from $\mathcal{D}^{\mathsf{RLWE}}_{K,q,\chi,s}$ and a uniform sampler over $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K$ (resp. $\mathcal{O}_K/q\mathcal{O}_K \times K_\mathbb{R}/q\mathcal{O}_K^\vee$), with non-negligible probability over the random choice of $s \leftarrow \mathcal{U}(\mathcal{O}_K/q\mathcal{O}_K)$ (resp. $s \leftarrow \mathcal{U}(\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee)$).

When $\chi = D_{\alpha q}$ is a continuous gaussian distribution with standard deviation αq for some $\alpha \in (0, 1)$, we write $\mathsf{RLWE}_{K,q,\alpha}$ instead of $\mathsf{RLWE}_{K,q,\chi}$.

Middle-Product Learning with Errors Problem. We first describe the distribution that underpins the MP-LWE problem, and then formally define the problem.

Definition 2.24 (MP distribution). *Let $n, d > 0$, $q \geq 2$, and χ be a distribution over $\mathbb{R}^d$. For $s \in \mathbb{Z}_q^{<n+d-1}[x]$, we define the distribution $\mathcal{D}^{\mathsf{MPLWE}}_{q,n,d,\chi}(s)$ over $\mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<d}[x]$ as the one obtained by sampling $a \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n}[x])$, $e \leftarrow \varphi(\chi)$ and returning $(a, b = a \odot_d s + e)$.*

Definition 2.25 (MP-LWE). *Let $n, d > 0$, $q \geq 2$, and a distribution χ over $\mathbb{R}^d$. The (decision) $\mathsf{MP\text{-}LWE}_{q,n,d,\chi}$ problem consists in distinguishing between arbitrarily many samples from $\mathcal{D}^{\mathsf{MPLWE}}_{q,n,d,\chi}(s)$ and the same number of samples from $\mathcal{U}(\mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<d}[x])$, with non-negligible probability over the choices of $s \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n+d-1}[x])$.*

When $\chi = D_{\alpha q}$ is a continuous gaussian distribution with standard deviation αq for some $\alpha \in (0, 1)$, we write $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha}$ instead of $\mathsf{MP\text{-}LWE}_{q,n,d,\chi}$.

Known reductions for MP-LWE. We now state two known reductions, that we will use to relate different versions of the MP-LWE problem with different parameters. The first reduction was explicitly stated in [RSSS17], and the second one was implicitly used in the same article.

Lemma 2.26 (Lemma 3.8 in [RSSS17]). *Let $n, d > 0$, $q \geq 2$, $\sigma > 0$ and $\|\|\mathbf{\Sigma}_0\|\| < (\sigma)^2$. Then, there exists a* ppt *reduction from decision $\mathsf{MP\text{-}LWE}_{q,n,d,D_{\mathbf{\Sigma}_0}}$ to decision $\mathsf{MP\text{-}LWE}_{q,n,d,D_\sigma}$.*

The second reduction will be used to decrease the parameter d of the MP-LWE problem.

Lemma 2.27 (Implicit in [RSSS17]). *Let $n > 0$, $d_1 \geq d_2 > 0$, $q \geq 2$, and $\alpha \in (0, 1)$. Then, there exists a* ppt *reduction from decision $\mathsf{MP\text{-}LWE}_{q,n,d_1,\alpha}$ to decision $\mathsf{MP\text{-}LWE}_{q,n,d_2,\alpha}$.*

We provide a proof of this lemma for completeness. The key ingredient is the observation that truncating the middle product $a \odot_{d_1} s$ (i.e., keeping only the first coefficients of the polynomial) is equal to the middle product $a \odot_{d_2} s'$, for s' obtained by truncating s. This is stated formally in the lemma below.

Lemma 2.28. *Let $a \in \mathbb{R}^{<n}[x]$ and $s \in \mathbb{R}^{<n+d_1-1}[x]$. For any d_2 such that $0 < d_2 \leq d_1$, the following identity holds:*

$$(a \odot_{d_1} s) \bmod x^{d_2} = a \odot_{d_2} (s \bmod x^{n+d_2-1}).$$

Proof. Let $c = a \cdot s = \sum c_k x^k$. By Definition 2.12, the middle product $a \odot_{d_1} s$ extracts a sequence of d_1 coefficients starting from index $n-1$, given by $\sum_{i=0}^{d_1-1} c_{i+n-1} x^i$. Applying the truncation $(\bmod\ x^{d_2})$ to this sum preserves only

the terms where $i < d_2$, resulting in $(a \odot_{d_1} s) \bmod x^{d_2} = \sum_{i=0}^{d_2-1} c_{i+n-1} x^i$. For the right-hand side, let $s' = s \bmod x^{n+d_2-1}$. The middle product $a \odot_{d_2} s'$ extracts d_2 coefficients of the product $a \cdot s'$, specifically $a \odot_{d_2} (s \bmod x^{n+d_2-1}) = \sum_{i=0}^{d_2-1} (a \cdot s')_{i+n-1} x^i$.

Each coefficient $(a \cdot s)_k$ is defined by the sum $\sum_{j=0}^{n-1} a_j s_{k-j}$. For the indices of interest where $k = i + n - 1$ and $i < d_2$, the maximum index of s required is $(d_2 - 1) + n - 1 = n + d_2 - 2$. Since s' is identical to s for all terms up to degree $n + d_2 - 2$, it follows that $(a \cdot s)_{i+n-1} = (a \cdot s')_{i+n-1}$ for all $0 \leq i < d_2$. Thus, the two expressions are identical. □

Proof (of Lemma 2.27). Given an $\mathsf{MP\text{-}LWE}_{q,n,d_1,\alpha}$ or uniform sample (a, b), the reduction algorithm simply truncates b into $b' = b \bmod x^{d_2}$, and sends (a, b') to the $\mathsf{MP\text{-}LWE}_{q,n,d_2,\alpha}$ oracle. This is a polynomial time algorithm as desired. Observe that the truncation preserves the uniform distribution, so if (a, b) was uniform, then (a, b') is still uniform.

Let us now consider the case where (a, b) is sampled from $\mathsf{MP\text{-}LWE}_{q,n,d_1,\alpha}$. Let $s \in \mathbb{Z}_q^{n+d_1-1}[x]$ be the secret associated to (a, b), i.e., $b = a \odot_{d_1} s + e$. Define $s' = s \bmod x^{n+d_2-1}$ the truncation of s. By Lemma 2.28, it holds that $b' = a \odot_{d_2} s' + e'$ with $e' = e \bmod x^{d_2}$. Since a truncated gaussian distribution remains a gaussian distribution of smaller dimension with the same standard deviation σ, we conclude that (a, b') is distributed as an $\mathsf{MP\text{-}LWE}_{q,n,d_2,\alpha}$ sample with secret s'. This concludes the proof. □

3 General framework

In this section, we describe our general framework that reduces RLWE to MP-LWE. This framework depends on the choice of two element $y_a, y_s \in K$. We will see in the next section that by choosing a specific values of y_a and y_s, we recover the reductions from Peikert-Pepin [PP24] and from Rosca et al. [RSSS17, RSW18, NP26] as special cases of our framework.

Our reduction framework is actually obtained via a simple algorithm: given as input a RLWE pair (a, b), multiply a by some y_a and multiply b by the product $y_a \cdot y_s$ (for some $y_a, y_s \in K$ to be chosen later) to obtain $(a', b') = (a \cdot y_a, b \cdot y_a \cdot y_s) \in K^2$. Then map these two field elements to $(a'', b'') \in \mathbb{R}[x]^2$, with a'' (resp. b'') being the polynomial obtained by taking as coefficients the coordinates of a' (resp. b') in the power basis (resp. dual basis). Said differently, $a'' = \varphi(\pi(a'))$ and $b'' = \varphi(\pi^\vee(b'))$. In order to prove that the pair (a'', b'') obtained is indeed an MP-LWE sample, we will need a few auxiliary lemmas, which we prove in Section 3.1 below.

3.1 Generalized M_f matrix and properties

We first introduce a generalization of the matrix $\mathbf{M}_f$ used in [RSSS17]. Our generalized matrix depends on the choice of some $y \in K$, and one recovers the matrix $\mathbf{M}_f$ of [RSSS17] by choosing $y = p_1^\vee$ (the first vector of the dual basis, see

Lemma 4.3 below). Looking forward, this element y will be equal to the product $y_a \cdot y_s$ mentioned above. The generalized matrix $\mathbf{M}_f$ will be useful to help us write the coordinates of $b'' = \varphi(\pi^\vee(b \cdot y))$ as a matrix-vector product.

Definition 3.1 ($\mathbf{M}_f(y)$). *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree m, and $K = \mathbb{Q}[X]/f(X)$ the associated number field. For any $y \in K$, we define the m-dimensional square matrix $\mathbf{M}_f(y) := \mathbf{V}_f^\top \cdot \mathbf{T}(y) \cdot \mathbf{V}_f$.*

As suggested by its construction, the entries of $\mathbf{M}_f(y)$ have a natural algebraic interpretation using the trace form, which we state in the following lemma.

Lemma 3.2. *Let $y \in K_\mathbb{R}$, then we have $(\mathbf{M}_f(y))_{i,j} = \mathrm{Tr}(p_i p_j y)$.*

Proof. By the definitions of $\mathbf{V}_f$ and $\mathbf{T}(y)$, their entries are given by $(\mathbf{V}_f)_{k,j} = \alpha_k^{j-1} = \sigma_k(p_j)$ and $\mathbf{T}(y)_{k,k} = \sigma_k(y)$. Thus, direct matrix multiplication yields:

$$\begin{aligned}(\mathbf{M}_f(y))_{i,j} &= [\mathbf{V}_f^\top \cdot \mathbf{T}(y) \cdot \mathbf{V}_f]_{i,j} \\ &= \sum_{k=1}^{m} \alpha_k^{i+j-2} \sigma_k(y) \\ &= \sum_{k=1}^{m} \sigma_k(p_i p_j y) \\ &= \mathrm{Tr}(p_i p_j y).\end{aligned}$$

□

As said above, one of the useful properties of the matrix $\mathbf{M}_f(y)$ is that is allows to express the quantity $\pi^\vee(c \cdot y)$ as a matrix-vector product, where the matrix depends only on y and the vector depends only on c.

Lemma 3.3. *For any $c, y \in K = \mathbb{Q}[X]/f(X)$, we have $\pi^\vee(c \cdot y) = \mathbf{M}_f(y) \cdot \pi(c)$.*

Proof. By applying Lemma 2.3 twice (which yields $\pi^\vee(a) = \mathbf{V}_f^\top \cdot \tau(a)$ and $\tau(c) = \mathbf{V}_f \cdot \pi(c)$), we directly obtain:

$$\pi^\vee(c \cdot y) = \mathbf{V}_f^\top \cdot \tau(c \cdot y) = \mathbf{V}_f^\top \cdot \mathbf{T}(y) \cdot \tau(c) = \left(\mathbf{V}_f^\top \cdot \mathbf{T}(y) \cdot \mathbf{V}_f\right) \cdot \pi(c) = \mathbf{M}_f(y) \cdot \pi(c).$$

□

The next lemma provides another interesting property of the matrix $\mathbf{M}_f(y)$. It will be used only as an intermediate result for the proof of Lemma 3.5 below.

Lemma 3.4. *For any $c, y \in K = \mathbb{Q}[X]/f(X)$, we have*

$$\mathbf{M}_f(y) \cdot \pi(c) = \mathsf{Rot}_f(c) \cdot \pi^\vee(y).$$

Proof. From Lemma 3.3, we have $(\mathbf{M}_f(y) \cdot \pi(c))_i = (\pi^\vee(c \cdot y))_i = \mathrm{Tr}(cyp_i)$, where the last equality comes from Lemma 2.1. Recall that $\mathsf{Rot}_f(c) \in \mathbb{Q}^{m \times m}$ is the matrix whose i-th row corresponds to the coefficients of the polynomial $c \cdot x^{i-1} \bmod f$. By definition of the p_i, the coefficients of $c \cdot x^{i-1} \bmod f$ are precisely $\pi(c \cdot p_i)$, so we obtain $c \cdot p_i = \sum_{k=1}^m (\pi(c \cdot p_i))_k \cdot p_k = \sum_{k=1}^m \mathsf{Rot}_f(c)_{i,k} \cdot p_k$. Overall, we obtain

$$\begin{aligned}(\mathbf{M}_f(y) \cdot \pi(c))_i = \mathrm{Tr}(y \cdot c \cdot p_i) &= \mathrm{Tr}(y \cdot \sum_{k=1}^m \mathsf{Rot}_f(c)_{i,k} p_k) \\ &= \sum_{k=1}^m \mathsf{Rot}_f(c)_{i,k} \cdot \mathrm{Tr}(y \cdot p_k) \\ &= \sum_{k=1}^m \mathsf{Rot}_f(c)_{i,k} \cdot (\pi^\vee(y))_k \\ &= (\mathsf{Rot}_f(c) \cdot \pi^\vee(y))_i,\end{aligned}$$

where the second equality follows from the $\mathbb{Q}$-linearity of the trace map, and the third one follows from Equation (4). This concludes the proof. □

Lemma 3.4 above is used in the proof of the following lemma, which will be central to the proof of our reduction in the next section.

Lemma 3.5. *Let $n \geq m > 0$, and let $K = \mathbb{Q}[X]/f(X)$ with f monic irreducible of degree m. Let $a, s \in K = \mathbb{Q}[X]/f(X)$, and $r \in \mathbb{Z}^{<n-m}[x]$. Define $a' := \varphi(\pi(a)) + f \cdot r \in \mathbb{Q}^{<n}[x]$ and $s' := \varphi(\overleftarrow{\mathsf{Rot}_f^{n+m-1}(1) \cdot \pi^\vee(s)}) \in \mathbb{Q}^{<n+m-1}[x]$. It holds that*

$$a' \odot_m s' = \varphi(\overleftarrow{\pi^\vee(a \cdot s)}).$$

Proof. From Lemma 3.3 and Lemma 3.4, we have $\pi^\vee(a \cdot s) = \mathbf{M}_f(s) \cdot \pi(a) = \mathsf{Rot}_f(a) \cdot \pi^\vee(s)$. By definition of Rot_f and since $a' = \varphi(\pi(a)) \bmod f$, then $\mathsf{Rot}_f(a) = \mathsf{Rot}_f(a')$, so we get

$$\pi^\vee(a \cdot s) = \mathsf{Rot}_f(a') \cdot \pi^\vee(s).$$

Applying Lemma 2.16 to a' (whose degree is $< n$) and $k = m$, we see that $\mathsf{Rot}_f(a') = \mathsf{Toep}^{m,n}(a') \cdot \mathsf{Rot}_f^{n+m-1}(1)$. We conclude using Lemma 2.17, and the fact that $\overleftarrow{\varphi^{-1}(s')} = \mathsf{Rot}_f^{n+m-1}(1) \cdot \pi^\vee(s)$ by definition of s':

$$\begin{aligned}a' \odot_m s' &= \varphi(\overleftarrow{\mathsf{Toep}^{m,n}(a') \cdot \mathsf{Rot}_f^{n+m-1}(1) \cdot \pi^\vee(s)}) \\ &= \varphi(\overleftarrow{\mathsf{Rot}_f(a') \cdot \pi^\vee(s)}) \\ &= \varphi(\overleftarrow{\pi^\vee(a \cdot s)}),\end{aligned}$$

as desired. □

3.2 General reduction from RLWE to MP-LWE

We are now ready to describe our general reduction framework from RLWE to MP-LWE. The algorithm (named $\texttt{MPLWE-Red}_{y_a,y_s}(a,b)$) is described in Algorithm 1 below. We will prove that this algorithm terminates in polynomial time, that it sends RLWE samples to MP-LWE samples, and that it sends uniform samples to uniform samples. This will give us our desired reduction from RLWE to MP-LWE (we handle both primal-RLWE and dual-RLWE at the same time).

Parameters: $n \geq m$ two integers;
$f \in \mathbb{Z}[X]$ of degree m defining $K = \mathbb{Q}[X]/f(X)$;
$y_a, y_s \in K \setminus \{0\}$;
Input : $(a, b) \in K \times K_{\mathbb{R}}$;
Output : $(a', b') \in \mathbb{Q}^{<n}[x] \times \mathbb{R}^{<m}[x]$;
Function $\texttt{MPLWE-Red}_{y_a,y_s}(a, b)$**:**
  Sample $r \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n-m}[x])$;
  $a' = \varphi(\pi(y_a \cdot a)) + f \cdot r$;
  $b' \leftarrow \varphi(\overleftarrow{\pi^\vee(y_a \cdot y_s \cdot b)})$;
  return (a', b')

Algorithm 1: General reduction framework for MP-LWE.

Lemma 3.6. *Algorithm 1 runs in polynomial time, which is bounded by $\mathcal{O}(n^2)$.*

Proof. To prove that the reduction $\texttt{MPLWE-Red}_{y_a,y_s}$ runs in polynomial time, we bound the complexity of its arithmetic operations. Sampling the polynomial r takes $O((n-m)\log q)$ time. Computing a' involves multiplication in the number field K requiring $O(m^2)$ operations, and standard polynomial multiplication $f \cdot r$ taking $O(m(n-m))$ operations, yielding a total of $O(mn)$ time. Computing b' requires multiplication in K followed by an $m \times m$ matrix multiplication to map to the dual basis via $\pi^\vee$, bounded by $O(m^2)$ operations. As the linear formatting maps π and φ operate in strictly $O(m)$ time, the overall runtime is dominated by $O(n^2)$ polynomial arithmetic operations. Given that the input bit-lengths are polynomially bounded, the algorithm executes in polynomial time. □

Proposition 3.7. *Let $n \geq m > 0$ be integers. Let $K = \mathbb{Q}[X]/f(X)$ be a number field of degree m, and let $\mathcal{O} = \mathbb{Z}[X]/f(X)$. Let $I \subset K$ be either $I = \mathcal{O}_K$ (primal-RLWE case) or $I = \mathcal{O}_K^\vee$ (dual-RLWE case). Let $q \geq 2$ be an integer such that $q\mathcal{O}_K$ is coprime to $\mathcal{C}_\mathcal{O}$. Let $y_s \in I^\vee \setminus \{0\}$ and $y_a \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ such that the quotient ideal $y_a \cdot \mathcal{C}_\mathcal{O}^{-1}$ is coprime to $q\mathcal{O}_K$. Then, the following holds*

1. *[RLWE **case**] Let $s \in I/qI$ and χ be a probability distribution over $\tau(K_{\mathbb{R}})$. If $(a, b) \leftarrow \mathcal{D}^{\mathsf{RLWE}}_{K,q,\chi}(s)$ (the RLWE distribution, see Definition 2.23), then $(a', b') := \texttt{MPLWE-Red}_{y_a,y_s}(a, b)$ is distributed as $\mathcal{D}^{\mathsf{MPLWE}}_{q,n,m,\chi'}(s')$ (the MP-LWE distribution, see Definition 2.24), where*

$$s' = \varphi(\overleftarrow{\mathsf{Rot}_f^{m+n-1}(1) \cdot \pi^\vee(y_s \cdot s)}) \in \mathbb{Z}_q^{<n+m-1}[x]$$

and $\chi' = \mathbf{J} \cdot \mathbf{M}_f(y_a \cdot y_s) \cdot \mathbf{V}_f^{-1} \cdot \chi,$

with $\mathbf{J} \in \mathbb{Z}^{m\times m}$ *the anti-diagonal identity matrix.*

2. ***[Uniform case]*** *If* $(a, b) \leftarrow \mathcal{U}(\mathcal{O}_K/q\mathcal{O}_K \times K_{\mathbb{R}}/qI)$*, then the distribution of* $(a', b') :=$ $\texttt{MPLWE-Red}_{y_a,y_s}(a, b)$ *follows* $\mathcal{U}(\mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<m}[x])$.

Proof. We start by proving that if $a \leftarrow \mathcal{U}(\mathcal{O}_K/q\mathcal{O}_K)$, then $a' := \varphi\circ\pi(y_a\cdot a)+f\cdot r$ (with $r \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n-m}[x])$ as in the algorithm) is distributed uniformly at random in $\mathbb{Z}_q^{<n}[x]$. This will be useful for both cases. By Lemma 2.6, and since f is monic and $r \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n-m}[x])$, it suffices to prove that $\varphi \circ \pi(y_a \cdot a)$ is uniformly distributed in $\mathbb{Z}_q^{<m}[x]$. Recall that both $\mathcal{C}_{\mathcal{O}}$ and $y_a \cdot \mathcal{C}_{\mathcal{O}}^{-1}$ are coprime to the ideal $q\mathcal{O}_K$. So we can apply Lemma 2.19, which tells us that $y_a \cdot a$ is uniformly distributed in $\mathcal{O}/q\mathcal{O}$. Finally, using Lemma 2.21, we see that $\varphi \circ \pi(y_a \cdot a)$ is uniformly distributed in $\mathbb{Z}_q^{<m}[x]$, as desired. Summing up, we have proven that a' is distributed as $\mathcal{U}(\mathbb{Z}_q^{<n}[x])$. It now remains to prove that b' follows the desired distribution. We distinguish the two cases.

1. The RLWE case. In the RLWE case, we know that $b = as+e$, where $e \in K_{\mathbb{R}}$ is such that $\tau(e) \sim \chi$. Let $b' = \varphi(\overleftarrow{\pi^\vee(b \cdot y_a \cdot y_s)})$ as in the algorithm. We want to prove that b' is distributed as in the MP-LWE distribution, i.e., $b' = a' \odot_m s' + e'$, with $e' \sim \chi'$. First, note that $s' = \varphi(\overleftarrow{\mathsf{Rot}_f^{m+n-1}(1) \cdot \pi^\vee(y_s \cdot s)}) \in \mathbb{Z}_q^{<n+m-1}[x]$ as desired. Indeed, $s \cdot y_s \in I \cdot I^\vee = \mathcal{O}_K^\vee \subseteq \mathcal{O}^\vee$, implying that $\pi^\vee(s \cdot y_s) \in \mathbb{Z}^m$. And the matrix $\mathsf{Rot}_f^{n+m-1}(1)$ lives in $\mathbb{Z}^{n+m-1\times m}$ (because f is monic and has integer coefficients), so s' has integer coefficients as wanted.

Applying Lemma 3.5 (with $a = a \cdot y_a \in K$ and $s = s \cdot y_s \in K$), we obtain

$$a' \odot_m s' = \varphi(\overleftarrow{\pi^\vee(ay_a \cdot sy_s)}).$$

Moreover, replacing b by its definition in b', and using the linearity of the maps φ, $\pi^\vee$ and the inversion map $\overleftarrow{\cdot}$, we see that

$$b' = \varphi(\overleftarrow{\pi^\vee(as \cdot y_a y_s)}) + \varphi(\overleftarrow{\pi^\vee(e \cdot y_a y_s)}).$$

Combining both equations, we conclude that $b' = a' \odot_m s' + e'$, where

$$e' = \varphi(\overleftarrow{\pi^\vee(e \cdot y_a y_s)}).$$

To conclude the proof in the RLWE case, it only remains to prove that e' is distributed as $\varphi(\chi') = \varphi\left(\mathbf{J} \cdot \mathbf{M}_f(y_a \cdot y_s) \cdot \mathbf{V}_f^{-1} \cdot \chi\right)$.

Recall that e is such that $\tau(e) \sim \chi$. From Lemma 2.3, we obtain that $\pi(e) = \mathbf{V}_f^{-1} \cdot \tau(e)$ is distributed as $\mathbf{V}_f^{-1} \cdot \chi$. Then, applying Lemma 3.3, we have that

$$\pi^\vee(e \cdot y_a y_s) = \mathbf{M}_f(y_a \cdot y_s) \cdot \pi(e),$$

from which we obtain that $\pi^\vee(e\cdot y_a y_s) \sim \mathbf{M}_f(y_a\cdot y_s)\cdot\mathbf{V}_f^{-1}\cdot\chi$. To conclude, it only remains to observe that multiplying a vector on the left by the matrix $\mathbf{J}$ (the anti-diagonal identity matrix) performs the reverse operation $\overleftarrow{\cdot}$ on the coordinates of the vector. Combining everything, we obtain that $e' = \varphi(\overleftarrow{\pi^\vee(e \cdot y_a y_s)}) \sim \varphi\left(\mathbf{J} \cdot \mathbf{M}_f(y_a \cdot y_s) \cdot \mathbf{V}_f^{-1} \cdot \chi\right) = \chi'$ as desired.

2. The uniform case. In this case, we have $b \leftarrow \mathcal{U}(K_{\mathbb{R}}/qI)$, and we want to prove that $b' = \varphi(\overleftarrow{\pi^\vee}(b \cdot y_a \cdot y_s))$ is uniformly distributed in $\mathbb{R}_q^{<m}[x]$. Note that since the randomness of b' comes from the one in b, and b is independent from a (and a'), then b' will be independent from a', and so we can safely consider the distribution of b' alone (instead of considering the distribution of the pair (a', b')).

Since $y_a \in \mathcal{C}_{\mathcal{O}}$ and $y_s \in I^\vee$, we have $y_a \cdot y_s \in I^\vee$ according to Lemma 2.4. Moreover, $y_a y_s \neq 0$ since both y_a and y_s are in K and are non-zero. From Lemma 2.18, this implies that $b \cdot (y_a y_s)$ is uniform over $K_{\mathbb{R}}/q\mathcal{O}^\vee$ since b is uniform over $K_{\mathbb{R}}/qI$. Finally, using Lemma 2.20, the map $\varphi \circ \pi^\vee$ sends the uniform distribution over $K_{\mathbb{R}}/q\mathcal{O}^\vee$ to the uniform distribution over $\mathbb{R}_q^{<m}[x]$. Note that the reverse operation $\overleftarrow{\cdot}$ preserves the uniform distribution. So we conclude that $b' \sim \mathcal{U}(\mathbb{R}_q^{<m}[x])$ as desired. □

Theorem 3.8. *Let $n \geq m \geq d > 0$ be integers and $\alpha \in (0, 1)$ a real number. Let $K = \mathbb{Q}[X]/f(X)$ be a number field of degree m, and let $\mathcal{O} = \mathbb{Z}[X]/f(X)$. Let $q \geq 2$ be an integer such that $q\mathcal{O}_K$ is coprime to $\mathcal{C}_{\mathcal{O}}$. Let $I = \mathcal{O}_K$ (resp. $I = \mathcal{O}_K^\vee$). Let $y_s \in I^\vee \setminus \{0\}$ and $y_a \in \mathcal{C}_{\mathcal{O}} \setminus \{0\}$ such that the quotient ideal $y_a \cdot \mathcal{C}_{\mathcal{O}}^{-1}$ is coprime to $q\mathcal{O}_K$. Then there exists a* ppt *reduction from decision primal-$\mathsf{RLWE}_{K,q,\alpha}$ (resp. dual-$\mathsf{RLWE}_{K,q,\alpha}$) to $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha'}$, where $\alpha' = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(y_a \cdot y_s) \right|\right|\right|$.*

Proof. From Lemma 2.27, there is a ppt reduction from decision $\mathsf{MP\text{-}LWE}_{q,n,m,\alpha'}$ to decision $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha'}$ (since $d \leq m$). So it suffices to prove that decision (primal/dual) $\mathsf{RLWE}_{K,q,\alpha}$ reduces to decision $\mathsf{MP\text{-}LWE}_{q,n,m,\alpha'}$ (with $d = m$).

Let us first describe a ppt reduction algorithm from decision (primal/dual) $\mathsf{RLWE}_{K,q,\alpha}$ to decision $\mathsf{MP\text{-}LWE}_{q,n,m,\chi'}$, where $\chi' = \mathbf{J} \cdot \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1} \cdot D_{\alpha q}$, for $y := y_a y_s$. The algorithm first samples $t \leftarrow \mathcal{U}(\mathbb{Z}_q^{<n+m-1}[x])$. Then, every time that the algorithm is given as input some RLWE sample (a, b), it runs $(a', b') = \mathtt{MPLWE\text{-}Red}_{y_a, y_s}(a, b)$ and returns $(a'', b'') := (a', b') + (0, a' \odot_d t)$. By Proposition 3.7, we know that when (a, b) is uniform, then the pair (a', b') (and so a fortiori the pair (a'', b'') is also uniform. Moreover, when $(a, b) \leftarrow \mathcal{D}_{K,q,\alpha}^{\mathsf{RLWE}}(s)$, then $(a', b') \sim \mathcal{D}_{q,n,m,\chi'}^{\mathsf{MPLWE}}(s')$ for some $s' \in \mathbb{Z}_q^{<n+m-1}[x]$ (defined in Proposition 3.7, but the definition is not needed here) and χ' as above. Then, the pair (a'', b'') is distributed as $\mathcal{D}_{q,n,m,\chi'}^{\mathsf{MPLWE}}(s' + t)$. Note that since t is uniform in $\mathbb{Z}_q^{<n+m-1}[x]$, so is $s+t$. Hence, we conclude that the algorithm described above provides a reduction from decision (primal/dual) $\mathsf{RLWE}_{K,q,\alpha}$ to decision $\mathsf{MP\text{-}LWE}_{q,n,m,\chi'}$.

In order to conclude, recall that $\chi' = \mathbf{J} \cdot \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1} \cdot D_{\alpha q} = D_{\mathbf{\Sigma}}$, where $\mathbf{\Sigma} = (\alpha q)^2 \cdot (\mathbf{J} \cdot \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1})^\top \cdot (\mathbf{J} \cdot \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1})$. Hence, by Lemma 2.26, there exists a ppt reduction from $\mathsf{MP\text{-}LWE}_{q,n,m,\chi'}$ to $\mathsf{MP\text{-}LWE}_{q,n,m,\alpha'}$ for any $\alpha' > \alpha \cdot \left|\left|\left| \mathbf{J} \cdot \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1} \right|\right|\right|$. Note that multiplication by $\mathbf{J}$ preserves the operator norm, hence we obtain

$$\left|\left|\left| \mathbf{J} \cdot \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1} \right|\right|\right| = \left|\left|\left| \mathbf{M}_f(y) \cdot \mathbf{V}_f^{-1} \right|\right|\right| = \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(y) \right|\right|\right|,$$

where in the last equality we used the definition of $\mathbf{M}_f(y)$ (see Definition 3.1). Combining all the three reductions concludes the proof. □

4 Recovering known reductions as special cases

In this section, we show that by instantiating our reduction framework from the previous section with appropriate choices of (y_a, y_s), we can recover the previous reductions from [PP24] and [RSSS17, RSW18, NP26].

4.1 Reduction from [PP24]

In their article, Peikert and Pepin provide a reduction from order-LWE ($\mathcal{O}$-LWE) to MP-LWE, where the order $\mathcal{O}$ is $\mathbb{Z}[X]/f(X)$. In the monogenic case, when $\mathbb{Z}[X]/f(X) = \mathcal{O}_K$, it turns out that $\mathcal{O}$-LWE is equal to dual RLWE, hence [PP24] gives us a reduction from dual RLWE to MP-LWE in this special monogenic case. We recall below this reduction.

Theorem 4.1 (Adapted from [PP24, Corollary 5.5]). *Let $n \geq d > 0$. Let f be a monic irreducible polynomial of degree $m \in [d, n]$ and define $K = \mathbb{Q}[X]/f(X)$. Assume that $\mathcal{O}_K = \mathbb{Z}[X]/f(x)$. Let $q > 0$ be an integer and $\alpha \in (0, 1)$. There exists a* ppt *reduction from dual-$\mathsf{RLWE}_{K,q,\alpha}$ to $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha'}$, where $\alpha' = \alpha \cdot |||\mathbf{V}_f|||$.*

By unrolling the reduction algorithms of [PP24] in the special case where $\mathcal{O}_K = \mathbb{Z}[X]/f(X)$, one can see that their final reduction algorithm coincide with our Algorithm 1, with $y_a = y_s = 1$. We prove below that by instantiating our framework this way, we indeed recover the same result as in [PP24].

Lemma 4.2. *Theorem 4.1 can be recovered by choosing $y_a = y_s = 1$ in Theorem 3.8.*

Proof. First of all, observe that under our assumption that $\mathcal{O}_K = \mathbb{Z}[X]/f(X) = \mathcal{O}$, we have that $\mathcal{C}_\mathcal{O} = \mathcal{O}_K$. The constraint from Theorem 3.8 that $\mathcal{C}_\mathcal{O}$ should be coprime to $q\mathcal{O}_K$ is then automatically satisfied. Moreover, since we consider the dual RLWE problem, this means that we take $I = \mathcal{O}_K^\vee$. Taking $y_a = y_s = 1$ is then a valid choice of parameters, since $1 \in \mathcal{O}_K = I^\vee$ and $1 \in \mathcal{O}_K = \mathcal{C}_\mathcal{O}$, and $y_a \mathcal{C}_\mathcal{O}^{-1} = \mathcal{O}_K$ is coprime to $q\mathcal{O}_K$. Applying Theorem 3.8, we then obtain a ppt reduction from dual-$\mathsf{RLWE}_{K,q,\alpha}$ to $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha'}$ where

$$\alpha' = \alpha \cdot \left|\left|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(1)\right|\right|\right|.$$

To conclude, it remains to observe that $\mathbf{T}(1)$ is the identity matrix, and so $\left|\left|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(1)\right|\right|\right| = \left|\left|\left|\mathbf{V}_f^\top\right|\right|\right| = |||\mathbf{V}_f|||$. □

4.2 Reduction from [RSSS17, RSW18, NP26]

Before recalling the reduction from [RSSS17, RSW18, NP26], we first observe that this reduction depends on some matrix, which is called $\mathbf{M}_f$ in [RSSS17, NP26], and which coincides with the matrix $\mathbf{M}_f(p_1^\vee)$ with our notations.

Lemma 4.3. *Taking $y = p_1^\vee$ the first vector of the dual basis, then $\mathbf{M}_f(p_1^\vee)$ is the matrix whose (i,j)-th coefficient is the constant coefficient of $x^{i+j-2} \bmod f$ (i.e., this is the matrix $\mathbf{M}_f$ from [RSSS17, Definition 2.3]).*

Proof. From Lemma 3.2, we have proven that the (i,j)-th coefficient of $\mathbf{M}_f(y)$ is $\mathrm{Tr}(p_i p_j y)$. Instantiating with $y = p_1^\vee$ and recalling that $p_i = x^{i-1}$ and $p_j = x^{j-1}$, we obtain $(\mathbf{M}_f(p_1^\vee))_{i,j} = \mathrm{Tr}(x^{i+j-2} \cdot p_1^\vee)$. Using Equation (3) from Lemma 2.1, this is equal to $(\pi(x^{i+j-2}))_1$, which is exactly the constant coefficient of $x^{i+j-2} \bmod f$ by definition of π. □

We now recall the reduction from [RSSS17, RSW18], as analyzed in [NP26]. Our statement differs slightly from [NP26, Th. 5.3], since we keep the quantity $\left|\left|\left|\mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1}\right|\right|\right|$ in the bound, instead of upper bounding it by $\sqrt{md} \cdot D(f)$ as in [NP26, Th. 5.3] (where $D(f)$ is some quantity defined in [NP26, Def. 4.2]). The slightly different statement can be recovered by looking at the proof of [NP26, Th. 5.3].

Theorem 4.4 (Adapted from [NP26, Th. 5.3]). *Let $n \geq d > 0$ be integers. Let $f(x)$ be a monic irreducible polynomial of degree $m \in [d, n]$. Let $K = \mathbb{Q}[X]/f(X)$ and $\mathcal{O} = \mathbb{Z}[X]/f(X)$. Let $q \geq 8m$ be a prime integer not dividing the constant coefficient of f nor $\mathcal{N}(\mathcal{C}_\mathcal{O})$. Let $\alpha \in (0,1)$. There exist a* ppt *reductions from both primal-$\mathsf{RLWE}_{K,q,\alpha}$ and dual-$\mathsf{RLWE}_{K,q,\alpha}$ to $\mathsf{MP\text{-}LWE}_{q,n,m,\alpha'}$, where*

- ***primal*-RLWE *case:*** $\alpha' = \alpha \cdot 64 \cdot m^4 \cdot \Delta_K^{4/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{2/m} \left|\left|\left|\mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1}\right|\right|\right|$;
- ***dual*-RLWE *case:*** $\alpha' = \alpha \cdot 512 \cdot m^6 \cdot \Delta_K^{7/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{2/m} \left|\left|\left|\mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1}\right|\right|\right|$.

In order to obtain this reduction, the authors of [NP26] choose two elements: $t_1 \in (\mathcal{O}_K^\vee)^{-1} \setminus \{0\}$ such that $t_1(\mathcal{O}_K^\vee) + q\mathcal{O}_K = \mathcal{O}_K$, and $t_2 \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ such that $t_2 \mathcal{C}_\mathcal{O}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$. Using Lemma 2.5, they show that there exists such t_1 and t_2 satisfying $\|\tau(t_1)\| \leq 8m^2 \Delta_K^{3/m}$ and $\|\tau(t_2)\| \leq 8m^2 \Delta_K^{2/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m}$. Unrolling the different steps of their reduction, one can see that their final reduction algorithm coincides with our Algorithm 1 instantiated with $y_a = t_2$ and $y_s = p_1^\vee \cdot t_2$ in the primal-RLWE case or $y_s = p_1^\vee \cdot t_2 \cdot t_1$ in the dual-RLWE case. We prove below that if we instantiate our framework this way, we can recover the same result as in [NP26].

Lemma 4.5. *Theorem 4.4 can be recovered by instantiating Theorem 3.8 with*

- $y_a = t_2$ *and* $y_s = p_1^\vee \cdot t_2$ *in the primal-*RLWE *case,*
- $y_a = t_2$ *and* $y_s = p_1^\vee \cdot t_2 \cdot t_1$ *in the dual-*RLWE *case,*

for some well chosen $t_1 \in (\mathcal{O}_K^\vee)^{-1} \setminus \{0\}$ and $t_2 \in \mathcal{C}_\mathcal{O} \setminus \{0\}$.

Proof. Let $t_1 \in (\mathcal{O}_K^\vee)^{-1} \setminus \{0\}$ be such that $t_1(\mathcal{O}_K^\vee) + q\mathcal{O}_K = \mathcal{O}_K$ and $\|\tau(t_1)\| \leq 8m^2\Delta_K^{3/m}$. Let $t_2 \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ be such that $t_2\mathcal{C}_\mathcal{O}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$ and $\|\tau(t_2)\| \leq 8m^2\Delta_K^{2/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m}$. We know that such t_1 and t_2 exists thanks to Lemma 2.5, which we can apply because we assumed that $q \geq 8m$ is prime. Note that $\mathcal{N}((\mathcal{O}_K^\vee)^{-1}) = \Delta_K$, which gives us the bound on $\|\tau(t_1)\|$.

1. Primal-RLWE case. We set $I = \mathcal{O}_K$, so that $I^\vee = \mathcal{O}_K^\vee$. We have $y_a = t_2 \in \mathcal{C}_\mathcal{O}$ and $y_s = p_1^\vee \cdot t_2 \in \mathcal{O}_K^\vee = I^\vee$, because $\mathcal{O}_K^\vee$ is an $\mathcal{O}_K$-ideal and $t_2 \in \mathcal{O}_K$. Applying Theorem 3.8 with these choices yields a ppt reduction from decision primal-$\mathsf{RLWE}_{K,q,\alpha}$ to $\mathsf{MP\text{-}LWE}_{q,n,m,\alpha'}$, where

$$\alpha' = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(p_1^\vee \cdot t_2^2) \right|\right|\right| = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(p_1^\vee) \cdot \mathbf{T}(t_2^2) \right|\right|\right| = \alpha \cdot |||\mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1} \cdot \mathbf{T}(t_2^2)|||.$$

The second equality holds by multiplicativity of $\mathbf{T}$ and the last equality holds because $\mathbf{M}_f(p_1^\vee) = \mathbf{V}_f^\top \cdot \mathbf{T}(p_1^\vee) \cdot \mathbf{V}_f$ by definition (see Definition 3.1). Finally, let us observe that since $\mathbf{T}(t_2^2)$ is a diagonal matrix whose diagonal coefficients are the coefficients of $\tau(t_2^2)$, then $\left|\left|\left|\mathbf{T}(t_2^2)\right|\right|\right| \leq \|\tau(t_2^2)\| \leq \|\tau(t_2)\|^2$. Using the submultiplicativity of the spectral norm and the upper bound on $\|\tau(t_2)\|$, we obtain as desired

$$\alpha' \leq \alpha \cdot \left|\left|\left| \mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1} \right|\right|\right| \cdot (8m^2\Delta_K^{2/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m})^2.$$

2. Dual-RLWE case. We set $I = \mathcal{O}_K^\vee$, so that $I^\vee = \mathcal{O}_K$. We have $y_a = t_2 \in \mathcal{C}_\mathcal{O}$ and $y_s = p_1^\vee \cdot t_2 \cdot t_1 \in \mathcal{O}_K = I^\vee$, because $p_1^\vee \cdot t_1 \in \mathcal{O}_K^\vee \cdot (\mathcal{O}_K^\vee)^{-1} = \mathcal{O}_K$ and $t_2 \in \mathcal{O}_K$. Applying Theorem 3.8 with these choices yields a ppt reduction from decision dual-$\mathsf{RLWE}_{K,q,\alpha}$ to $\mathsf{MP\text{-}LWE}_{q,n,m,\alpha'}$, where

$$\alpha' = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(p_1^\vee \cdot t_1 t_2^2) \right|\right|\right| = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(p_1^\vee) \cdot \mathbf{T}(t_1 t_2^2) \right|\right|\right| = \alpha \cdot |||\mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1} \cdot \mathbf{T}(t_1 t_2^2)|||.$$

Using the same reasoning as before, we know that $\left|\left|\left|\mathbf{T}(t_1 t_2^2)\right|\right|\right| \leq \|\tau(t_1 t_2^2)\| \leq \|\tau(t_1)\| \cdot \|\tau(t_2)\|^2$. Using the submultiplicativity of the spectral norm and the upper bounds on $\|\tau(t_1)\|$ and $\|\tau(t_2)\|$, we obtain as desired

$$\alpha' \leq \alpha \cdot \left|\left|\left| \mathbf{M}_f(p_1^\vee) \cdot \mathbf{V}_f^{-1} \right|\right|\right| \cdot (8m^2\Delta_K^{3/m}) \cdot (8m^2\Delta_K^{2/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m})^2.$$

□

Note that in the proof using our new framework, we do not need to assume that q is coprime with the constant coefficient of f, as was needed in [NP26, Th. 5.3]. We also note that our framework reduction gives a simple way to improve the reduction from [NP26, Th. 5.3]: take $y_s = p_1^\vee$ (primal case) or $y_s = p_1^\vee \cdot t_1$ (dual case), i.e., do not multiply y_s by t_2. The proof would work exactly the same and this would slightly reduce the bounds in Theorem 4.4. In the next section, we give another instantiation of (y_a, y_s) that improves significantly the noise growth of the reduction, and subsumes Theorems 4.1 and 4.4.

5 A new reduction covering all polynomials

In this section, we prove that for all monic irreducible polynomials f (up to a coprimality condition with q), there exists a choice of (y_a, y_s) that makes the noise growth of our reduction polynomial in the degree m of f and in the maximum B of the absolute values of the coefficients of f. We start by proving a lemma giving the existence of a good y making the quantity $\left|\left|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right|\right|\right|$ small.

Proposition 5.1. *Let $K = \mathbb{Q}[X]/f(X)$ be a number field of degree m. Let $q \geq 8m$ be a prime integer and $J \subset K$ be an fractional ideal. Then there exists $y \in J \setminus \{0\}$ such that $yJ^{-1} + q\mathcal{O}_K = \mathcal{O}_K$ and satisfying*

$$\left|\left|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right|\right|\right| \leq 8m^3 \cdot \Delta_K^{2/m} \cdot \mathcal{M}(f) \cdot \mathcal{N}(J)^{1/m}.$$

Proof. Let us consider an arbitrary $y \in K$, and look at the coefficients of the matrix $\mathbf{V}_f^\top \cdot \mathbf{T}(y)$. By definition of $\mathbf{V}_f$ and $\mathbf{T}(y)$, for $1 \leq i, j \leq m$, it holds that

$$(\mathbf{V}_f^\top \cdot \mathbf{T}(y))_{i,j} = \alpha_j^{i-1} \cdot \sigma_j(y).$$

Observe that for each column, the maximum (in absolute value) is reached either by the first coefficient of the column (if $|\alpha_j| \leq 1$) or by the last coefficient of the column (if $|\alpha_j| \geq 1$). In particular, it holds that for any $1 \leq i, j \leq m$, we have

$$\left|(\mathbf{V}_f^\top \cdot \mathbf{T}(y))_{i,j}\right| \leq \max(1, |\alpha_j|^{m-1}) \cdot |\sigma_j(y)|. \tag{8}$$

Our objective is to prove that there exists a $y \in J$, coprime to q, that makes this quantity small for all j's.

To do so, let us consider $\beta \in K_\mathbb{R}$ that satisfies $\sigma_i(\beta) = \max(1, |\alpha_i|^{m-1})$ for $1 \leq i \leq m$ (note that such a β exists because for any pair of complex roots $\alpha_{i_1} = \overline{\alpha_{i_2}}$, we have $\max(1, |\alpha_{i_1}|^{m-1}) = \max(1, |\alpha_{i_2}|^{m-1})$).

Consider the ideal $\widetilde{J} := \beta \cdot J$. We have that $\mathcal{N}(\widetilde{J}) = |\mathcal{N}(\beta)| \cdot \mathcal{N}(J)$. But by definition of the Mahler measure (see Definition 2.10), it holds that $\mathcal{N}(\beta) = \prod_{i=1}^m \max(1, |\alpha_i|^{m-1}) = \left(\prod_{i=1}^m \max(1, |\alpha_i|)\right)^{m-1} = \mathcal{M}(f)^{m-1}$. Hence, we obtain that $\mathcal{N}(\widetilde{J}) = \mathcal{M}(f)^{m-1} \cdot \mathcal{N}(J)$.

We want to apply Lemma 2.5 to the ideal $\widetilde{J}$, but unfortunately this is not a fractional ideal of K (because β may not be in K), so we need to work a little bit more to apply the lemma. We know that K is dense in $K_\mathbb{R}$, so for any $\varepsilon > 0$, there exists some $\beta_0 \in K$ and $e \in K_\mathbb{R}$ such that $\beta = (1 + e) \cdot \beta_0$ and $\|\tau(e)\|_\infty \leq \varepsilon$. The ideal $\beta_0 \cdot J$ is fractional and so we can apply Lemma 2.5 to it, in order to obtain an non-zero element $y_0 \in \beta_0 \cdot J$ such that $\|\tau(y_0)\| \leq 8m^2 \cdot \Delta_K^{2/m} \cdot \mathcal{N}(\beta_0 \cdot J)^{1/m}$ and $y_0 \cdot (\beta_0 \cdot J)^{-1}$ is coprime to $q\mathcal{O}_K$. Define $\widetilde{y} = (1 + e) \cdot y_0$, then $\widetilde{y} \in \widetilde{J}$ and $\widetilde{y} \cdot \widetilde{J}^{-1} = y_0 \cdot (\beta_0 \cdot J)^{-1}$ is also coprime to $q\mathcal{O}_K$. Moreover, $\|\tau(\widetilde{y})\| \leq \|\tau(1 + e)\|_\infty \cdot \|\tau(y_0)\| \leq (1 + \varepsilon) \cdot \|\tau(y_0)\|$. We also have that $\mathcal{N}(\widetilde{J}) = \mathcal{N}(1 + e) \cdot \mathcal{N}(\beta_0 \cdot J) \geq (1 - \varepsilon)^m \cdot \mathcal{N}(\beta_0 \cdot J)$.

Combining everything and taking $\varepsilon = 2^{-\ell}$, we have proven that for any $\ell \geq 1$, there exists a non-zero element $\widetilde{y}_\ell \in \widetilde{J}$ such that $\widetilde{y}_\ell \cdot \widetilde{J}^{-1}$ is coprime to $q\mathcal{O}_K$ and $\|\tau(\widetilde{y}_\ell)\| \leq (1+2^{-\ell})(1-2^{-\ell})^{-1} \cdot 8m^2 \cdot \Delta_K^{2/m} \cdot \mathcal{N}(\widetilde{J})^{1/m}$. Since $\tau(\widetilde{J})$ is a lattice, it is in particular discrete, and so the set $\{\widetilde{y}_\ell\}_{\ell \geq 1}$ is finite. This implies that there must exist a non-zero $\widetilde{y} \in \widetilde{J}$ such that $\widetilde{y}\widetilde{J}^{-1}$ is coprime to $q\mathcal{O}_K$ and satisfying

$$\begin{aligned}\|\tau(\widetilde{y})\| &\leq 8m^2 \cdot \Delta_K^{2/m} \cdot \mathcal{N}(\widetilde{J})^{1/m} \\ &\leq 8m^2 \cdot \Delta_K^{2/m} \cdot \mathcal{M}(f) \cdot \mathcal{N}(J)^{1/m}.\end{aligned}$$

Let us define $y := \beta^{-1} \cdot \widetilde{y}$. Since $\widetilde{y} \in \widetilde{J} = \beta \cdot J$, then $y \in J$ (and $y \neq 0$ since $\widetilde{y} \neq 0$). Moreover, we have that $y \cdot J^{-1} = \widetilde{y} \cdot \widetilde{J}^{-1}$, so the ideal yJ^{-1} is coprime to $q\mathcal{O}_K$ as desired. Finally, for such a y and for any $1 \leq j \leq m$, we have

$$\begin{aligned}\max(1, |\alpha_j|^{m-1}) \cdot |\sigma_j(y)| &= |\sigma_j(\beta)| \cdot |\sigma_j(y)| \\ &= |\sigma_j(\beta \cdot y)| \\ &= |\sigma_j(\widetilde{y})| \\ &\leq \|\tau(\widetilde{y})\| \\ &\leq 8m^2 \cdot \Delta_K^{2/m} \cdot \mathcal{M}(f) \cdot \mathcal{N}(J)^{1/m}.\end{aligned}$$

From this, we finally conclude that

$$\left\|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right|\right\| \leq m \cdot \|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\|_{\max} \leq 8m^3 \cdot \Delta_K^{2/m} \cdot \mathcal{M}(f) \cdot \mathcal{N}(J)^{1/m}.$$

where we used Equation (7) for the first inequality and Equation (8) for the second inequality. □

Instantiating the proposition above with $f \in \mathrm{Pol}_{m,B}$ (monic irreducible polynomial of degree m and coefficients bounded by B), and $J = \mathcal{C}_\mathcal{O}$ for $\mathcal{O} = \mathbb{Z}[X]/f(X)$, we obtain the following corollary.

Corollary 5.2. *Let $m > 0$ be an integer and $B > 0$ be a real number. Let $f \in \mathrm{Pol}_{m,B}$, $K = \mathbb{Q}[X]/f(X)$ and $\mathcal{O} = \mathbb{Z}[X]/f(X)$. Let $q \geq 8m$ be a prime integer. Then there exists $y \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ such that $y \cdot \mathcal{C}_\mathcal{O}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$ and satisfying*

$$\left\|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right|\right\| \leq 16 \cdot m^8 B^5.$$

Proof. We instantiate Proposition 5.1 with $J = \mathcal{C}_\mathcal{O}$. This gives us the existence of $y \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ such that $y \cdot \mathcal{C}_\mathcal{O}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$ and satisfying

$$\left\|\left|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right|\right\| \leq 8m^3 \cdot \Delta_K^{2/m} \cdot \mathcal{M}(f) \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m}.$$

It remains to prove that this upper bound is $\leq 16 \cdot m^8 B^5$. Since $f \in \mathrm{Pol}_{m,B}$, we know from Equation (5) that $\Delta_K \leq \Delta_K \cdot \mathcal{N}(\mathcal{C}_\mathcal{O}) \leq (mB)^{2m}$. Hence we obtain that $\Delta_K^{2/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m} \leq (mB)^4$. From Lemma 2.11, we also know that $\mathcal{M}(f) \leq 1 + mB \leq 2mB$. Combining all, we obtain the desired upper bound. □

We can now combine this proposition and corollary with our framework, in order to obtain our main result.

Theorem 5.3. *Let $n \geq m \geq d > 0$ be integers. Let f be a monic irreducible polynomial of degree m, and define $K = \mathbb{Q}[X]/f(X)$ and $\mathcal{O} = \mathbb{Z}[X]/f(X)$. Let $q \geq 8m$ be a prime integer such that $q\mathcal{O}_K$ is coprime to $\mathcal{C}_\mathcal{O}$, and let $\alpha \in (0,1)$. Then there exists a* ppt *reduction from primal-*$\mathsf{RLWE}_{K,q,\alpha}$ *(resp. dual-*$\mathsf{RLWE}_{K,q,\alpha}$*) to* $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha'}$*, where $\alpha' = \alpha \cdot 8m^3 \cdot \Delta_f^{2/m} \cdot \mathcal{M}(f)$.*

Note that our reduction works for both primal-RLWE and dual-RLWE with the same increase on the noise rate α. In the case of primal-RLWE, one may hope to reduce slightly the noise increase, by taking a smaller value for y_s (see the proof). However, this does not seem easy to implement, and it looks like the gain would be a factor $\Delta_K^{1/m}$ at most, so we did not pursue this.

Proof. The result follows by combining Theorem 3.8 and Proposition 5.1. First, we set $y_s = 1$, which is valid since $1 \in I^\vee \setminus \{0\}$ for both primal and dual-RLWE cases. Next, Theorem 3.8 requires an element $y_a \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ such that the quotient ideal $y_a \mathcal{C}_\mathcal{O}^{-1}$ is coprime to $q\mathcal{O}_K$. By applying Proposition 5.1 to the conductor ideal $J = \mathcal{C}_\mathcal{O}$ with $q \geq 8m$, we are guaranteed the existence of an element $y \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ that exactly satisfies $y\mathcal{C}_\mathcal{O}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$. Therefore, it is valid to take $y_a = y$. With these choices, the parameter from Theorem 3.8 becomes $\alpha' = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(y) \right|\right|\right|$. Proposition 5.1 upper bounds this operator norm by $8m^3 \cdot \Delta_K^{2/m} \cdot \mathcal{M}(f) \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m}$. To derive the final inequality, we use the algebraic relation $\Delta_f = \Delta_K \cdot [\mathcal{O}_K : \mathcal{O}]^2$. Since the norm of the conductor $\mathcal{N}(\mathcal{C}_\mathcal{O})$ divides the square of the index $[\mathcal{O}_K : \mathcal{O}]^2$, we have $\mathcal{N}(\mathcal{C}_\mathcal{O}) \leq \Delta_f / \Delta_K$. Substituting this yields $\Delta_K^{2/m} \cdot \mathcal{N}(\mathcal{C}_\mathcal{O})^{1/m} \leq \Delta_K^{2/m} \cdot (\Delta_f/\Delta_K)^{1/m} = (\Delta_K \cdot \Delta_f)^{1/m}$. Using the fact that $\Delta_K \leq \Delta_f$, this term is bounded by $(\Delta_f^2)^{1/m} = \Delta_f^{2/m}$. Consequently, $\left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(y) \right|\right|\right| \leq 8m^3 \cdot \Delta_f^{2/m} \cdot \mathcal{M}(f)$, which yields the final target parameter $\alpha' \leq \alpha \cdot 8m^3 \cdot \Delta_f^{2/m} \cdot \mathcal{M}(f)$. □

Corollary 5.4. *Let $n \geq d > 0$ be integers. Let $q \geq 8n$ be a prime integer and let $\alpha \in (0,1)$. Let $B > 0$ be a real number, and define $\alpha' = \alpha \cdot 16 \cdot n^8 B^5$. Then,* $\mathsf{MP\text{-}LWE}_{q,n,d,\alpha'}$ *is at least as hard as primal-*$\mathsf{RLWE}_{K,q,\alpha}$ *(resp. dual-*$\mathsf{RLWE}_{K,q,\alpha}$*) for all number field $K = \mathbb{Q}[X]/f(X)$ with $f \in \mathrm{Pol}_{m,B,q}$.*

Proof. Following the proof of Theorem 5.3, the reduction holds with the target noise parameter given by $\alpha^* = \alpha \cdot \left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(y) \right|\right|\right|$, provided that $y \in \mathcal{C}_\mathcal{O} \setminus \{0\}$ satisfies $y\mathcal{C}_\mathcal{O}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$. Since $q \geq 8n \geq 8m$, we can directly apply Corollary 5.2, which guarantees the existence of such a y and bounds its operator norm by $\left|\left|\left| \mathbf{V}_f^\top \cdot \mathbf{T}(y) \right|\right|\right| \leq 16 \cdot m^8 B^5$. Substituting this bound yields $\alpha^* \leq \alpha \cdot 16 \cdot m^8 B^5$. Because $n \geq m$, we immediately obtain the final bound $\alpha^* \leq \alpha \cdot 16 \cdot n^8 B^5 =: \alpha'$. □

Improvement over previous works. We illustrate here the advantage of our new framework, compared to the previously known reductions. To do so, we exhibit a family of polynomials for which our new reduction achieve a polynomial noise growth (using Theorem 5.3), whereas the two previous reductions from [PP24] and [RSSS17, RSW18, NP26] get an exponential noise growth.

Consider the polynomial family $f(x) = x^m - bx^{m-1} + b(ax-1)^2$ for some constant $a, b \geq 2$, and $m \geq 4$ growing to infinity. Note that these polynomials are irreducible by Eisenstein's criterion. Moreover, these polynomials are constructed to have one root of the order of b, and two roots that are exponentially close to $1/a$ (when m tends to infinity). We show below that the existence of these roots break the noise expansion bounds of both previous reductions [PP24, NP26].

- **Failure of [PP24] ($y_a = y_s = 1$):** The noise growth is governed by $\|\|\mathbf{V}_f\|\|$. By definition, the entries of the Vandermonde matrix are $(\mathbf{V}_f)_{i,j} = \alpha_j^{i-1}$. The polynomial $f(x)$ possesses a large root $\alpha_1 \approx b \geq 2$, hence the matrix norm grows exponentially with respect to the degree m:

$$\|\|\mathbf{V}_f\|\| \geq \|\mathbf{V}_f\|_{\max} \geq |\alpha_1|^{m-1} \approx b^{m-1} = \Omega(2^m).$$

- **Failure of [NP26] ($y_s = p_1^\vee$):** Let us ignore the polynomial factors in the noise growth of Theorem 4.4, and focus on the quantity $\left\|\left\|\mathbf{M}_f(p_1^\vee)\mathbf{V}_f^{-1}\right\|\right\|$. It was proved in [NP26, Lemma 4.1] that

$$\left(\mathbf{M}_f(p_1^\vee)\mathbf{V}_f^{-1}\right)_{i,j} = \frac{-f_0 \cdot \alpha_j^{i-2}}{f'(\alpha_j)},$$

  for all i, j. Taking α_j to be one of the two roots exponentially close to $1/a$, we have that $|f'(\alpha_j)| = \mathcal{O}(2^{-m})$. Choosing $i = 2$ and plugging this into the formula for $(\mathbf{M}_f(p_1^\vee)\mathbf{V}_f^{-1})_{i,j}$, we see that

$$\left\|\left\|\mathbf{M}_f(p_1^\vee)\mathbf{V}_f^{-1}\right\|\right\| \geq \left|\left(\mathbf{M}_f(p_1^\vee)\mathbf{V}_f^{-1}\right)_{2,j}\right| = \frac{b}{|f'(\alpha_j)|} = \Omega(2^m).$$

- **Success of Theorem 5.3:** applying our reduction from Theorem 5.3 to these polynomials, we obtain a noise growth of $8m^3 \cdot \Delta_f^{2/m} \cdot \mathcal{M}(f)$. Equation (5) tells us that $\Delta_f^{2/m} \leq (m(a^2b))^4$ and Lemma 2.11 tells us that $\mathcal{M}(f) \leq \sum_i |f_i| \leq 3ba^2$. Hence, the noise growth that we obtain is upper bounded by $O(m^4)$ (since we took a and b to be constant).

Numerical experiments. We performed numerical experiments to estimate the tightness of our upper bound in Corollary 5.2.[8] In order to avoid computing the spectral norm of the matrix, we used Eq. (7), which tells us that $\left\|\left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|\right\| \leq m \left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|_{\max}$. Therefore, to assess the tightness of the

[8] The code for our experiments is available at `https://github.com/Summwer/code-unified-reduction-MP-LWE`.

upper bound $\left\|\left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|\right\| \leq 16m^8B^5$ derived in Corollary 5.2, it suffices to evaluate the relationship $\left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|_{\max} \leq 16m^7B^5$. As illustrated in Figure 1 (varying m with $B = 2$) and Figure 2 (varying B with $m = 5$), the observed maximum norms remain extremely small. In contrast, the scaled theoretical bound of $16m^7B^5$ grows rapidly. This suggests that the true value of $\left\|\left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|\right\|$ is substantially smaller than $16m^8B^5$ and that the worst-case theoretical bound is highly pessimistic in practice.

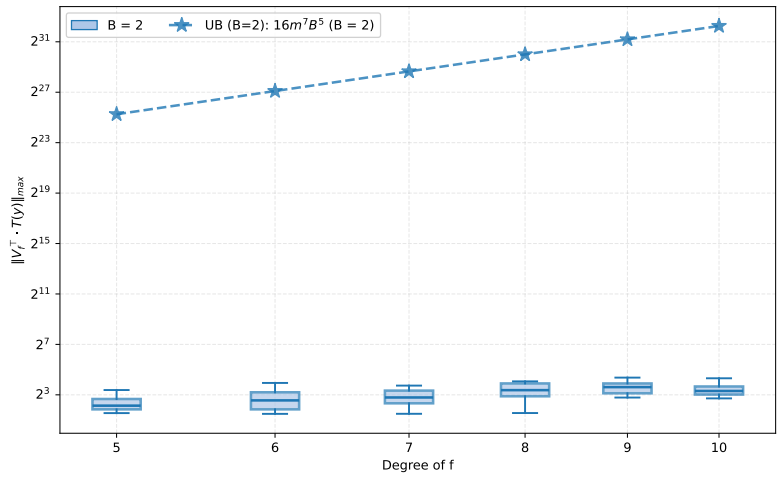

Fig. 1. Test values of $\left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|_{\max}$ versus the theoretical upper bound for varying degrees $m \in \{5, \ldots, 10\}$ by taking 30 independent random samples for $B = 2$.

Acknowledgement. The authors would like to warmly thank Rahinatou Yuh Njah Nchiwo for her comments on a first version of this article. We are also grateful to the Asiacrypt'26 reviewers for their constructive feedback. Wenwen Xia was supported by the National Cryptologic Science Fund of China under Grant No. 2025NCSF01005. Wenwen Xia and Alice Pellet-Mary were supported by France 2030 under the French National Research Agency award number "ANR-22-PNCQ-0002" (HQI initiative). Alice Pellet-Mary is supported by the TOTORO ANR grant (ANR-23-CE48-0002) and by the France 2030 program, managed by the French National Research Agency (ANR-22-PETQ-0008 PQ-TLS).

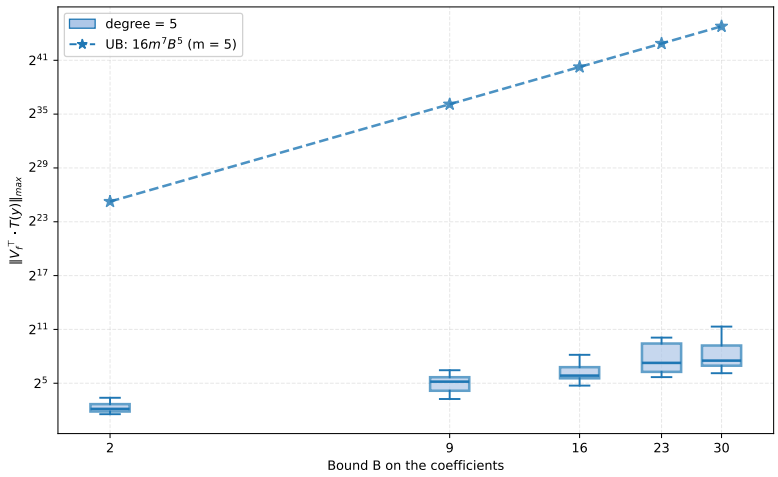

Fig. 2. Test values of $\left\|\mathbf{V}_f^\top \cdot \mathbf{T}(y)\right\|_{\max}$ versus the theoretical upper bound for degree 5 and varying coefficient bounds $B \in \{2, 9, 16, 23, 30\}$ by taking 30 independent random samples for each B.

References

BBD+19. Shi Bai, Katharina Boudgoust, Dipayan Das, Adeline Roux-Langlois, Weiqiang Wen, and Zhenfei Zhang. Middle-product learning with rounding problem and its applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 55–81. Springer, 2019.

BBPS19. Madalina Bolboceanu, Zvika Brakerski, Renen Perlman, and Devika Sharma. Order-lwe and the hardness of ring-lwe with entropic secrets. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 91–120. Springer, 2019.

BDH+20. Shi Bai, Dipayan Das, Ryo Hiromasa, Miruna Rosca, Amin Sakzad, Damien Stehlé, Ron Steinfeld, and Zhenfei Zhang. Mpsign: a signature from small-secret middle-product learning with errors. In *IACR International Conference on Public-Key Cryptography*, pages 66–93. Springer, 2020.

BGV14. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1–36, 2014.

Con09a. Keith Conrad. The conductor ideal of an order. *Expository paper/Lecture notes. Available at:* `https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf`, 2009.

Con09b. Keith Conrad. The different ideal. *Expository papers/Lecture notes. Available at: http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/different.pdf*, 2009.

DAZ19. Dipayan Das, Man Ho Au, and Zhenfei Zhang. Ring signatures based on middle-product learning with errors problems. In *Progress in Cryptology–AFRICACRYPT 2019: 11th International Conference on Cryptology in*

Africa, Rabat, Morocco, July 9–11, 2019, Proceedings 11, pages 139–156. Springer, 2019.

FLA23. Jingjing Fan, Xingye Lu, and Man Ho Au. Adaptively secure identity-based encryption from middle-product learning with errors. In *Australasian Conference on Information Security and Privacy*, pages 320–340. Springer, 2023.

Hir18. Ryo Hiromasa. Digital signatures from the middle-product lwe. In *Provable Security: 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings 12*, pages 239–257. Springer, 2018.

LPR10. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 1–23. Springer, 2010.

LS15. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

LSW+23. Hao Lin, Shi-Feng Sun, Mingqiang Wang, Joseph K Liu, and Weijia Wang. Shorter linkable ring signature based on middle-product learning with errors problem. *The Computer Journal*, 66(12):2974–2989, 2023.

LVV19. Alex Lombardi, Vinod Vaikuntanathan, and Thuy Duong Vuong. Lattice trapdoors and ibe from middle-product lwe. In *Theory of Cryptography Conference*, pages 24–54. Springer, 2019.

Lyu16. Vadim Lyubashevsky. Digital signatures based on the hardness of ideal lattice problems in all rings. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 196–214. Springer, 2016.

Mah64. Kurt Mahler. An inequality for the discriminant of a polynomial. *Michigan Math. J*, 11(3):257–262, 1964.

NP26. Rahinatou Yuh Njah Nchiwo and Alice Pellet-Mary. Improved reduction from rlwe to mp-lwe. *PKC*, 2026.

PP24. Chris Peikert and Zachary Pepin. Algebraically structured lwe, revisited: C. peikert, z. pepin. *Journal of Cryptology*, 37(3):28, 2024.

RSSS17. Miruna Roşca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. Middle-product learning with errors. In *Annual International Cryptology Conference*, pages 283–297. Springer, 2017.

RSW18. Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-lwe and polynomial-lwe problems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 146–173. Springer, 2018.

SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 617–635. Springer, 2009.

SSZ19. Ron Steinfeld, Amin Sakzad, and Raymond K Zhao. Practical mp-lwe-based encryption balancing security-risk versus efficiency. *Designs, Codes and Cryptography*, 87(12):2847–2884, 2019.

Sut16. Andrew Sutherland. The different and the discriminant. *Lecture notes: Number theory I, Fall 2016. Lecture 12. Available at https://math.mit.edu/classes/18.785/2016fa/LectureNotes12.pdf*, 2016.