On the Integer Polynomial Learning with Errors Problem

Julien Devevey[1(✉)], Amin Sakzad[2], Damien Stehlé[1,3], and Ron Steinfeld[2]

[1] ENS de Lyon, Laboratoire LIP (University of Lyon, CNRS, ENSL, INRIA, UCBL), Lyon, France
julien.devevey@ens-lyon.fr
[2] Faculty of Information Technology, Monash University, Clayton, Australia
[3] Institut Universitaire de France, Paris, France

Abstract. Several recent proposals of efficient public-key encryption are based on variants of the polynomial learning with errors problem (PLWE^f) in which the underlying *polynomial* ring $\mathbb{Z}_q[x]/f$ is replaced with the (related) modular *integer* ring $\mathbb{Z}_{f(q)}$; the corresponding problem is known as *Integer Polynomial Learning with Errors* (I-PLWE^f). Cryptosystems based on I-PLWE^f and its variants can exploit optimised big-integer arithmetic to achieve good practical performance, as exhibited by the ThreeBears cryptosystem. Unfortunately, the average-case hardness of I-PLWE^f and its relation to more established lattice problems have to date remained unclear.

We describe the first polynomial-time average-case reductions for the search variant of I-PLWE^f, proving its computational equivalence with the search variant of its counterpart problem PLWE^f. Our reductions apply to a large class of defining polynomials f. To obtain our results, we employ a careful adaptation of Rényi divergence analysis techniques to bound the impact of the integer ring arithmetic carries on the error distributions. As an application, we present a deterministic public-key cryptosystem over integer rings. Our cryptosystem, which resembles ThreeBears, enjoys one-way (OW-CPA) security provably based on the search variant of I-PLWE^f.

1 Introduction

The Learning with Errors (LWE) problem was first introduced by Regev in [Reg09]. This problem, in its search form, consists in finding $\mathbf{s} \in \mathbb{Z}_q^m$ for some parameters $q > 2$ and $m \geq 1$, given arbitrarily many samples of the form $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$ over $\mathbb{Z}_q^m \times \mathbb{Z}_q$. Here, the so-called error e_i is a random small-magnitude integer and $\mathbf{a}_i$ is uniform in $\mathbb{Z}_q^m$. A variant of this problem can be defined by replacing $\mathbb{Z}$ by a polynomial ring $\mathbb{Z}[x]/f$, where $f \in \mathbb{Z}[x]$ is monic and irreducible. In that case, the problem is called Polynomial-LWE (PLWE) if $m = 1$ [SSTX09], and Module-LWE (MLWE) if $m \geq 1$ [BGV12]. As illustrated by their prominence in the NIST post-quantum cryptography project [NIS], in practice, these problems over polynomial rings are typically preferred to LWE, as

J. A. Garay (Ed.): PKC 2021, LNCS 12710, pp. 184–214, 2021.
https://doi.org/10.1007/978-3-030-75245-3_8

they lead to more efficient cryptographic constructions. Their intractability has been (quantumly) linked to some worst-case problems for some restricted classes of Euclidean lattices (see, e.g., [SSTX09,LPR10,LS15,AD17,PRS17,RSW18]).

More recently, Gu [Gu17,Gu19] introduced another variant of LWE which we will refer to as the Integer Polynomial Learning With Errors problem (I-PLWE), by consistency with PLWE (in [Gu17,Gu19], it is called integer ring learning with errors). It is related to PLWE, as follows. For an integer q, evaluation in q is a homomorphism from $\mathbb{Z}[x]/f$ to $\mathbb{Z}_{f(q)}$. Note that it does not naturally extend to a homomorphism from $\mathbb{Z}_q[x]/f$ to $\mathbb{Z}_{f(q)}$ (this will actually be the main source of technical difficulty throughout this article). Nevertheless, for a polynomial $a(x) = \sum_{i<\deg f} a_i x^i \in \mathbb{Z}_q[x]/f$, we can assume that $a_i \in (-q/2, q/2]$ for all i and consider the integer $a(q) := \sum_{i<\deg f} a_i q^i \in \mathbb{Z}_{f(q)}$. This allows to relate an element of $\mathbb{Z}_q[x]/f$ to an integer $\mathbb{Z}_{f(q)}$. In this spirit, I-PLWE asks to find $s \in \mathbb{Z}_{f(q)}$ given arbitrarily many samples of the form $(a_i, a_i s + e_i)$ over $\mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}$, where the a_i's are uniform in $\mathbb{Z}_{f(q)}$ and the e_i's have a centered q-ary decomposition with small-magnitude coefficients (we refer the reader to Sect. 2 for a formal definition). This problem was investigated for $f = x^m + 1$ in [Gu17,Gu19], which also contain an asymptotically efficient public-key encryption scheme with IND-CPA security inherited from I-PLWE's presumed hardness. This encryption scheme was generalized in [BCSV20]. A module extension of I-PLWE was considered for $f = x^m - x^{m/2} - 1$ in the ThreeBears candidate [Ham17] to the NIST PQC project [NIS]. Taking I-PLWE (or its module extension) allows to replace a polynomial ring by large integers, and to take advantage of efficient large-integer arithmetic algorithms and libraries. A somewhat similar intractability assumption was considered in [AJPS18,Sze17], with error terms of small Hamming weight in their binary decomposition.

The presence of *carries* in the integer operations underlying those integer-ring problems distinguishes them from their carry-free polynomial analogues, and creates technical annoyances when analyzing their intractability and building cryptosystems. In particular, the only reduction from PLWE to I-PLWE known so far, due to [Gu17], holds only for a worst-case variant of I-PLWE, in which the error terms are arbitrary (among small-magnitude errors). The reduction proceeds by converting PLWE samples (i.e., polynomials) to I-PLWE samples (i.e., integers). The reduction analysis only shows that the error terms resulting from the conversion have q-ary decompositions with small-magnitude coefficients (see [Gu17, Lemma 3.7]). As noted in [Gu19], which mentions proving hardness of I-PLWE as an open problem, this is insufficient to support the intractability of the average-case variant I-PLWE, with random error terms. The situation is identical for the converse direction, from I-PLWE to PLWE. Unfortunately, it seems very difficult to design a public-key encryption scheme with security inherited from the intractability of this worst-case variant of I-PLWE. For example, Gu's encryption scheme [Gu17,Gu19] is proved secure under the presumed intractability of a *decision* and *average-case* variant of I-PLWE, in which the error terms are randomly distributed, and one only asks to distinguish I-PLWE samples from uniform samples rather than finding the secret s from I-PLWE samples.

A concrete security analysis of I-PLWE is given in [BCF20] against certain attacks, such as classical meet-in-the-middle and lattice-based attacks. When $f = x^m + 1$ with m composite with an odd divisor, they give an improved attack that can be viewed as the I-PLWE analogue of Gentry's attack on NTRU with a composite defining polynomial [Gen01]. This improved attack does not apply when f is irreducible. In particular, classical meet-in-the-middle and lattice-based techniques are combined in order to build an improved lattice-based attack for $f = x^m + 1$ with m composite with an odd divisor.

Contributions. We exhibit polynomial-time reductions between the *search* and *average-case* variant of I-PLWE$^{(f)}$ and the *search* and *average-case* variant of PLWE$^{(f)}$, for a large class of defining polynomials f: the reductions only require that f is monic.[1] Compared to [Gu17], the reduction analyses do consider the error term distributions. Our results show the hardness equivalence of search I-PLWE and search PLWE. The reduction loss in success probability depends on the degree of f, its expansion factor (the definition of the expansion factor is recalled in Sect. 2), the relative magnitude of the error terms and secret, and the number of samples. In particular, we can set q polynomial in the degree of f such that the loss is polynomial for a constant number of samples.

These reductions handle random error terms, but are limited to the *search* variants, as opposed to the *decision* variants. This makes it complicated to devise a public-key encryption scheme with security based on the presumed intractability of PLWE. In particular, we do not know how to prove the security of Gu's encryption scheme under well-established assumptions: indeed, this scheme was designed to provide IND-CPA security based on the presumed intractability of the decision version of I-PLWE. As our second main contribution, we exhibit a *deterministic* public-key encryption scheme, which can be viewed as a mild variant of Gu's. It is designed to provide one-way security under chosen plaintext attacks (OW-CPA), under the *search* I-PLWE and the *decision* PLWE intractability assumptions. By adapting the techniques developed in [RSW18], one can devise reductions between appropriately defined search and decision versions of PLWE for large families of defining polynomials f and with limited parameter losses. Thanks to our first contribution, this means that our scheme can be adapted to enjoy security based on any single intractability assumption among search I-PLWE, search PLWE and decision PLWE. Finally, we note that a deterministic public-key encryption scheme enjoying OW-CPA security can be converted in an IND-CCA key-exchange mechanism in the random oracle model [HHK17].

Our techniques and results readily extend to the module case: one can define I-MLWE analogously to I-PLWE, and reduce the search variants of I-MLWE and MLWE to one another. Our deterministic encryption scheme can also be adapted to the module case, and it then somewhat resembles the ThreeBears candidate to the NIST PQC project [Ham17].

[1] As commonly done, we also impose irreducibility of f in the problem definitions, to avoid weaknesses such as those pointed out in [BCF20].

Techniques. In the reductions to/from I-PLWE from/to PLWE, the main idea is to convert integers into polynomials and vice-versa via the 'approximate' (due to the 'small' carries) relations between the integer and polynomial ring operations studied in Sect. 3. We then use the Rényi divergence analysis approach [LSS14,BLRL+18] to show that, for suitably chosen parameters, the small carry errors incurred by the format conversions do not shift the error distribution "too far" from the desired distribution. This allows to reduce these average-case problems to one another. The restriction to search problems (as opposed to decision problems) in our hardness results is inherited from the use of the Rényi divergence.

Beyond the distributional analysis of the error terms, our reductions are also more general than those of [Gu17] as they apply for any monic defining polynomial f. The main difficulty here is to handle the homomorphism defect of the map from $\mathbb{Z}_q[x]$ to $\mathbb{Z}_{f(q)}$ by taking a polynomial a with coefficients a_i viewed as integers in $(-q/2, q/2]$ and computing $a(q) := \sum_{i<\deg f} a_i q^i \in \mathbb{Z}_{f(q)}$. In particular, we distinguish two cases, depending whether $f(q) > q^{\deg f}$, for which this map is injective, or $f(q) < q^{\deg f}$, for which it is surjective. When the map is injective, we randomize it so that it reaches the whole range, and when it is surjective, we consider a randomized inverse mapping. Overall, this leads to four reductions, corresponding to converting integers to polynomials or polynomials to integers, depending on whether $f(q) > q^{\deg f}$ or $f(q) < q^{\deg f}$. Importantly, for our reductions to go through, we need the I-PLWE secret s to have a q-ary decomposition with small coefficients, which corresponds to taking a small-coefficient secret in PLWE: in our analysis, this is needed to ensure that carries due the multiplication $a_i \cdot s$ remain small.

The design of the encryption scheme is relatively standard. We use an I-PLWE sample $\mathsf{pk} := (a, b) = (a, as + e)$ as a public key. We encrypt a triple (t, e', e'') of integers with q-ary decompositions with small coefficients, by generating two I-PLWE samples $(c_1, c_2) := (at + Ke', bt + Ke'')$. Here K is a small integer that enables decryption: given $c_2 - c_1 s$, one recovers t by reducing the q-ary decomposition coefficients modulo K and dividing the resulting integer by e modulo $f(q)$. Once t is known, one may recover e' and e''. Overall, this provides a deterministic public-key encryption scheme. The proof of OW-CPA security exploits the intractability of decision PLWE to argue that pk is somewhat close to uniform: this is achieved by game hops with distributional updates on pk whose effects on the OW-CPA winning probability are controlled by Rényi divergence arguments. The compatibility of OW-CPA security with the Rényi divergence was similarly exploited in the security proof of the Frodo candidate to the NIST PQC project [ABD+17]. Finally, once pk is replaced by a uniform pair $(a, b) \in \mathbb{Z}_{f(q)}^2$, OW-CPA security follows from the presumed intractability of I-PLWE.

Open Problems. Similarly to I-PLWE, the one-dimensional LWE problem also involves samples of the form $(a_i, a_i s + e_i)$ over $\mathbb{Z}_p \times \mathbb{Z}_p$ for some integer p. Reductions between one-dimensional LWE and standard multi-dimensional LWE have been given in [BLP+13], hence supporting the hardness of one-dimensional LWE (for a large modulus p). Unfortunately, one-dimensional LWE is different

from I-PLWE in that the error term e_i is small compared to p in one-dimensional LWE, and has a q-ary decomposition with small coefficients in I-PLWE. Obtaining a reduction from one-dimensional LWE to I-PLWE would be an interesting avenue to prove hardness of PLWE (with polynomially-bounded modulus) under LWE.

Interestingly, converting an error-free I-PLWE sample (a, as) into a PLWE sample $(A, AS + E)$ creates a non-zero error E, due to the carries in the multiplication of a by s modulo $f(q)$. This PLWE variant is insecure as one can recover s by dividing as by a modulo $f(q)$. Error-free I-PLWE resembles the polynomial-ring variant of Learning With Rounding [BPR12]: in the first, the error term is a deterministic function of (A, S), whereas in the second it is a deterministic function of AS. This raises the question of studying which functions of (A, S) lead to secure or insecure deterministic-error variants of PLWE.

One limitation of our techniques is due to the fact that the Rényi divergence is convenient to study search problems but not so for decision problems, notably because of the probability preservation property (see Definition 1) which is not meaningful in the case where the probabilities are close to $\frac{1}{2}$ instead of 0. For this reason, it is unclear how to extend our analysis to obtain reductions between decision I-PLWE and decision PLWE. Finding a reduction between decision I-PLWE and decision PLWE would require different techniques from ours. To prove hardness of decision I-PLWE, an alternative path would be to obtain a search to decision reduction. Unfortunately, it is also unclear whether existing search to decision reductions for PLWE (see [LPR10, PRS17, RSW18]) could be adapted to I-PLWE, mainly because of the highly structured noise distribution.

2 Preliminaries

We let $x \hookleftarrow D$ denote the action of sampling x from distribution D. We let $\mathcal{U}(S)$ denote the uniform distribution over any finite set S and we write $x \hookleftarrow S$ instead of $x \hookleftarrow \mathcal{U}(S)$. For any $P = \sum_i P_i x^i \in \mathbb{Z}[x]$, $P \bmod q$ denotes $\sum_i (P_i \bmod q) x^i$.

2.1 Integer Gaussian Distributions

For $\sigma > 0$, we define the centered Gaussian function of standard deviation parameter σ as $\rho_\sigma(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2/\sigma^2)$, for any $\mathbf{x} \in \mathbb{R}^m$. We define the centered integer Gaussian distribution $D_{\mathbb{Z}^m,\sigma}$ of standard deviation parameter σ by

$$\forall \mathbf{x} \in \mathbb{Z}^m : \; D_{\mathbb{Z}^m,\sigma}(\mathbf{x}) = \rho_\sigma(\mathbf{x})/\rho_\sigma(\mathbb{Z}^m).$$

For $B > 0$, we use $D_{\mathbb{Z}^m,\sigma,B}$ to denote the distribution obtained from $D_{\mathbb{Z}^m,\sigma}$ by cutting its tail (by rejection sampling) to take values in $(-B/2, B/2]^m$. Since we are going to reduce polynomials sampled from this distribution to $\mathbb{Z}_q[x]$, by reducing each of their coefficients modulo q, and then look at the representatives of said coefficients in $(-q/2, q/2]$, we will use $D_{\mathbb{Z}^{<m}[x],\sigma,q}$ to sample such polynomials. Doing so gives us polynomials whose coefficients are not affected by reductions modulo q.

We will let $D_{\mathbb{Z}^{<m}[x],\sigma,B}$ denote the distribution over integer polynomials of degree $< m$ obtained by sampling the coefficient vector according to $D_{\mathbb{Z}^m,\sigma,B}$. We also write $D_{\mathbb{Z}[x]/f,\sigma,B}$ for $f \in \mathbb{Z}[x]$ monic of degree m to denote the distribution $D_{\mathbb{Z}^{<m}[x],\sigma,B}$ while insisting that we view the sample as an element of $\mathbb{Z}[x]/f$.

2.2 The Rényi Divergence

The Rényi divergence is a prominent tool that we use throughout this work. Its relevance to security proofs in lattice-based cryptography was stressed in [BLRL+18].

Definition 1 (Rényi Divergence). *Let P and Q be two discrete probability distributions, such that we have $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$. The Rényi divergences of orders 2 and ∞ are respectively defined as follows:*

$$R(P||Q) := \sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^2}{Q(x)} \quad \text{and} \quad R_\infty(P||Q) := \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

The following lemma, listing classical properties of the Rényi divergence, is borrowed from [BLRL+18].

Lemma 1. *Let P and Q be two discrete probability distributions such that we have $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$. The following properties hold.*

- ***Log. Positivity:*** *$R(P||Q) \geq R(P||P) = 1$.*
- ***Data Processing Inequality:*** *$R(P^f||Q^f) \leq R(P||Q)$ for any function f, where X^f denotes the distribution of $f(x)$ when sampling $x \hookleftarrow X$.*
- ***Multiplicativity:*** *Let P and Q be two distributions of a pair of random variables X_1 and X_2 and P_i and Q_i denote the marginal distribution of X_i under P and Q, respectively. If X_1 and X_2 are independent, then $R(P||Q) = R(P_1||Q_1)R(P_2||Q_2)$. Otherwise, we have $R(P||Q) \leq R_\infty(P_1||Q_1) \cdot \max_{x_1 \in \mathrm{Supp}(P_1)} R((P_2|x_1)||(Q_2|x_1))$.*
- ***Probability Preservation:*** *Let $E \subseteq \mathrm{Supp}(Q)$ be an arbitrary event. Then, we have $Q(E) \geq P(E)^2/R(P||Q)$.*

2.3 The Polynomial Learning with Errors Problem

We recall here the PLWE problem studied, e.g., in [SSTX09,LPR10,RSW18]. Here we choose to tail-cut the Gaussian distribution such that each coefficient of the error already belongs to $(-q/2, q/2]$.

Definition 2 (P distribution). *Let $q \geq 2$, $f \in \mathbb{Z}[x]$ monic and $\sigma > 0$. Given $s \in \mathbb{Z}_q[x]/f$, we define the distribution $\mathsf{P}^{(f)}_{q,\sigma}(s)$ over $\mathbb{Z}_q[x]/f \times \mathbb{Z}[x]/f$ obtained by sampling $a \hookleftarrow \mathbb{Z}_q[x]/f$, $e \hookleftarrow D_{\mathbb{Z}[x]/f,\sigma,q}$ and returning $(a, b = a \cdot s + e) \in \mathbb{Z}_q[x]/f \times \mathbb{Z}_q[x]/f$.*

The distribution above is sometimes generalized to arbitrary covariance matrices. Our results carry over to this setting, as their proofs do not involve arguments specific to spherical Gaussians. For the sake of simplicity, we describe them using spherical Gaussian distributions.

Definition 3 (Search PLWE). *Let $q \geq 2$, $f \in \mathbb{Z}[x]$ irreducible and monic, and $\sigma > \sigma' > 0$. The problem $\mathsf{sPLWE}^{(f)}_{q,\sigma,\sigma'}$ consists in finding $s \hookleftarrow D_{\mathbb{Z}[x]/f,\sigma',q}$, given arbitrarily many samples from $\mathsf{P}^{(f)}_{q,\sigma}(s)$. For an algorithm $\mathcal{A}$, we define $\mathsf{Adv}^{\mathsf{sPLWE}}_{f,q,\sigma,\sigma'}(\mathcal{A})$ as the probability that $\mathcal{A}$ returns s (over the randomness of s, the samples and $\mathcal{A}$'s internal randomness). For $t \geq 1$, we write $\mathsf{sPLWE}^{(f)}_{q,\sigma,\sigma',t}$ to restrict the number of samples to at most t.*

For technical convenience, we use an average-case variant of search PLWE. It is computationally equivalent (by random self-reducibility) to the more standard worst-case variant in which s is arbitrary. We also assume that s is sampled from a Gaussian distribution, rather than the more common choice of uniform distribution. By adapting the technique from [ACPS09], sPLWE with uniform secret and error distribution $D_{\mathbb{Z}[x]/f,\sigma',q}$ reduces to $\mathsf{sPLWE}^{(f)}_{q,\sigma',\sigma',t}$ with identical secret and error distribution equal to $D_{\mathbb{Z}[x]/f,\sigma',q}$. By adding independent Gaussian samples to the second components of the sPLWE samples, one can reduce $\mathsf{sPLWE}^{(f)}_{q,\sigma',\sigma',t}$ to $\mathsf{sPLWE}^{(f)}_{q,\sigma',\sigma,t}$. The Gaussian sum may be analyzed using [BF11, Lemma 4.12]. Letting $m = \deg f$, one may set $\sigma' = \Omega(\sqrt{m})$ (to obtain a Gaussian error term) and $q = \Omega(\sigma\sqrt{m})$ (to handle the Gaussian tail-cutting), to limit the advantage loss to an additive $2^{-\Omega(m)}$ term.

Definition 4 (Decision PLWE). *Let $q \geq 2$, $f \in \mathbb{Z}[x]$ irreducible and monic, and $\sigma > \sigma' > 0$. The problem $\mathsf{dPLWE}^{(f)}_{q,\sigma,\sigma'}$ consists in distinguishing between oracle accesses to $D_0 = \mathcal{U}(\mathbb{Z}_q[x]/f \times \mathbb{Z}[x]/f)$ and $D_1 = \mathsf{P}^{(f)}_{q,\sigma}(s)$ where $s \hookleftarrow D_{\mathbb{Z}[x]/f,\sigma',q}$ is sampled once and for all. For an algorithm $\mathcal{A}$, we define*

$$\mathsf{Adv}^{\mathsf{dPLWE}}_{f,q,\sigma,\sigma'}(\mathcal{A}) = \left|\Pr[\mathcal{A}^{D_0} \to 1] - \Pr[\mathcal{A}^{D_1} \to 1]\right|.$$

For $t \geq 1$, we write $\mathsf{dPLWE}^{(f)}_{q,\sigma,\sigma',t}$ to restrict the number of samples to at most t.

The techniques from [RSW18] can be adapted to reduce sPLWE to dPLWE for exponentially many defining polynomials f as a function of the degree m. Note that for this reduction to go through, one needs to use non-spherical Gaussian distributions and to sample the covariance matrix from a specific distribution. The reduction incurs an increase of the maximum singular value of that covariance matrix, which is polynomial in m and the expansion factor of f.

Definition 5 (Expansion Factor). *Let $q \geq 2$. Let $f \in \mathbb{Z}[x]$ of degree m. The expansion factor of f, denoted $\mathsf{EF}(f)$ is defined as:*

$$\mathsf{EF}(f) := \max_{g \in \mathbb{Z}^{<2m-1}[x] \setminus \{0\}} (\|g \bmod f\|_\infty / \|g\|_\infty).$$

As an example of polynomial f with $\mathsf{EF}(f) \leq \mathrm{poly}(m)$, we can mention gap polynomials $f = x^m + g$ with $\deg(g) \leq m/2$ and $\|g\|_\infty \leq \mathrm{poly}(m)$ (see [LM06]).

2.4 The Integer Polynomial Learning with Errors Problem

The integer variant I-PLWE of PLWE is parameterized by a monic polynomial f and an integer $q > 2$ (and a noise parameters, as we will see below). It is defined using the set $\mathbb{Z}_{f(q)}$ of integers modulo $f(q)$. This set can be viewed as polynomials in $\mathbb{Z}_q[x]/f$, via the map consisting in taking the representative in $(-q/2, q/2]$ of every coefficient and evaluating the resulting polynomial in q. This format conversion is at the core of the reductions between I-PLWE and PLWE that we will describe. Unfortunately, this conversion is imperfect, most visibly because the two sets do not have the same sizes (unless $f = x^m$ for some integer m, but this case is excluded as PLWE is defined for f irreducible).

Before introducing I-PLWE, we define the integer range $I_{f,q}$ from where we choose the representatives of $\mathbb{Z}_{f(q)}$. It is not always $(-f(q)/2, f(q)/2]$. This oddity stems from the fact that when q is even, the set of evaluations in q of polynomials in $\mathbb{Z}_q[x]/f$ with their coefficients seen as integers in $(-q/2, q/2]$, is not zero-centered. The specific definition of $I_{f,q}$ is justified by Lemma 4.

Definition 6 (Representatives range for $\mathbb{Z}_{f(q)}$). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ monic of degree $m > 0$. We define:*

$$I_{f,q} = \begin{cases} (\frac{q}{2}\frac{q^m-1}{q-1} - f(q), \frac{q}{2}\frac{q^m-1}{q-1}] & \text{if } q \text{ even and } q\frac{q^m-1}{q-1} \geq f(q) \geq q^m, \\ (-\frac{q-2}{2}\frac{q^m-1}{q-1}, f(q) - \frac{q-2}{2}\frac{q^m-1}{q-1}] & \text{if } q \text{ even and } q^m > f(q) > (q-2)\frac{q^m-1}{q-1}, \\ (-f(q)/2, f(q)/2] & \text{otherwise.} \end{cases}$$

Whenever we consider an element $\bar{a}$ of $\mathbb{Z}_{f(q)}$ and want to choose a representative a in $\mathbb{Z}$ for it, we will choose it such that $a \in I_{f,q}$.

We now recall (and generalize) the I-PLWE problem introduced by Gu [Gu19].

Definition 7 (IP distribution). *Let $q > 2$, $f \in \mathbb{Z}[x]$ monic of degree $m > 0$, and $\sigma > 0$. We first define the distribution $D_{\mathbb{Z}_{f(q)},\sigma,q}$ as the distribution obtained by sampling $E \hookleftarrow D_{\mathbb{Z}^{<m+1}[x],\sigma,q}$, setting $e = E(q)$ and rejecting if it does not belong to $I_{f,q}$. Given $s \in \mathbb{Z}_{f(q)}$, we define the distribution $\mathsf{IP}^{(f)}_{q,\sigma}(s)$ over $\mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}$ obtained by sampling $a \hookleftarrow \mathbb{Z}_{f(q)}$, $e \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma,q}$ and returning $(a, b = a \cdot s + e) \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}$.*

Note that this definition slightly diverges from Gu's, as we choose a different noise distribution. Previously, the noise was sampled from $D_{\mathbb{Z}^{<m}[x],\sigma}$, evaluated on q and reduced modulo $f(q)$. To sample from the distribution $D_{\mathbb{Z}_{f(q)},\sigma,q}$ from Definition 7, one can do the following:

- If $f(q) < q^m$, sample $E \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma,q}$ and reject it if $E(q) \notin I_{f,q}$. This greatly reduces the rejection probability while still defining a probability distribution over the whole set $I_{f,q}$.
- If $f(q) \geq q^m$, sample $E \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma,q}$. Compute $e' := E(q)$. Next let $C := 1 + 2\exp(-\pi/\sigma^2)$ and $p := \exp(-\pi/\sigma^2)/C$. Then set $e'' = q^m$ with probability p, $e'' = -q^m$ with probability p and $e'' := 0$ else. Finally set $e := e' + e''$ and reject it if it does not belong to $I_{f,q}$. In that case, the rejection probability is at most $2p = 2\exp(-\pi/\sigma^2)/C$.

The different claims made here can be proven using the results from Lemma 4.

Our reductions will only concern the search version of I-PLWE, so we only define this one. The definition can be adapted to a decision version.

Definition 8 (Search I-PLWE). *Let $q > 2$, $f \in \mathbb{Z}[x]$ irreducible and monic, and $\sigma > \sigma' > 0$. The problem* $\mathsf{sI\text{-}PLWE}^{(f)}_{q,\sigma,\sigma'}$ *consists in finding $s \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma',q}$, given arbitrarily many samples from* $\mathsf{IP}^{(f)}_{q,\sigma}(s)$*. For an algorithm $\mathcal{A}$, we define* $\mathsf{Adv}^{\mathsf{sI\text{-}PLWE}}_{f,q,\sigma,\sigma'}(\mathcal{A})$ *as the probability that $\mathcal{A}$ returns s (over the randomness of s, the samples and $\mathcal{A}$'s internal randomness). For $t \geq 1$, we write* $\mathsf{sI\text{-}PLWE}^{(f)}_{q,\sigma,t}$ *to restrict the number of samples to at most t.*

2.5 Public-Key Encryption

We recall the definition of deterministic encryption with perfect correctness.

Definition 9 (Deterministic public-key encryption). *A deterministic public-key encryption scheme is a triple of polynomial-time algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *with the following specifications.*

KeyGen(1^λ)**.** *Algorithm* KeyGen *is probabilistic. It takes as input the security parameter λ (in unary) and outputs a public key* pk *and a secret key* sk*. We assume that the keys contain descriptions of a plaintext set $\mathcal{M}_\lambda$ and a ciphertext set $\mathcal{C}_\lambda$ that depend only on λ.*

Enc(pk, M)**.** *Algorithm* Enc *is deterministic. It takes as input a public key* pk *and a plaintext $M \in \mathcal{M}$, and outputs a ciphertext $C \in \mathcal{C}_\lambda$.*

Dec(sk, C)**.** *Algorithm* Dec *is deterministic. It takes as input a secret key* sk *and a ciphertext $C \in \mathcal{C}$, and outputs a plaintext $M \in \mathcal{M}_\lambda$.*

The correctness requirement states that for all $(\mathsf{pk}, \mathsf{sk})$ *output by* KeyGen *and all $M \in \mathcal{M}$, we have* $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, M)) = M$.

For such a deterministic encryption scheme, we consider the security notion of One-Wayness under Chosen Plaintext Attacks (OW-CPA). Note that the security game is of a search type (the adversary should recover a plaintext), which will be convenient for two reasons. First, OW-CPA security of our encryption scheme will be proven under the presumed hardness of the search version of I-PLWE rather than its decision counterpart (recall that we obtain reductions between I-PLWE and PLWE only for the search variant of I-PLWE). Second, in the security proof of our scheme, we will rely on arguments based on the Rényi divergence, which is more amenable to search problems than decision problems.

Note that OW-CPA security is typically defined with respect to the uniform distribution on plaintexts. We consider a variant that handles more general plaintext distributions.

Definition 10 (OW-CPA security). OW-CPA *security of a deterministic public-key encryption scheme* $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *with respect to a family of distributions $\{D_{\mathcal{M}_\lambda}\}_\lambda$ over the plaintext spaces $\{\mathcal{M}_\lambda\}_\lambda$ is defined using the following game between a challenger and a adversary $\mathcal{A}$.*

- *The challenger runs* $\mathsf{KeyGen}(1^\lambda)$ *to obtain a public key* pk *and a secret key* sk. *It sends* pk *to* $\mathcal{A}$.
- *The challenger samples* M *from* $D_{\mathcal{M}_\lambda}$ *and sends* $C = \mathsf{Enc}(\mathsf{pk}, M)$ *to* $\mathcal{A}$.
- *Given* pk *and* C, *the adversary* $\mathcal{A}$ *replies with a plaintext* M'. *It wins the game if* $M' = M$.

The advantage $\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},D_{\mathcal{M}_\lambda}}(\mathcal{A})$ *of the adversary* $\mathcal{A}$ *is defined as the probability that* $\mathcal{A}$ *wins the game.*

As seen in [HHK17] (see also [BP18]), a OW-CPA-secure deterministic encryption scheme can be tightly converted into a Key Encapsulation Mechanism that is secure under Chosen Ciphertext Attacks (CCA-secure KEM), in the Random Oracle Model (ROM). The advantage loss in this conversion is an additive term $q_D \cdot 2^{-H_\infty(D_{\mathcal{M}_\lambda})}$, where q_D is the number of decryption queries made to the KEM, and $H_\infty(D_{\mathcal{M}_\lambda}) = -\log \max_M D_{\mathcal{M}_\lambda}[M]$ is the min-entropy of $D_{\mathcal{M}_\lambda}$. Note that [HHK17, Theorem 3.6] involves a term $q_D/|\mathcal{M}_\lambda|$, as it considers the uniform distribution on plaintexts, but the proof can be readily adapted to non-uniform plaintext distributions, leading to the adapted advantage loss.

In the Quantum Random Oracle Model (QROM), in which the adversary has a quantum access to the random oracle, a deterministic OW-CPA secure encryption scheme can also be converted into a CCA-secure KEM, but the currently known proofs are not tight (see, e.g., [HHK17,BHH+19,KSS+20]), unless one requires additional properties on the deterministic encryption scheme [SXY18]. For our scheme, we do not know how to ensure the disjoint simulatability property required of [SXY18] under standard assumptions.

3 Relations Between Computations over the Polynomial and Integer Rings

In order to relate the PLWE and I-PLWE problems, we first compare the rings over which they are defined: PLWE takes place over some polynomial ring $\mathbb{Z}_q[x]/(f)$ whereas I-PLWE takes place over some integer ring $\mathbb{Z}_{f(q)}$. We first show how operations over $\mathbb{Z}$ can be converted to operations in $\mathbb{Z}_q[x]$, and then how to adapt this conversion to the rings $\mathbb{Z}_q[x]/f$ and $\mathbb{Z}_{f(q)}$.

3.1 Computations over $\mathbb{Z}_q[x]$

A natural way to convert an integer to an element of $\mathbb{Z}_q[x]$ would be to write the q-ary decomposition of an element of $\mathbb{Z}$ to get a polynomial. We rather use a centered q-ary decomposition, which is better suited to capture the smallness of the I-PLWE error terms. In this centered q-ary decomposition, the coefficients are taken in $(-q/2, q/2]$ rather than $[0, q)$. In the following, we exclude the case of $q = 2$, as we cannot represent a negative integer as a combination of powers of 2 with coefficients in $(-q/2, q/2] = \{0, 1\}$.

Definition 11 (Centered q-ary decomposition of an integer). *Let $q > 2$ and $a \in \mathbb{Z}$. For all $0 \leq i \leq \lceil \log_q a \rceil$ we recursively define the i-th coefficient of a in the q-ary decomposition as:*

$$a_i := \frac{a - \sum_{j<i} a_j q^j}{q^i} \bmod q,$$

where the mod *operation outputs the representative that belongs to $(-q/2, q/2]$.*

We now define the map Φ_q that converts an integer a into the polynomial whose coefficients are the coefficients of the centered q-ary decomposition of a.

Definition 12 (Conversion from $\mathbb{Z}$ to $\mathbb{Z}_q[x]$). *Let $q > 2$. The map $\Phi_q : \mathbb{Z} \longrightarrow \mathbb{Z}_q[x]$ is defined as follows*

$$\Phi_q : a \longmapsto \sum_{i=0}^{\lceil \log_q a \rceil} a_i x^i.$$

The map $\Phi_q^{-1} : \mathbb{Z}_q[x] \longrightarrow \mathbb{Z}$ is defined as follows

$$\Phi_q^{-1} : P = \sum_i P_i x^i \longmapsto \sum_i \overline{P}_i q^i,$$

where $\overline{P}_i \in \mathbb{Z}$ is the representative of $P_i \in \mathbb{Z}_q$ belonging to $(-q/2, q/2]$.

Note that indeed Φ_q^{-1} is the inverse of Φ_q, and hence both of them are bijections. Moreover, the equality $f(q) = \Phi_q^{-1}(f \bmod q)$ holds for any $f \in \mathbb{Z}[x]$ whose coefficients belong to $(-q/2, q/2)$. This drives us to always require that $q > 2\|f\|_\infty$ in the following. If $\Phi_q(a)$ has every coefficient with representative in $(-q/2, q/2)$ then $\Phi_q(-a) = -\Phi_q(a)$. Importantly, note that even though Φ_q maps a ring to another ring, it is *not* a ring homomorphism: it is not compatible with addition and multiplication. For instance, for $q = 3$, we have $\Phi_q(1+1) = x - 1 \neq -1 = \Phi_q(1) + \Phi_q(1)$ and $\Phi_q(2 \cdot 2) = x + 1 \neq (x-1)^2 = \Phi_q(2) \cdot \Phi_q(2)$.

Below, our goal is to evaluate how far Φ_q is from being a ring homomorphism, by bounding the quantities $\Phi_q(a+b) - (\Phi_q(a) + \Phi_q(b))$ and/or $\Phi_q(a \cdot b) - \Phi_q(a) \cdot \Phi_q(b)$ for $a, b \in \mathbb{Z}$. When adding (resp. multiplying) two integers in $\mathbb{Z}$ via schoolbook addition (resp. multiplication) in base q, the computation of a given digit may interfere with the computation of the next digit, because of carries. Oppositely, when adding (resp. multiplying) two polynomials in $\mathbb{Z}_q[x]$, there are no carries: computations can be done in parallel. Moreover, if we choose an even basis q, computing $-a$ may not be as simple as taking the opposite of each one of its coefficients.

For the next lemma it will be useful to recall how to compute the Euclidean division with 0-centered remainder: let $a \in \mathbb{Z}$ and $q \geq 2$. The "standard" Euclidean division of $a + \lfloor (q-1)/2 \rfloor$ by q can be written as:

$$a + \left\lfloor \frac{q-1}{2} \right\rfloor = r + \left\lfloor \frac{a + \lfloor (q-1)/2 \rfloor}{q} \right\rfloor \cdot q,$$

with $r \in [0, q)$. We thus have:

$$a = r - \left\lfloor \frac{q-1}{2} \right\rfloor + \left\lfloor \frac{a + \lfloor (q-1)/2 \rfloor}{q} \right\rfloor \cdot q,$$

and since $r - \lfloor (q-1)/2 \rfloor \in (-q/2, q/2]$ we have $a \bmod q = r - \lfloor (q-1)/2 \rfloor$.

Definition 13 (Carries). *Let $q > 2$. Define $q' = \lfloor (q-1)/2 \rfloor$. For all $a, b \in \mathbb{Z}$ and $a_i = \frac{a - \sum_{j=0}^{i-1} a_j q^j}{q^i} \bmod q \in (-q/2, q/2]$ defined for $i \leq \lceil \log_q a \rceil$ and $b_i = \frac{b - \sum_{j=0}^{i-1} b_j q^j}{q^i} \bmod q \in (-q/2, q/2]$ defined for $i \leq \lceil \log_q b \rceil$, we recursively define the additive, multiplicative and opposite carries as follows.*

- *Addition carries $\mathbf{c}^{(a)}(a, b) \in \mathbb{Z}^{\lceil \max(\log_q |a|, \log_q |b|) \rceil + 1}$:*

$$\mathbf{c}^{(a)}(a, b) := \left(0 \left\lfloor \frac{a_0 + b_0 + q'}{q} \right\rfloor \ldots \left\lfloor \frac{c^{(a)}(a,b)_{i-1} + a_{i-1} + b_{i-1} + q'}{q} \right\rfloor \ldots\right)^\top.$$

- *Multiplication carries $\mathbf{c}^{(m)}(a, b) \in \mathbb{Z}^{\lceil \log_q |a| \rceil + \lceil \log_q |b| \rceil + 1}$:*

$$\mathbf{c}^{(m)}(a, b) := \left(0 \left\lfloor \frac{a_0 \cdot b_0 + q'}{q} \right\rfloor \ldots \left\lfloor \frac{c^{(m)}(a,b)_{i-1} + \sum_{j+k=i-1} a_j \cdot b_k + q'}{q} \right\rfloor \ldots\right)^\top.$$

- *Opposite carries: If q is odd, then $\mathbf{c}^{(o)}(a) := \mathbf{0}$. Else, define $h : a \mapsto \{1$ if $a = q/2,\ 0$ else$\}$ and*

$$\mathbf{c}^{(o)}(a) := \left(0 \ -h(a_0) \ldots -h(\mathbf{c}^{(o)}(a)_{i-1} + a_{i-1}) \ldots\right)^\top \in \mathbb{Z}^{\lceil \log_q |a| \rceil}.$$

Finally, define the associated carry polynomials $c^{(o)}(a) := \sum_{j=0} c^{(o)}(a)_j x^j$ and $c^{(i)}(a, b) := \sum_{j=0} (c^{(i)}(a, b)_j \bmod q) x^j$ for $i \in \{a, m\}$.

After having defined these carries, we move on to prove that the difference between operations in $\mathbb{Z}$ and $\mathbb{Z}_q[x]$ is the carry polynomial that stems from computations in $\mathbb{Z}$.

Lemma 2. *Let $q > 2$ and $a, b \in \mathbb{Z}$. Then the decomposition of their sum is $\Phi_q(a + b) = \Phi_q(a) + \Phi_q(b) + c^{(a)}(a, b)$. The decomposition of their product is $\Phi_q(a \cdot b) = \Phi_q(a) \cdot \Phi_q(b) + c^{(m)}(a, b)$. Finally the decomposition of the opposite of a is $\Phi_q(-a) = -\Phi_q(a) + c^{(o)}(a)$.*

The proof proceeds by induction. It is postponed to the appendix of the full version, where we only prove it for the addition, as the other two cases are similar. We now bound the magnitudes of the carries. Note that multiplication carries can be much larger than addition carries.

Lemma 3 (Bounds on carries). *Let $q > 2$ and $a, b \in \mathbb{Z}$. Define $q' = \lfloor (q-1)/2 \rfloor$. We have:*

$$\|c^{(a)}(a,b)\|_\infty \leq 1 \quad \textit{and} \quad \|c^{(o)}(a)\|_\infty \leq 1,$$
$$\|c^{(m)}(a,b)\|_\infty \leq \frac{q + q' + \min(\|a\|_\infty \cdot \|b\|_1, \|b\|_\infty \cdot \|a\|_1)}{q-1}.$$

The proof of this lemma is also postponed to the appendix of the full version, and also proceeds by induction.

3.2 Carries of $\mathbb{Z}_{f(q)}$ Operations in $\mathbb{Z}_q[x]/f$

Remember that the problems defined in Sect. 2 take place in a ring, either polynomial $\mathbb{Z}_q[x]/f$ or integer $\mathbb{Z}_{f(q)}$. Our understanding of the carries from $\mathbb{Z}$ in $\mathbb{Z}_q[x]$ from the previous subsection needs to be refined to understand what happens when we convert elements of $\mathbb{Z}_{f(q)}$ into elements of $\mathbb{Z}_q[x]/f$. We move on to study carries of $\mathbb{Z}_{f(q)}$ operations in $\mathbb{Z}_q[x]/f$.

So far, we introduced a conversion Φ_q from $\mathbb{Z}$ to $\mathbb{Z}_q[x]$ (for an arbitrary $q > 2$), and studied its homomorphism defect (concretely, carries of the basic operations over $\mathbb{Z}$). We progressively refine it so that it maps $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$.

Definition 14. *Let $q > 2$ and $f \in \mathbb{Z}[x]$ a monic polynomial. The map $\Phi_q^{(f)} : \mathbb{Z} \to \mathbb{Z}_q[x]/f$ is defined as follows:*

$$\Phi_q^{(f)} : a \mapsto \Phi_q(a) \bmod f.$$

If $\bar{a}$ is an element of $\mathbb{Z}_{f(q)}$, then $\Phi_q^{(f)}(\bar{a})$ is defined as $\Phi_q^{(f)}(a)$ where a is the representative of $\bar{a}$ in $I_{f,q}$, as defined in Definition 6.

Since its input and output sets are not the same size, the map $\Phi_q^{(f)} : \mathbb{Z}_{f(q)} \to \mathbb{Z}_q[x]/f$ cannot be a bijection. The following lemma shows that depending on the value of $f(q)$ compared to q^m, the map $\Phi_q^{(f)}$ or the evaluation map in q is surjective. Note that the choice of $I_{f,q}$, which may look somewhat arbitrary for q even and $f(q) \approx q^m$, is justified to guarantee this lemma.

Lemma 4. *Let $q > 2$ and $f \in \mathbb{Z}[x]$ be a monic polynomial whose coefficients belong to $(-q/2, q/2)$. Then:*

- *If $f(q) \geq q^m$, for all $P \in \mathbb{Z}_q[x]/f$, we have $\Phi_q^{(f)}(P(q) \bmod f(q)) = P$, i.e., the map $\Phi_q^{(f)}$ is surjective from $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$ and the map $P \mapsto P(q) \bmod f(q)$ is injective from $\mathbb{Z}_q[x]/f$ to $\mathbb{Z}_{f(q)}$.*
- *If $f(q) < q^m$, for all $a \in I_{f,q}$, we have $(\Phi_q^{(f)}(a))(q) = a \bmod f(q)$, i.e., the map $\Phi_q^{(f)}$ is injective from $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$ and the map $P \mapsto P(q) \bmod f(q)$ is surjective from $\mathbb{Z}_q[x]/f$ to $\mathbb{Z}_{f(q)}$.*

We exclude $q/2$ from the set of possible values of the coefficients of f, as it creates technical complications (with potential carries) and in our reductions we will impose that q is significantly larger than $2\|f\|_\infty$.

Proof. The first property is satisfied if $P(q) \bmod f(q) = P(q)$ for any polynomial $P \in \mathbb{Z}_q[x]/f$. This is equivalent to $\Phi_q^{-1}(\mathbb{Z}_q[x]/f) \subseteq I_{f,q}$. The second property is satisfied if $\Phi_q^{(f)}(a) = \Phi_q(a)$ for any $a \in \mathbb{Z}_{f(q)}$. This one is equivalent to $I_{f,q} \subseteq \Phi_q^{-1}(\mathbb{Z}_q[x]/f)$.

In the case where q is odd, we have $\Phi_q^{-1}(\mathbb{Z}_q[x]/f) = [-\frac{q^m-1}{2}, \frac{q^m-1}{2}]$ and $I_{f,q} = (-\frac{f(q)}{2}, \frac{f(q)}{2}]$. The claimed inclusions can be checked by direct computations.

Assume now that q is even. Then:

$$\Phi_q^{-1}(\mathbb{Z}_q[x]/f) = \mathbb{Z} \cap \frac{q^m-1}{q-1} \cdot \big(-\frac{q}{2}, \frac{q}{2}\big] = \left[-\frac{q-2}{2} \cdot \frac{q^m-1}{q-1}, \frac{q}{2} \cdot \frac{q^m-1}{q-1}\right]$$

is not zero-centered.

In the case $f(q) \geq q^m$, it is possible that $\frac{q}{2} \cdot \frac{q^m-1}{q-1} > \frac{f(q)}{2}$: if that is true, we choose $\frac{q}{2} \cdot \frac{q^m-1}{q-1}$ as the right side of the representative interval $I_{f,q}$. In that case, the left side of $I_{f,q}$ is (using $f(q) \geq q^m - 1$):

$$\frac{q}{2} \cdot \frac{q^m-1}{q-1} - f(q) \leq \frac{q}{2} \cdot \frac{q^m-1}{q-1} - (q^m - 1) = -\frac{q-2}{2}\frac{q^m-1}{q-1}.$$

We see here that our choice of $I_{f,q}$ leads to $\Phi_q^{-1}(\mathbb{Z}_q[x]/f) \subseteq I_{f,q}$.

In the case $f(q) < q^m$, it is possible that $-\frac{q-2}{2} \cdot \frac{q^m-1}{q-1} > -\frac{f(q)}{2}$: if that is true, we choose $-\frac{q-2}{2} \cdot \frac{q^m-1}{q-1}$ as the left side of the representative interval $I_{f,q}$. In that case, the right side of $I_{f,q}$ is (using $f(q) \leq q^m - 1$):

$$f(q) - \frac{q-2}{2} \cdot \frac{q^m-1}{q-1} \leq (q^m - 1) - \frac{q-2}{2} \cdot \frac{q^m-1}{q-1} = \frac{q}{2}\frac{q^m-1}{q-1}.$$

We see here that our choice of $I_{f,q}$ leads to $I_{f,q} \subseteq \Phi_q^{-1}(\mathbb{Z}_q[x]/f)$. □

Our understanding of the effect of $\Phi_q^{(f)}$ can be even more refined. In the case where $f(q) < q^m$, the next lemma states that each element of $\mathbb{Z}_{f(q)}$ has at most two predecessors by the map $P \mapsto P(q) \bmod f(q)$ from $\mathbb{Z}_q[x]/f$.

Lemma 5 (Surjectivity of the evaluation, when $f(q) < q^m$). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree m such that $f(q) < q^m$ and whose coefficients belong to $(-q/2, q/2)$. Then for any $a \in \mathbb{Z}_{f(q)}$, there exist at most 2 polynomials $P, Q \in \mathbb{Z}_q[x]/f$ such that $P(q) \bmod f(q) = Q(q) \bmod f(q) = a$. When evaluating P in q, the coefficients of P are taken in $(-q/2, q/2]$.*

Proof. We first note the following about f:

$$f(q) \geq q^m - \left\lfloor \frac{q-1}{2} \right\rfloor \frac{q^m-1}{q-1} \geq q^m - \frac{q-1}{2} \cdot \frac{q^m-1}{q-1} > \frac{q^m}{2}.$$

The equality $P(q) \bmod f(q) = Q(q) \bmod f(q)$ holds if and only if there exists some $k \in \mathbb{Z}$ such that $P(q) = Q(q) + kf(q)$. Since $|P(q) - Q(q)| \leq q^m$, we obtain:

$$|k| \leq \frac{q^m}{f(q)}.$$

Using the previous lower bound on $f(q)$, this is < 2. We must hence have $k \in \{-1, 0, 1\}$. Assume that an element $a \in \mathbb{Z}_{f(q)}$ has three predecessors $P, Q, R \in \mathbb{Z}_q[x]/f$ such that $P(q) = Q(q) + \delta_0 f(q)$ and $P(q) = R(q) + \delta_1 f(q)$ with δ_0, δ_1 both nonzero. This implies that $Q(q) - R(q) = (\delta_1 - \delta_0) f(q)$. By the above, we must have $|\delta_0 - \delta_1| \leq 1$, which implies that $Q(q) = R(q)$. Therefore, the element a has at most 2 predecessors. □

In the next lemma, we explore the case $f(q) \geq q^m$ and show that each polynomial has at most three predecessors in $\mathbb{Z}_{f(q)}$ by the map $\Phi_q^{(f)}$.

Lemma 6 (Surjectivity of the map $\Phi_q^{(f)}$, when $f(q) \geq q^m$). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree m such that $f(q) \geq q^m$ and whose coefficients belong to $(-q/2, q/2)$. For any $P \in \mathbb{Z}_q[x]/f$, there exist at most 3 integers $a, b, c \in \mathbb{Z}_{f(q)}$ such that $P = \Phi_q^{(f)}(a) = \Phi_q^{(f)}(b) = \Phi_q^{(f)}(c)$. Remember that when applying $\Phi_q^{(f)}$ on a, the representative of a is taken in $I_{f,q}$.*

Proof. We note that $\Phi_q^{(f)}(a) = \Phi_q^{(f)}(b)$ holds if and only if there exists some $\delta \in \mathbb{Z}$ such that $\Phi_q(a) = \Phi_q(b) + \delta f$. We have $\delta = a_m - b_m$, where $a = \sum_{i \leq m} a_i q^i, b = \sum_{i \leq m} b_i q^i$ with $a_i, b_i \in (-q/2, q/2]$ for all $i < m$ and $a_m, b_m \in \{-1, 0, 1\}$, by our choice of f and $I_{f,q}$. This implies that any $P \in \mathbb{Z}_q[x]/f$ has at most 3 predecessors. □

To study the carries from operations over $\mathbb{Z}$ in the ring of polynomials modulo f, it suffices to see that these carries are the same as in the previous section, but reduced modulo f. This observation helps bounding them, by using the expansion factor and Lemma 3. We now study the carries of operations done modulo $f(q)$ as seen in the ring of polynomials modulo f. To interpret operations from $\mathbb{Z}_{f(q)}$ in $\mathbb{Z}_q[x]/f$, one can first compute in $\mathbb{Z}$, reduce modulo $f(q)$, apply Φ_q and finally reduce modulo f. We define, for $a, b \in I_{f,q}$:

$$c_f^{(a)}(a, b) := \Phi_q^{(f)}(a + b \bmod f(q)) - \Phi_q^{(f)}(a) - \Phi_q^{(f)}(b),$$
$$c_f^{(m)}(a, b) := \left(\Phi_q^{(f)}(a \cdot b \bmod f(q)) - \Phi_q^{(f)}(a) \cdot \Phi_q^{(f)}(b)\right) \bmod f,$$

where assume that the output of the "$\bmod f(q)$" operation is an integer in $I_{f,q}$.

Lemma 7 (Carries of $\mathbb{Z}_{f(q)}$ in $\mathbb{Z}_q[x]/f$). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree m whose coefficients belong to $(-q/2, q/2)$. Let $a, b \in I_{f,q}$. We assume that the output of the "$\bmod f(q)$" operation is an integer in $I_{f,q}$.*

- *Addition carries. We have, for some* $\delta_0, \delta_1 \in \{-1, 0, 1\}$*:*

  $$\Phi_q^{(f)}(a+b \bmod f(q)) = \Phi_q(a)+\Phi_q(b)+c^{(a)}(a,b)+c^{(a)}(a+b, \delta_0 f(q))+(\delta_0+\delta_1)f.$$

  In particular:

  $$c_f^{(a)}(a,b) = c^{(a)}(a,b) + c^{(a)}(a+b, \delta_0 f(q)) + (\delta_0 + \delta_1 + a_m + b_m) \cdot f,$$

  where $a = \sum_{i \leq m} a_i q^i, b = \sum_{i \leq m} b_i q^i$ *with* $a_i, b_i \in (-q/2, q/2]$ *for all* $i < m$ *and* $a_m, b_m \in \{-1, 0, 1\}$.
- *Multiplication carries. We have:*

  $$c_f^{(m)}(a,b) = \left(c^{(m)}(a,b) + c^{(m)}\left(-\delta, f(q)\right) + c^{(a)}\left(a \cdot b, -\delta f(q)\right) \right) \bmod f,$$

  where $\delta = \lfloor (a \cdot b - (a \cdot b \bmod f(q)))/f(q) \rfloor$.

Note that the lemma statement on addition carries is more detailed than for multiplication carries. We use this extra information on addition carries to prove Lemma 8 below. Apart from this, it will be sufficient to note that $c_f^{(a)}(a,b) = (c^{(a)}(a,b) + c^{(a)}(a+b, \delta_0 f(q))) \bmod f$.

Proof. We study addition carries first. As $a, b \in I_{f,q}$ and the "mod $f(q)$" map takes values in $I_{f,q}$, there exists $\delta_0 \in \{-1, 0, 1\}$ such that $a + b \bmod f(q) = a + b + \delta_0 f(q)$. Using Lemma 2, we obtain:

$$\Phi_q(a + b \bmod f(q)) = \Phi_q(a) + \Phi_q(b) + c^{(a)}(a,b) + \delta_0 f + c^{(a)}(a+b, \delta_0 f(q)).$$

Here we used the fact that $\Phi_q(\delta_0 f(q)) = \delta_0 f$, which holds because $\delta_0 \in \{-1, 0, 1\}$ and the coefficients of f belong to $(-q/2, q/2)$, so there are no opposition carries. We now reduce the latter polynomial modulo f:

$$\begin{aligned}
\Phi_q^{(f)}(a + b \bmod f(q)) &= \Phi_q(a) + \Phi_q(b) + c^{(a)}(a,b) + c^{(a)}(a+b, \delta_0 f(q)) \\
&\quad + \delta_0 f - \left\lfloor \frac{\Phi_q(a + b \bmod f(q))}{f} \right\rfloor f \\
&= \Phi_q(a) + \Phi_q(b) + c^{(a)}(a,b) + c^{(a)}(a+b, +\delta_0 f(q)) \\
&\quad + (\delta_0 + \delta_1) f.
\end{aligned}$$

Note that for any $a \in I_{f,q}$, we have $|a| < 3q^m/2$, which implies that $\delta_1 \in \{-1, 0, 1\}$. The second statement on addition carries follows from the same fact that for any $a \in I_{f,q}$, we have $|a| < 3q^m/2$. This implies that $a_m, b_m \in \{-1, 0, 1\}$.

We now consider multiplication carries. By definition of δ, we have $a \cdot b \bmod f(q) = a \cdot b - \delta f(q)$. Using Lemma 2, we obtain:

$$\begin{aligned}
\Phi_q(a \cdot b \bmod f(q)) &= \Phi_q(a \cdot b) + \Phi_q\left(-\delta \cdot f(q)\right) + c^{(a)}(a \cdot b, -\delta f(q)) \\
&= \Phi_q(a) \cdot \Phi_q(b) + c^{(m)}(a,b) + \Phi_q\left(-\delta\right) \cdot f \\
&\quad + c^{(m)}\left(-\delta, f(q)\right) + c^{(a)}\left(a \cdot b, -\delta f(q)\right).
\end{aligned}$$

Finally, by reducing both sides modulo f, we obtain the lemma statement. □

In the following section, we will be confronted to expressions of the form $b + E(q) \bmod f(q)$, where $b \in \mathbb{Z}_{f(q)}$ and $E \in \mathbb{Z}_q[x]/f$, and we will turn them into polynomials by applying $\Phi_q^{(f)}$. From what precedes, we already know that:

$$\begin{aligned}
&\Phi_q^{(f)}(b + E(q) \bmod f(q)) \\
&\quad = \Phi_q^{(f)}(b) + \Phi_q^{(f)}(E(q) \bmod f(q)) + c_f^{(a)}(b, E(q) \bmod f(q)) \\
&\quad = \Phi_q^{(f)}(b) + E + c_f^{(a)}(b, E(q) \bmod f(q)) + c^{(a)}(E(q), \delta f(q)),
\end{aligned}$$

where $\delta = \lfloor [E(q) - \overline{E(q)}]/f(q) \rfloor$ and $\overline{E(q)} = E(q) \bmod f(q)$. During the computations, we will remove the constant term $\Phi_q^{(f)}(b)$, and do separate computations on the carries and on E. We will end up with expressions:

$$E + \ell \cdot c_f^{(a)}(b, E(q) \bmod f(q)) + \ell \cdot c^{(a)}(E(q), \delta f(q)),$$

where $\ell = -1$ or $\ell = 2$ depending on which reduction between PLWE and $\mathsf{I-PLWE}$ we are currently working on. To analyze the reductions, we use the fact that this expression, when seen as a map with input E, is injective.

Lemma 8 (Injectivity of the carries). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree m whose coefficients belong to $(-q/2, q/2)$. Let $b \in I_{f,q}$. We assume that the output of the "$\bmod f(q)$" operation is an integer in $I_{f,q}$. We define, for $\delta_1, \delta_2, \delta_3 \in \{-1, 0, 1\}$:*

$$\begin{aligned}
I_{\delta_1,\delta_2,\delta_3}^{(b)} := \Bigg\{ P \in \mathbb{Z}_q[x]/f : &\left\lfloor \frac{P(q) - \overline{P(q)}}{f(q)} \right\rfloor = \delta_1 \\
&\wedge \left\lfloor \frac{(b + \overline{P(q)}) - (b + \overline{P(q)} \bmod f(q))}{f(q)} \right\rfloor = \delta_2 \\
&\wedge \left\lfloor \frac{\Phi_q(b + P(q) \bmod f(q))}{f} \right\rfloor = \delta_3 \Bigg\},
\end{aligned}$$

where $\overline{P(q)} = (P(q) \bmod f(q)) \in I_{f,q}$. Then the following two statements hold.

1. *We have that:*
$$\mathbb{Z}_q[x]/f = \bigsqcup_{\delta_1,\delta_2,\delta_3 \in \{-1,0,1\}} I_{\delta_1,\delta_2,\delta_3}^{(b)}.$$
2. *For any non-zero $\ell \in \mathbb{Z}$, define $g_\ell : P \mapsto P + \ell \cdot c^{(a)}(\overline{P(q)}, \delta_1(P) \cdot f(q)) + \ell \cdot c_f^{(a)}(b, P(q))$, where the map δ_1 from $\mathbb{Z}_q[x]/f$ to itself is defined as $\delta_1 : P \mapsto \lfloor (P(q) - \overline{P(q)})/f(q) \rfloor$. For any $\delta_1, \delta_2, \delta_3 \in \{-1, 0, 1\}$, the restriction of g_ℓ to $I_{\delta_1,\delta_2,\delta_3}^{(b)}$ is injective over $\mathbb{Z}_q[x]/f$.*

Proof. We have the following partition of $\mathbb{Z}_q[x]/f$:

$$\mathbb{Z}_q[x]/f = \bigsqcup_{\delta_1,\delta_2,\delta_3 \in \mathbb{Z}} I_{\delta_1,\delta_2,\delta_3}^{(b)},$$

and hence it suffices to prove that $I^{(b)}_{\delta_1,\delta_2,\delta_3} = \emptyset$ for $(\delta_1, \delta_2, \delta_3) \notin \{-1, 0, 1\}^3$. We distinguish two cases. In the case where $f(q) < q^m$, since $q^m/2 < f(q) < q^m$, the integer $P(q)$ is reduced at most once modulo $f(q)$, thus $\delta_1 \in \{-1, 0, 1\}$ captures all possibilities for δ_1. In the case where $f(q) \geq q^m$, the integer $P(q)$ cannot be non-trivially reduced modulo $f(q)$, thanks to our choice of $I_{f,q}$. In this case, the set $\{0\}$ captures all possibilities for δ_1. For δ_2 and δ_3, note that they correspond to the δ's defined in the addition carries of Lemma 7.

To prove the second item, let $\delta_1, \delta_2, \delta_3 \in \{-1, 0, 1\}$ and $P, Q \in I^{(b)}_{\delta_1,\delta_2,\delta_3}$ such that $g_\ell(P) = g_\ell(Q)$. Since they are in the same $I^{(b)}_{\delta_1,\delta_2,\delta_3}$, it means that the δ's corresponding to the addition carries between b and $\overline{P(q)}$, and to those between b and $Q(q)$, are identical (these are δ_2 and δ_3). Moreover, it holds by definition that $\delta_1(P) = \delta_1(Q) = \delta_1$. As $g_\ell(P) = g_\ell(Q)$, we have, using Lemma 7:

$$\begin{aligned}\frac{P-Q}{\ell} &= (c_f^{(a)}(b, \overline{Q(q)}) - c_f^{(a)}(b, \overline{P(q)})) + (c^{(a)}(Q(q), \delta_1 f(q)) - c^{(a)}(P(q), \delta_1 f(q))) \\ &= (c^{(a)}(b, \overline{Q(q)}) - c^{(a)}(b, \overline{P(q)}) + c^{(a)}(b + \overline{Q(q)}, \delta_2 f(q)) \\ &\quad - c^{(a)}(b + \overline{P(q)}, \delta_2 f(q))) + (c^{(a)}(Q(q), \delta_1 f(q)) - c^{(a)}(P(q), \delta_1 f(q))).\end{aligned}$$

We will show by induction that the above implies that $P = Q$. Define (H_k) as "$P_n = Q_n$ for all $n \leq k$". Note that (H_0) follows from the definition of $c^{(a)}$. Assume now that (H_k) holds for some $0 \leq k < m$. Recall the definitions of $\overline{P(q)} = P(q) - \delta_1(P) f(q)$ and $\overline{Q(q)} = Q(q) - \delta_1(Q) f(q)$, so $\overline{P(q)}_n = \overline{Q(q)}_n$ holds for all $n \leq k$.

1. As the addition carry at rank $k+1$ only depends on $\overline{P(q)}_n = \overline{Q(q)}_n$ and b_n for $n \leq k$, we have $c^{(a)}(b, \overline{P(q)})_{k+1} = c^{(a)}(b, \overline{Q(q)})_{k+1}$. Similarly, we have $c^{(a)}(P(q), \delta_1 f(q))_{k+1} = c^{(a)}(Q(q), \delta_1 f(q))_{k+1}$.
2. Similarly, we also have $(b + \overline{P(q)})_n = (b + \overline{Q(q)})_n$ for all $n \leq k+1$.
3. For the same reason, we obtain $c^{(a)}(b + \overline{P(q)}, \delta_2 f(q))_{k+1} = c^{(a)}(b + \overline{Q(q)}, \delta_2 f(q))_{k+1}$.

By the above equality on $\frac{P-Q}{\ell}$, we obtain that $P_{k+1} = Q_{k+1}$. This completes the induction, and the proof that $P = Q$. Therefore, the restriction of g_ℓ to $I^{(b)}_{\delta_1,\delta_2,\delta_3}$ is indeed injective. □

4 Reductions Between sPLWE and sI-PLWE

We exhibit reductions between the search variants of the PLWE and I-PLWE problems, as defined in Sect. 2, for a large class of defining polynomials f. As discussed in Sect. 1, our reductions fill some missing gaps in the prior work of Gu [Gu19] for $f = x^m + 1$, and generalize the results to many different defining polynomials f. For each reduction, the study depends on whether the integer set has more elements than the polynomial set or not. The four reductions and their analyses are very similar, yet each of them has its own subtleties. Nonetheless, the following lemma will be used in every case.

Lemma 9 (Carries of an IP sample). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ monic and irreducible of degree m, whose coefficients belong to $(-q/2, q/2)$. Define $C(P,Q) := \Phi_q^{(f)}(Q(q) - P(q)s \bmod f(q)) - (Q - PS \bmod q)$ and $b := -P(q)s \bmod f(q)$, for any $P, Q, S \in \mathbb{Z}_q[x]/f$ and $s := S(q) \bmod f(q)$. Then:*

- $\|C(P,Q)\|_\infty \leq \mathsf{EF}(f) \cdot (6 + \|f\|_1 + 2m\|S\|_\infty)$
- *For fixed $P \in \mathbb{Z}_{f(q)}$ and any $\delta_1, \delta_2, \delta_3 \in \{-1, 0, 1\}$ and $\ell \in \mathbb{Z}_q \backslash 0$, the map $Q \mapsto Q + \ell C(P,Q) - PS$ is injective from $I^{(b)}_{\delta_1,\delta_2,\delta_3}$ to $\mathbb{Z}_q[x]/f$, where $I^{(b)}_{\delta_1,\delta_2,\delta_3}$ is as defined in Lemma 8.*

Note that we will use this lemma only for $\ell = -1$ and $\ell = 2$. Due to space constraints, the proof of this lemma and several results from this section are postponed to the appendix of the full version.

4.1 Reducing sPLWE to sI-PLWE when $f(q) < q^m$

In this subsection, we are given samples from the P distribution and we try to obtain samples from the IP distribution. Since the polynomial set is bigger than the integer one, we can evaluate it for q and get a distribution whose support is $(\mathbb{Z}_{f(q)})^2$. Moreover the next lemma will prove that it is indeed close enough to IP to use an adversary against sI-PLWE to solve sPLWE.

Lemma 10. *Let $q \geq 3$, $m > 0$, $f \in \mathbb{Z}_q[x]$ be a monic polynomial of degree m such that $f(q) < q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > 0$. Let $S \in \mathbb{Z}_q[x]/f$ and $s \in \mathbb{Z}_{f(q)}$ such that $S(q) = s \bmod f(q)$. Given a sample $(A,B) \hookleftarrow \mathsf{P}^{(f)}_{q,\sigma}(S)$, set $(a,b) := (A(q) \bmod f(q), B(q) \bmod f(q))$. Then:*

$$R_{\mathsf{IP}\ \text{to}\ \mathsf{P}} := R(\mathsf{IP}^{(f)}_{q,\sigma}(s)||(a,b)) \leq 216 \exp\left(38\, m^3 \frac{\mathsf{EF}(f)^2(\|f\|_\infty + \|S\|_\infty)^2}{\sigma^2}\right).$$

Proof. We start by proving that the divergence is well defined. Recall that the support of $\mathsf{IP}^{(f)}_{q,\sigma}(s)$ is $\mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}$. Since $\Phi_q^{-1}(I_{f,q}) \subseteq \mathbb{Z}_q[x]/f$, the divergence is well-defined as the support of (a,b) is exactly $(\mathbb{Z}_{f(q)})^2$.

We move on to bounding the divergence:

$$\begin{aligned} R_{\mathsf{IP}\ \text{to}\ \mathsf{P}} &= \sum_{(i,j)\in(\mathbb{Z}_{f(q)})^2} \frac{\Pr_{a'\hookleftarrow\mathbb{Z}_{f(q)}, e'\hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma,q}}(a' = i \wedge a's + e' \bmod f(q) = j)^2}{\Pr_{a,b}(a = i \wedge b = j)} \\ &\leq \sum_{(i,j)\in(\mathbb{Z}_{f(q)})^2} \frac{q^m}{f(q)^2} \cdot \frac{D_{\mathbb{Z}_{f(q)},\sigma,q}(\Phi_q(j - is \bmod f(q)))^2}{\sum\limits_{\substack{A\in\mathbb{Z}_q[x]/f \\ A(q)=i \bmod f(q)}} \Pr\limits_{e\hookleftarrow D_{\mathbb{Z}[x]/f,\sigma,q}}((AS + e \bmod f)(q) = j \bmod f(q))}, \end{aligned}$$

where we condition on the values of a' and A. Since $\Phi_q^{(f)}(i)(q) = i \bmod f(q)$, we bound from below the sum at the denominator by keeping only the term $A = \Phi_q^{(f)}(i)$. Moreover, we notice that $j = \Phi_q^{(f)}(j)(q) = [\Phi_q^{(f)}(i)S + \Phi_q^{(f)}(j) -$

$\Phi_q^{(f)}(i)S](q)$, which implies that the denominator is at least $D_{\mathbb{Z}[x]/f,\sigma,q}(\Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S)$. We therefore obtain the bound:

$$R_{\mathsf{IP\ to\ P}} \leq \sum_{(i,j)\in(\mathbb{Z}_{f(q)})^2} \frac{q^m}{f(q)^2} \frac{D_{\mathbb{Z}_{f(q)},\sigma,q}(j - is \bmod f(q))^2}{D_{\mathbb{Z}[x]/f,\sigma,q}(\Phi_q^{(f)}(j) - \Phi_q^{(f)}(j)S)}.$$

To bound the Gaussian ratio, we can split the work into bounding two ratios:

- The first one is a ratio of Gaussian functions and can be thus expressed as a difference $\exp(-\pi(2\|\Phi_q^{(f)}(j - is \bmod f(q))\|^2 - \|(\Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S)\|^2)/\sigma^2)$.
- The second one is the ratio of normalization constants of the Gaussian distributions $\rho_\sigma(\mathbb{Z}_q[x]/f)/\rho_\sigma(\mathbb{Z}_{f(q)})$.

First, let $C(i,j) := \Phi_q^{(f)}(j - is \bmod f(q)) - \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S \in \mathbb{Z}_q[x]/f$. Recall the identity $2\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}\|^2 = \|\mathbf{x}+2\mathbf{y}\|^2 - 2\|\mathbf{y}\|^2$. In our case, we instantiate this with $\mathbf{x} = \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S$ and $\mathbf{y} = C(i,j)$. We now have to study $\|C(i,j)\|_\infty$ and the map $j \mapsto \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S + 2C(i,j)$.

If we let $P = \Phi_q^{(f)}(i)$ and $Q = \Phi_q^{(f)}(j)$, we notice that $C(i,j)$ corresponds to the $C(P,Q)$ defined in the Lemma 9. Recalling here the results from its analysis, we know that $\|C(i,j)\|_\infty \leq \mathsf{EF}(f)(6 + \|f\|_1 + 2m\|S\|_\infty)$ and that the map $j \mapsto \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S + 2C(i,j)$ is injective from each of the 27 intervals defined in Lemma 8 to $\mathbb{Z}_q[x]/f$, where we moreover recall that $\Phi_q^{(f)}$ is injective from $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$ in the case $f(q) < q^m$. It is then possible to reindex each of the 27 summation terms, to get:

$$\begin{aligned}\sum_{(i,j)\in(\mathbb{Z}_{f(q)})^2} \exp(-\pi\|\Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S + 2C(i,j)\|^2/\sigma^2) &\leq 27 \cdot \sum_{i\in\mathbb{Z}_{f(q)}} \rho_\sigma(\mathbb{Z}_q[x]/f) \\ &\leq 27 \cdot f(q) \cdot \rho_\sigma(\mathbb{Z}_q[x]/f).\end{aligned}$$

Recalling that $q^m < 2f(q)$, we then get the bound:

$$R_{\mathsf{IP\ to\ P}} \leq 54 \cdot \frac{\rho_\sigma(\mathbb{Z}_q[x]/f)^2}{\rho_\sigma(\mathbb{Z}_{f(q)})^2} \cdot \exp\left(2\pi m \frac{\mathsf{EF}(f)^2(6 + \|f\|_1 + 2m\|S\|_\infty)^2}{\sigma^2}\right).$$

We now move on to bounding the ratio $\rho_\sigma(\mathbb{Z}_q[x]/f)/\rho_\sigma(\mathbb{Z}_{f(q)})$. We write:

$$\begin{aligned}\frac{\rho_\sigma(\mathbb{Z}_q[x]/f)}{\rho_\sigma(\mathbb{Z}_{f(q)})} &= \frac{\sum_{Q\in\mathbb{Z}_q[x]/f} \exp(-\pi\|Q\|^2/\sigma^2)}{\sum_{P\in\Phi_q^{(f)}(\mathbb{Z}_{f(q)})} \exp(-\pi\|P\|^2/\sigma^2)} \\ &= 1 + \frac{\sum_{Q\in\mathbb{Z}_q[x]/f\setminus\Phi_q^{(f)}(\mathbb{Z}_{f(q)})} \exp(-\pi\|Q\|^2/\sigma^2)}{\sum_{P\in\Phi_q^{(f)}(\mathbb{Z}_{f(q)})} \exp(-\pi\|P\|^2/\sigma^2)}.\end{aligned}$$

First, notice that the Φ_q map preserves ordering, if the ordering considered for polynomials is the lexicographical ordering: $m < n$ if and only if $\Phi_q(m) < \Phi_q(n)$.

Let $P \in \mathbb{Z}_q[x]/f \setminus \Phi_q^{(f)}(\mathbb{Z}_{f(q)})$. Assume that its leading coefficient is positive, up to replacing P with $-P$. Then, since it holds that $f(q) > \sum_{i=0}^{m-1} \lfloor q/2 \rfloor q^i$ and $P(q) \geq f(q)/2$, the leading coefficient of P is at least $q' := \lceil \lfloor q/2 \rfloor / 2 \rceil$. This proves that $P - q'x^{m-1} \in \Phi_q^{(f)}(\mathbb{Z}_{f(q)})$ as either its degree is now strictly smaller than $m-1$ or its leading coefficient is strictly smaller than q', since $2q' > q/2$. Moreover, $P - q'x^{m-1} > 0$. The same kind of reasoning can be held for P with negative leading coefficient, to map it to an element of $\Phi_q^{(f)}(\mathbb{Z}_{f(q)})$ with negative leading coefficient. Both maps are injective as they are translations. Their image sets do not overlap and the image of any element has smaller norm than said element. By combining these two maps, this proves that there exists an injective map $g : \mathbb{Z}_q[x]/f \setminus \Phi_q^{(f)}(\mathbb{Z}_{f(q)}) \to \Phi_q^{(f)}(\mathbb{Z}_{f(q)})$ such that $\|g(P)\| \leq \|P\|$ holds for any $P \in \mathbb{Z}_q[x]/f \setminus \Phi_q^{(f)}(\mathbb{Z}_{f(q)})$. This proves that

$$\sum_{Q \in \mathbb{Z}_q[x]/f \setminus \Phi_q^{(f)}(\mathbb{Z}_{f(q)})} \exp\Big(-\pi \frac{\|Q\|^2}{\sigma^2}\Big) \leq \sum_{P \in \Phi_q^{(f)}(\mathbb{Z}_{f(q)})} \exp\Big(-\pi \frac{\|P\|^2}{\sigma^2}\Big),$$

and hence that the ratio is ≤ 2. The total multiplicative constant is then 216. □

The result below follows from the Rényi divergence probability preservation.

Theorem 1. *Let $q > 2$ and $f \in \mathbb{Z}[x]$ irreducible and monic of degree $m > 0$ such that $f(q) < q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > \sigma' > 0$ such that $q > \sqrt{m}\sigma$. Let t be a number of samples, such that:*

$$\exp\Big(6t + 38tm^3 \frac{\mathsf{EF}(f)^2(\|f\|_\infty + m^{1/2}\sigma')^2}{\sigma^2}\Big) = \mathsf{poly}(m).$$

Then $\mathsf{sPLWE}^{(f)}_{q,\sigma,\sigma',t}$ *reduces to* $\mathsf{sl\text{-}PLWE}^{(f)}_{q,\sigma,\sigma',t}$.

We refer to the discussion just after Theorem 2 for how to set parameters so that the theorem conditions are fulfilled.

Proof. Assume that there exists an adversary $\mathcal{A}$ with success probability ε_0 against the $\mathsf{sl\text{-}PLWE}^{(f)}_{q,\sigma,\sigma',t}$ game. We introduce a sequence of games to prove the theorem:

Game 0**:** This is the genuine $\mathsf{sl\text{-}PLWE}^{(f)}_{q,\sigma,\sigma',t}$ game.

Game 1**:** In this game, we change the distribution of the secret. We now sample $s \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}}$. Recall that the statistical distance between $D_{\mathbb{Z}_{f(q)},\sigma',q}$ and $D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}}$ is $2^{-\Omega(m)}$, since $q > \sqrt{m}\sigma'$.

Game 2**:** In this game we change the distribution of samples. They are now sampled according to the process introduced in Lemma 10, where the polynomial secret S is sampled according to $D_{\mathbb{Z}[x]/f,\sigma',\sqrt{m}\sigma'}$ and $s := S(q) \bmod f(q)$.

Game 3**:** In this game, we change the distribution of the secret S: it is now sampled according to $D_{\mathbb{Z}[x]/f,\sigma',q}$. The statistical distance between the distribution of the polynomial secret in this game and the previous one is $2^{-\Omega(m)}$.

Call ε_i the success probability of $\mathcal{A}$ in Game i. From the remarks on statistical distance, it already holds that $|\varepsilon_0 - \varepsilon_1| < 2^{-\Omega(m)}$ and $|\varepsilon_2 - \varepsilon_3| < 2^{-\Omega(m)}$. In the context of Game 1 versus Game 2, by using the probability preservation and multiplicativity of the Rényi divergence, it holds that

$$\varepsilon_2 \geq \frac{\varepsilon_1^2}{R_\infty(D_1||D_2) \cdot \max\limits_{S:\|S\|_\infty \leq \sqrt{m}\sigma'} R^t_{\mathsf{P\ to\ IP}}},$$

where D_1 and D_2 denote the distributions of the secret s in Games 1 and 2, respectively. Note that in D_2, for a given integer secret s, there are at most two polynomial secrets S_i such that $s = S_i(q) \bmod f(q)$. We can bound from below the probability by keeping only $S := \Phi_q^{(f)}(s) \in \mathbb{Z}_q[x]/f$. We compute the divergence.

$$\begin{aligned} R_\infty(D_1||D_2) &\leq \max_{s \in \mathrm{Supp}(D_1)} \frac{D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}}(s)}{D_{\mathbb{Z}[x]/f,\sigma',\sigma'\sqrt{m}}(\Phi_q^{(f)}(s))} \\ &\leq \frac{\rho_{\sigma'}(\mathbb{Z}^{<m}_{\sigma'\sqrt{m}}[x])}{\rho_{\sigma'}(\Phi_q(\mathrm{Supp}(D_1)))} \max_{s \in \mathrm{Supp}(D_1)} \frac{\exp(-\pi\|\Phi_q(s)\|^2)/\sigma'^2}{\exp(-\pi\|\Phi_q^{(f)}(s)\|^2)/\sigma'^2}. \end{aligned}$$

Since s is in $I_{f,q}$, we have $\Phi_q^{(f)}(s) = \Phi_q(s)$ and the rightmost ratio is always 1. Recall the existence of the g injective map from Lemma 10. This maps every element of $\mathbb{Z}^{<m}_{\sigma'\sqrt{m}}[x]$ that is not in $\Phi_q(\mathrm{Supp}(D_1))$ to an element in $\Phi_q(\mathrm{Supp}(D_1))$, which has smaller norm. This implies that $R_\infty(D_1||D_2) \leq 2$, by partitioning. This shows with our choice of parameters that the success probability loss is at most polynomial in m when switching from Game 1 to Game 2.

Finally we build an adversary $\mathcal{B}$ against the $\mathsf{sPLWE}^{(f)}_{q,\sigma,\sigma',t}$ game. It suffices to notice that $\mathcal{B}$ can exactly simulate $\mathcal{A}$'s view in Game 3. Moreover, if $\mathcal{A}$ wins, then its output s is such that $s = S(q) \bmod f(q)$, where S is the secret that $\mathcal{B}$ has to guess. Then $\mathcal{B}$ outputs S uniformly among the predecessors of s by the evaluation map $P \mapsto P(q) \bmod f(q)$. Since this set is comprised of at most two integers, the probability that $\mathcal{B}$ wins is $\geq \varepsilon_3/2$. □

4.2 Reducing sPLWE to sI-PLWE when $f(q) \geq q^m$

In this subsection we are given polynomial samples from a ring that is smaller than the target integer ring. To compensate, we will not simply evaluate our samples for q but instead choose uniformly an integer pair among the predecessors of the sample by the map $\Phi_q(f)$. The following lemma proves that the resulting distribution is close to IP.

Lemma 11. *Let $q > 2$, $f \in \mathbb{Z}[x]$ monic and irreducible of degree m such that $f(q) \geq q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > 0$, $S \in \mathbb{Z}_q[x]/f$*

and $s \in \mathbb{Z}_{f(q)}$ *such that* $S = \Phi_q^{(f)}(s)$. *Let* $(A, B) \hookleftarrow \mathsf{P}_{q,\sigma}^{(f)}(S)$. *Choose* (a, b) *uniformly randomly in* $\{(i, j) \in \mathbb{Z}_{f(q)} | \Phi_q^{(f)}(i, j) = (A, B)\}$. *Then:*

$$R_{\mathsf{IP\ to\ P}} := R(\mathsf{IP}_{q,\sigma}^{(f(q))}(s)||(a, b)) \leq 243 \exp\left(114 \frac{m^3 \mathsf{EF}(f)^2 (\|f\|_\infty + \|S\|_\infty)^2}{\sigma^2}\right).$$

Proof. We start by proving that the divergence is well-defined. We already know that $\Phi_q^{(f)}$ is surjective from $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$ in the case where $f(q) \geq q^m$. Since the support of (A, B) is $(\mathbb{Z}_q[x]/f)^2$, this implies that the support of (a, b) is $(\mathbb{Z}_{f(q)})^2$. We can now start bounding it:

$$\begin{aligned} R_{\mathsf{IP\ to\ P}} &= \sum_{(i,j) \in (\mathbb{Z}_{f(q)})^2} \frac{\Pr_{a' \hookleftarrow \mathbb{Z}_{f(q)}, e \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma,q}}(a' = i \wedge a's + e = j)^2}{\Pr_{(a,b)}(a = i \wedge b = j)} \\ &\leq \sum_{(i,j) \in (\mathbb{Z}_{f(q)})^2} \frac{\left(\frac{1}{f(q)} D_{\mathbb{Z}_{f(q)},\sigma,q}(j - is \bmod f(q))\right)^2}{\frac{1}{q^m} \cdot \Pr_{(A,B)}(\Phi_q^{(f)}(j) = B | \Phi_q^{(f)}(i) = A) \cdot \Pr_b(b = j | B = \Phi_q^{(f)}(j))}, \end{aligned}$$

using the chain rule. We moreover know the following facts for the denominator:

- we already used that $\Pr_{A \hookleftarrow \mathbb{Z}_q[x]/f}(\Phi_q^{(f)}(i) = A) = 1/q^m$.
- For $E = \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S \bmod f$, it holds that $\Phi_q^{(f)}(j) = AS + E$, under the hypothesis that $\Phi_q^{(f)}(i) = A$. Thus it holds that:

$$\Pr_{(A,B)}(\Phi_q^{(f)}(j) = B | \Phi_q^{(f)}(i) = A) \geq \Pr_{E \hookleftarrow D_{\mathbb{Z}[x]/f,\sigma,q}}(\Phi_q^{(f)}(i)S + E = \Phi_q^{(f)}(j)).$$

- Since any polynomial in $\mathbb{Z}_q[x]/f$ has at most 3 predecessors in $\mathbb{Z}_{f(q)}$ by $\Phi_q^{(f)}$, it holds that the probability $\Pr_{(a,b)}(b = j | \Phi_q^{(f)}(b) = \Phi_q^{(f)}(j))$ is at least $1/3$.

The above three statements give:

$$R_{\mathsf{IP\ to\ P}} \leq \sum_{(i,j) \in (\mathbb{Z}_{f(q)})^2} \frac{3q^m}{f(q)^2} \cdot \frac{D_{\mathbb{Z}_{f(q)},\sigma,q}(j - is \bmod f(q))^2}{D_{\mathbb{Z}[x]/f,\sigma,q}(\Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S)}.$$

Recall that in the case $f(q) \geq q^m$, $\mathbb{Z}_q[x]/f \subseteq \Phi_q(I_{f,q})$. This immediately shows $\rho_\sigma(\mathbb{Z}_q[x]/f) \leq \rho_\sigma(\Phi_q(I_{f,q}))$. We then have:

$$R_{\mathsf{IP\ to\ P}} \leq \frac{3q^m}{\rho_\sigma(\Phi_q(\mathbb{Z}_{f(q)}))f(q)^2} \cdot \sum_{(i,j) \in (\mathbb{Z}_{f(q)})^2} \frac{\exp(-2\pi \|\Phi_q(j - is \bmod f(q))\|^2/\sigma^2)}{\exp(-\pi \|\Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S\|^2/\sigma^2)}.$$

Define $C(i, j) := \Phi_q^{(f)}(j - is \bmod f(q)) - \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S \bmod f$, as we previously did. The mod$f$ may not be trivial and we know that there exists some $\delta \in \{-1, 0, 1\}$ such that $\Phi_q(j - is \bmod f(q)) = \Phi_q^{(f)}(j - is \bmod f(q)) + \delta f$.

Instead of guessing for each pair (i,j) which δ is the right one, we simply bound the divergence by a sum over each of the three possible values for δ:

$$R_{\mathsf{IP\ to\ P}} \leq \frac{3q^m}{f(q)^2} \cdot \sum_{\substack{\delta\in\{-1,0,1\} \\ (i,j)\in(\mathbb{Z}_{f(q)})^2}} \frac{\exp(-2\pi\|(\Phi_q^{(f)}(j)-\Phi_q^{(f)}(i)S \bmod f)+C(i,j)+\delta f\|^2/\sigma^2)}{\rho_\sigma(\Phi_q(\mathbb{Z}_{f(q)}))\exp(-\pi\|\Phi_q^{(f)}(j)-\Phi_q^{(f)}(i)S \bmod f\|^2/\sigma^2)}.$$

We know that $P(i,j) := \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S \bmod f$ and $C(i,j)$ have degree $\leq m$. Recall the identity $2\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}\|^2 = \|\mathbf{x}+2\mathbf{y}\|^2 - 2\|\mathbf{y}\|^2$. In our case, we instantiate this with $\mathbf{x} = \Phi_q^{(f)}(j) - \Phi_q^{(f)}(i)S$ and $\mathbf{y} = C(i,j)$. To bound the last norm, we recall that the analysis of $C(P,Q)$ done in Lemma 9, applies here by setting $P = \Phi_q^{(f)}(i)$ and $Q = \Phi_q^{(f)}(j)$. Then we have:

$$\|C(i,j)+\delta f\|^2 \leq 1 + m\mathsf{EF}(f)^2(6+\|f\|_1+2m\|S\|_\infty)^2 + m\|f\|_\infty^2.$$

Let us fix $i \in \mathbb{Z}_{f(q)}$. We study $j \mapsto P(i,j)+2C(i,j)$. As proved in Lemma 9, this is injective over each of $(\Phi_q^{(f)})^{-1}(I_{\delta_1,\delta_2,\delta_3}^{(-is)})$ where $I_{\delta_1,\delta_2,\delta_3}^{(-is)}$ are the intervals introduced in Lemma 8. Since $f(q) \geq q^m$, $I_{\delta_1,\delta_2,\delta_3}^{(-is)}$ is empty if $i \neq 0$. We have:

$$\|P(i,j)+2C(i,j)+\delta f\|^2 = \delta^2 + \|P(i,j)+2C(i,j)+2\delta(f-x^m)\|^2,$$

and note how $\exp(-\pi\delta^2/\sigma^2) \leq 1$ and $f(q) \geq q^m$. Our global bound becomes:

$$R_{\mathsf{IP\ to\ P}} \leq 27\exp\left(2\pi\frac{3m\mathsf{EF}(f)^2(6+m\|f\|_\infty+2m\|S\|_\infty)^2}{\sigma^2}\right) \cdot \sum_{\substack{\delta\in\{-1,0,1\} \\ j\in\mathbb{Z}_{f(q)}}} \frac{\exp(-\pi\|\Phi_q^{(f)}(j)+\delta(f-x^m)\|^2/\sigma^2)}{\rho_\sigma(\mathbb{Z}_{f(q)})}.$$

Moreover, we know that every $P \in \mathbb{Z}_q[x]/f$ has at most 3 predecessors by $\Phi_q^{(f)}$ from $\mathbb{Z}_{f(q)}$. We can thus replace the sum over $j \in \mathbb{Z}_{f(q)}$ by 3 times a sum over $P \in \mathbb{Z}_q[x]/f$. Since $P \mapsto P+\delta(f-x^m)$ is a bijection of $\mathbb{Z}_q[x]/f$, we get:

$$R_{\mathsf{IP\ to\ P}} \leq 243\exp\left(6\pi\frac{m\mathsf{EF}(f)^2(6+m\|f\|_\infty+2m\|S\|_\infty)^2}{\sigma^2}\right)\frac{\rho_\sigma(\mathbb{Z}_q[x]/f)}{\rho_\sigma(\mathbb{Z}_{f(q)})}.$$

To conclude, we recall $\rho_\sigma(\mathbb{Z}_q[x]/f) \leq \rho_\sigma(\mathbb{Z}_{f(q)})$ since $\mathbb{Z}_q[x]/f \subseteq \Phi_q(\mathbb{Z}_{f(q)})$. □

The below result follows from the Rényi divergence probability preservation.

Theorem 2. *Let $q > 2$ and $f \in \mathbb{Z}[x]$ irreducible and monic of degree $m > 0$ such that $f(q) \geq q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > \sigma' > 0$ such that $q > \sqrt{m}\sigma$. Let t be a number of samples, such that:*

$$\exp\left(\frac{7\,m\|f\|_\infty^2}{\sigma'^2} + 114t\left(1+\frac{m^3\mathsf{EF}(f)^2(\|f\|_\infty+m^{1/2}\sigma')^2}{\sigma^2}\right)\right) = \mathsf{poly}(m).$$

Then $\mathsf{sPLWE}_{q,\sigma,\sigma',t}^{(f)}$ reduces to $\mathsf{sI\text{-}PLWE}_{q,\sigma,\sigma',t}^{(f)}$.

Along with Theorem 1, this provides a concrete way to find a range of parameters for which sPLWE reduces to sl-PLWE. One should start by choosing an irreducible monic polynomial f of degree $m > 0$. Note that f already determines which theorem will be used: if the second highest nonzero coefficient of f is negative (resp. positive), it holds that $f(q) < q^m$ (resp. $f(q) \geq q^m$) for any integer $q \geq 2\|f\|_\infty$. The value of $t = O(\log m)$ can then be fixed depending on the needs. In Sect. 5, we will have $t = 2$.

The next step is to choose the noise parameter $\sigma' > 0$. When $f(q) \leq q^m$, it can be chosen freely, whereas in the case where $f(q) \geq q^m$, it must satisfy $\sigma' = \Omega(\|f\|_\infty \sqrt{m/\log(m)})$. Then the other noise parameter $\sigma > 0$ should be chosen such that $\sigma^2 \geq \Omega(tm^3\mathsf{EF}(f)^2(\|f\|_\infty + m^{1/2}\sigma')^2/\log(m))$. Last is to choose an integer $q > \max(2\|f\|_\infty, \sqrt{m}\sigma)$. In Sect. 5, further conditions are discussed as they are needed for the encryption application.

4.3 Reducing sl-PLWE to sPLWE when $f(q) < q^m$

When reducing sl-PLWE to sPLWE, we are given samples from the IP distribution, and we want to obtain samples from the P distribution. Here, the integer set is smaller than the polynomial one, so the mapping cannot be deterministic if we want to cover the whole range. For this purpose, we uniformly choose polynomials that are predecessors of our samples by the evaluation $P \mapsto P(q) \bmod f(q)$.

Lemma 12 (Divergence between P and IP, when $f(q) < q^m$). *Let $q > 2$ and $f \in \mathbb{Z}[x]$ monic and irreducible of degree $m > 0$ such that $f(q) < q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > 0$. Let $S \in \mathbb{Z}[x]/f$ and $s = S(q) \bmod f(q) \in I_{f,q}$. Sample $(a, b) \hookleftarrow \mathsf{IP}^{(f)}_{q,\sigma}(s)$ and choose A (resp. B) uniformly in the set of predecessors of a $\{P \in \mathbb{Z}_q[x]/f : P(q) \bmod f(q) = a\}$ (resp. the set of predecessors of b $\{P \in \mathbb{Z}_q[x]/f : P(q) \bmod f(q) = b\}$) via the evaluation map. Then:*

$$R_{\mathsf{P\ to\ IP}} := R(\mathsf{P}^{(f)}_{q,\sigma}(S)||(A, B)) \leq 108 \exp\left(38 \cdot m^3 \mathsf{EF}(f)^2 \frac{(\|f\|_\infty + \|S\|_\infty)^2}{\sigma^2}\right).$$

The below result follows from the Rényi divergence probability preservation.

Theorem 3. *Let $q > 2$ and $f \in \mathbb{Z}[x]$ irreducible and monic of degree $m > 0$ such that $f(q) < q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > \sigma' > 0$ such that $q > \sqrt{m}\sigma$. Let t be a number of samples, such that:*

$$\exp\left(\frac{7\,m\|f\|_\infty^2}{\sigma'^2} + 76t\left(1 + m^3\mathsf{EF}(f)^2 \frac{(\|f\|_\infty + m^{1/2}\sigma')^2}{\sigma^2}\right)\right) \leq \mathsf{poly}(m).$$

Then $\mathsf{sl\text{-}PLWE}^{(f)}_{q,\sigma,\sigma',t}$ reduces to $\mathsf{PLWE}^{(f)}_{q,\sigma,\sigma',t}$.

4.4 Reducing sl-PLWE to sPLWE Reduction when $f(q) \geq q^m$

In this subsection, the integer set is bigger than the polynomial set. Simply applying $\Phi^{(f)}_q$ on the samples that we get is thus enough to get a distribution

that covers the entirety of $(\mathbb{Z}_q[x]/f)^2$. Moreover, the next lemma proves that this distribution is close to P.

Lemma 13. *Let $q > 2$, $f \in \mathbb{Z}[x]$ monic and irreducible of degree m such that $f(q) \geq q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > 0$, $S \in \mathbb{Z}_q[x]/f$ and $s \in \mathbb{Z}_{f(q)}$ such that $\Phi_q^{(f)}(s) = S$. Then we have:*

$$\begin{aligned} R_{\mathsf{P\ to\ IP}} &:= R(\mathsf{P}_{q,\sigma}^{(f)}(S) || \Phi_q^{(f)}(\mathsf{IP}_{q,\sigma}^{(f)}(s))) \\ &\leq 162 \exp\Big(114 \frac{m^3 \mathsf{EF}(f)^2 (\|f\|_\infty + \|S\|_\infty)^2}{\sigma^2}\Big). \end{aligned}$$

The below result follows from the Rényi divergence probability preservation.

Theorem 4. *Let $q > 2$ and $f \in \mathbb{Z}[x]$ irreducible and monic of degree $m > 0$ such that $f(q) < q^m$ and whose coefficients belong to $(-q/2, q/2)$. Let $\sigma > \sigma' > 0$ such that $q > \sqrt{m}\sigma$. Let t be a number of samples, such that:*

$$\exp\Big(114t\Big(1 + 114m^3 \mathsf{EF}(f)^2 \frac{(\|f\|_\infty + m^{1/2}\sigma')^2}{\sigma^2}\Big)\Big) = \mathsf{poly}(m).$$

Then $\mathsf{sI\text{-}PLWE}_{q,\sigma,\sigma',t}^{(f)}$ reduces to $\mathsf{sPLWE}_{q,\sigma,\sigma',t}^{(f)}$.

5 A Public-Key Encryption Scheme Based on sI-PLWE

We now describe a deterministic public-key encryption scheme, whose OW-CPA security will be proved based on the presumed hardness of sI-PLWE and dPLWE.

KeyGen(1^λ)**.** On input the security parameter, the key generation algorithm first chooses parameters $\mathsf{pp} := (f, q, \sigma, \sigma', K)$ as explained below. First, let $m := \deg f$. Define $\mathcal{C} = \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}$ and

$$\mathcal{M} = \Big\{ \Big(\sum_i t_i q^i, \sum_i e_i' q^i, \sum_i e_i'' q^i \Big) \in \mathbb{Z}_{f(q)}^3 \mid \forall i : |t_i| \leq \sigma' \sqrt{m} \ \wedge \ |e_i'|, |e_i''| \leq \sigma \sqrt{m} \Big\}.$$

Sample $a \hookleftarrow \mathcal{U}(\mathbb{Z}_{f(q)})$, $s \hookleftarrow D_{\mathbb{Z}_{f(q)}, \sigma', \sigma'\sqrt{m}}$ and $e \hookleftarrow D_{\mathbb{Z}_{f(q)}, \sigma, \sigma\sqrt{m}}$. If $e = 0$, then restart. Compute $b = as + e \in \mathbb{Z}_{f(q)}$ and output:

$$\mathsf{pk} := (\mathsf{pp}, a, b) \ \text{ and } \ \mathsf{sk} := (\mathsf{pp}, s, e).$$

Enc(pk, M)**.** On input the public key $\mathsf{pk} = (\mathsf{pp}, a, b)$ and any valid plaintext message $M = (t, e', e'') \in \mathcal{M}$, compute and output:

$$(c_1, c_2) := (a \cdot t + K \cdot e', \ b \cdot t + K \cdot e'') \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}.$$

Dec$(\mathsf{sk}, (c_1, c_2))$**.** On input the secret key $\mathsf{sk} = (\mathsf{pp}, s, e)$ comprised of the public parameters and two short vectors, and a ciphertext (c_1, c_2), the decryption algorithm first computes:

$$d := c_2 - c_1 \cdot s.$$

Writing $d = \sum_i d_i q^i$, it computes $d' = \sum_i (d_i \bmod K) \cdot q^i \bmod f(q)$. It then recovers the message $t = d'/e \bmod f(q)$, $e' = (c_1 - at)/K \bmod f(q)$ and $e'' = (c_2 - bt)/K \bmod f(q)$. Finally, it outputs (t, e', e'').

We make a few comments on the scheme. By a standard tail bound, the distributions $D_{\mathbb{Z}_{f(q)},\sigma,\sigma\sqrt{m}}$ and $D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}}$ can be efficiently sampled by rejection sampling from $D_{\mathbb{Z}_{f(q)},\sigma}$ and $D_{\mathbb{Z}_{f(q)},\sigma'}$, respectively. Also, the probability that $e = 0$ is $2^{-\Omega(m)}$. We explicitly exclude this possibility to prove perfect correctness. We will prove OW-CPA security with respect to the distribution

$$D_{\mathcal{M}} = D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}} \times D_{\mathbb{Z}_{f(q)},\sigma,\sigma\sqrt{m}} \times D_{\mathbb{Z}_{f(q)},\sigma,\sigma\sqrt{m}}$$

over the plaintext space $\mathcal{M}$. For the same reasons as above, it can be sampled efficiently, and its min-entropy is $H_\infty(D_{\mathcal{M}}) = \Omega(m \log \sigma)$. Finally, in the decryption algorithm, we make several divisions modulo $f(q)$. To guarantee its possibility, we impose that $f(q)$ is prime and make sure that e and K are non-zero.

We choose $f \in \mathbb{Z}[x]$ monic and irreducible of degree $m > 0$. We choose $q > 2$ such that $f(q)$ is prime. Note that $f(q)$ has bit-length $\approx m \log q$, so if q is $\Omega(m^{1+\varepsilon})$ for any $\varepsilon > 0$, we heuristically expect that $f(q)$ is prime after a polynomial number of trials for q will make $f(q)$ prime. Note that in full generality, it may not be possible to find any q that makes $f(q)$ prime (for example, consider $f = x^2 + x + 4$).

The other parameters are set as follows. For correctness (Theorem 5), we impose that $K > 14\sigma\sigma' m^2 \|f\|_\infty \mathsf{EF}(f)$ and $q > 84Km^2\|f\|_\infty \mathsf{EF}(f)\sigma\sigma'$. For OW-CPA security (Theorem 6), we impose that $\sigma > \sqrt{m}\mathsf{EF}(f)(\|f\|_1 + m^{3/2}\sigma')$ and $\sigma' \geq \sqrt{m}$. These inequalities can be handled by first setting σ', then σ, K and q. For security against known PLWE attacks, one may choose $m = \Omega(\lambda)$ and $q, \sigma, \sigma' \in \mathrm{poly}(m)$.

Theorem 5 (Correctness). *Assume that* $K > 14\sigma\sigma' m^2 \|f\|_\infty \mathsf{EF}(f)$ *and also* $q > 84K\sigma\sigma' m^2 \|f\|_\infty \mathsf{EF}(f)$*. Then the above encryption scheme is correct.*

Proof. Let (c_1, c_2) be an encryption of $M = (t, e', e'') \in \mathcal{M}$ under pk. We want to show that given sk and (c_1, c_2), the decryption algorithm indeed recovers M. Note first that $d = c_2 - c_1 \cdot s = K \cdot (e'' - e' \cdot s) + e \cdot t \bmod f(q)$. By carries analysis from Lemma 14 found in appendix of the full version, we have

$$\forall i < m : d_i = d'_i + K \cdot d''_i \quad \text{with} \quad |d'_i| < K/2 \quad \text{and } d' = \sum_i d'_i q^i = e \cdot t \bmod f(q).$$

This exploits the parameter conditions on K and q. Once the decryption algorithm has recovered $d' = e \cdot t \bmod f(q)$, it can recover t, e' and e'' using division in the field $\mathbb{Z}_{f(q)}$. □

Lemma 14. *Let* $K > 14\sigma\sigma' m^2 \|f\|_\infty \mathsf{EF}(f)$ *and* $q > 84K\sigma\sigma' m^2 \|f\|_\infty \mathsf{EF}(f)$. *Let* (c_1, c_2) *be an encryption of* $M = (t, e', e'') \in \mathcal{M}$ *under* $\mathsf{pk} = (a, as + e)$. *Then let* $d = \sum_i d_i q^i := c_2 - c_1 \cdot s$ *and write* $d_i = d'_i + K \cdot d''_i$ *with* $|d'_i| < K/2$, *for any* $i < m$. *Then* $d' := \sum_i d'_i q^i = e \cdot t \bmod f(q)$.

We now study the OW-CPA security of the above deterministic cryptosystem.

Theorem 6 (Security). *Assuming that* $\sigma \geq \sqrt{m}\mathsf{EF}(f) \cdot (\|f\|_1 + m^{3/2}\sigma')$ *and* $\sigma' \geq \sqrt{m}$, *the above* PKE *scheme is* OW-CPA *secure for distribution* $D_{\mathcal{M}}$, *under the* $\mathsf{sl\text{-}PLWE}^{(f)}_{q,\sigma,\sigma',2}$ *and* $\mathsf{dPLWE}^{(f)}_{q,\sigma,\sigma',1}$ *assumptions. More concretely, if there exists a* OW-CPA *adversary* $\mathcal{A}$, *then there exist algorithms* $\mathcal{B}$ *and* $\mathcal{C}$ *for* dPLWE *and* sl-PLWE, *respectively, with run-times similar to the run-time of* $\mathcal{A}$ *and such that:*

$$\mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},D_{\mathcal{M}}}(\mathcal{A}) \leq O\left(\mathsf{Adv}^{\mathsf{sl\text{-}PLWE}}_{f,q,\sigma,\sigma'}(\mathcal{C})^{1/4} + \mathsf{Adv}^{\mathsf{dPLWE}}_{f,q,\sigma,\sigma'}(\mathcal{B})^{1/2}\right) + 2^{-\Omega(m)}.$$

Our security proof relies on two security assumptions: the search problem sl-PLWE and the decision problem dPLWE. As recalled in Sect. 2, dPLWE and sPLWE can be set so that they reduce to one another (up to some limited parameter losses). From Sect. 4, we know that sPLWE and sl-PLWE reduce to one another. Therefore, Theorem 6 could be adapted to make security rely on a single hardness assumption, e.g., sl-PLWE.

Proof. Assume that there exists an adversary $\mathcal{A}$ against the OW-CPA game of the PKE with non-negligible success probability ε_0. We define the following games:

Game 0**:** This is the OW-CPA game.

Game 1**:** In this game, we sample $s \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma'}$ and $e \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma}$ instead of $s \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}}$ and $e \hookleftarrow D_{\mathbb{Z}_{f(q)},\sigma,\sigma\sqrt{m}}$, respectively. Also, we do not reject when $e = 0$.

Game 2**:** In this game, we change the distribution of the public key pk. First we start by sampling $A \hookleftarrow \mathcal{U}(\mathbb{Z}_q[x]/f)$, $S \hookleftarrow D_{\mathbb{Z}[x]/f,\sigma',q}$ and $E \hookleftarrow D_{\mathbb{Z}[x]/f,\sigma,q}$ and then set $B = AS + E \bmod f$. Then

- If $f(q) \geq q^m$, choose a and b uniformly among the predecessors of A and B by the map $\Phi_q^{(f)}$, respectively.
- If $f(q) < q^m$, compute $(a, b) = (A(q) \bmod f(q), B(q) \bmod f(q))$.

Game 3**:** In this game, we change the generation of B. Instead of sampling (A, B) as above, we sample $(A, B) \hookleftarrow \mathcal{U}((\mathbb{Z}_q[x]/f)^2)$.

Game 4**:** In this game, we change the generation of (a, b) once more. Instead of sampling $(A, B) \hookleftarrow \mathcal{U}((\mathbb{Z}_q[x]/f)^2)$ and computing predecessors (a, b), we directly sample $a, b \hookleftarrow \mathcal{U}(\mathbb{Z}_{f(q)})$.

Let ε_i denote the success probability of $\mathcal{A}$ in Game i. By definition, we have $\varepsilon_0 = \mathsf{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE},D_{\mathcal{M}}}(\mathcal{A})$. For any random variables (a, b, t, e, e', a', b'), the following inequality holds by using the data processing inequality and the multiplicativity of the Rényi divergence:

$$R((a, b, at + Ke, bt + Ke')||(a', b', a't + Ke, b't + Ke')) \leq R((a, b)||(a', b')). \quad (1)$$

In the context of Game 0 versus Game 1, note that the statistical distance between $D_{\mathbb{Z}_{f(q)},\sigma}$ and $D_{\mathbb{Z}_{f(q)},\sigma,\sigma\sqrt{m}}$ is $2^{-\Omega(m)}$. The same holds for $D_{\mathbb{Z}_{f(q)},\sigma'}$ and $D_{\mathbb{Z}_{f(q)},\sigma',\sigma'\sqrt{m}}$. Further, the probability that $e = 0$ is also $2^{-\Omega(m)}$. Therefore, we have $|\varepsilon_0 - \varepsilon_1| \leq 2^{-\Omega(m)}$.

In the context of Game 1 versus Game 2, we can instantiate (1) with (a, b) as in Game 1 and (a', b') as in Game 2. By Lemmas 10 and 11 and thanks to our choice of parameters, this divergence is $\leq O(1)$. Then, by the probability preservation property, we have: $\varepsilon_2 \geq \Omega(\varepsilon_1^2)$.

For Game 2 versus Game 3, we use the hardness of dPLWE. Indeed, one can build an algorithm $\mathcal{B}$ against dPLWE that would exploit a behavioural difference of $\mathcal{A}$ between Game 2 and Game 3. We have:

$$\mathsf{Adv}^{\mathsf{dPLWE}}_{f,q,\sigma,\sigma'}(\mathcal{B}) \geq |\varepsilon_3 - \varepsilon_2| - 2^{-\Omega(m)}.$$

In the context of Game 3 versus Game 4, we instantiate (1) with (a, b) as in Game 3 and (a', b') as in Game 4. In Game 3, the probability of $a = k$ for a given $k \in \mathbb{Z}_{f(q)}$ is $\leq 3/q^m$, and the same holds for b. Therefore:

$$R((a,b)||(a',b')) \leq f(q)^2 \cdot \frac{(3/q^m)^4}{1/f(q)^2} = 81 \cdot \frac{f(q)^4}{q^{4m}}.$$

Since $f(q) < 2q^m$, the divergence is ≤ 1296. By using the probability preservation probability, we have that $\varepsilon_4 \geq \Omega(\varepsilon_3^2)$. Finally, we handle Game 4 using hardness of sI-PLWE. We build an sI-PLWE algorithm $\mathcal{C}$ as follows. Upon receiving two sI-PLWE samples $(a, a \cdot t + e')$ and $(b, b \cdot t + e'')$, it sets

$$\begin{aligned}
\mathsf{pk} &:= (K \cdot a, K \cdot b),\\
c_1 &:= K \cdot (a \cdot t + e') = (K \cdot a) \cdot t + K \cdot e',\\
c_2 &:= K \cdot (b \cdot t + e') = (K \cdot b) \cdot t + K \cdot e''.
\end{aligned}$$

It then calls the OW-CPA adversary $\mathcal{A}$ on the challenge $\mathsf{pk}, (c_1, c_2)$ and waits for its answer (t, e, e'). Then $\mathcal{C}$ outputs t. As K is coprime to $f(q)$, multiplication by K modulo $f(q)$ is a bijection, and the view of $\mathcal{A}$ is as in Game 4. As a result, we have that $\mathsf{Adv}^{\mathsf{sI\text{-}PLWE}}_{f,q,\sigma,\sigma'}(\mathcal{C}) \geq \varepsilon_3$. The result follows by collecting terms. □

Acknowledgments. This work was supported in part by European Union Horizon 2020 Research and Innovation Program Grant 780701, Australian Research Council Discovery Project Grant DP180102199, and by BPI-France in the context of the national project RISQ (P141580).

References

[ABD+17] Alkim, E., et al.: Frodo: Candidate to NIS (2017)

[ACPS09] Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_35

[AD17] Albrecht, M.R., Deo, A.: Large modulus ring-LWE ≥ module-LWE. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8

[AJPS18] Aggarwal, D., Joux, A., Prakash, A., Santha, M.: A new public-key cryptosystem via Mersenne numbers. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10993, pp. 459–482. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96878-0_16

[BCF20] Budroni, A., Chetioui, B., Franch, E.: Attacks on integer-RLWE. IACR Cryptol. ePrint Arch. **2020**, 1007 (2020)

[BCSV20] Bootland, C., Castryck, W., Szepieniec, A., Vercauteren, F.: A framework for cryptographic problems from linear algebra. J. Math. Cryptol. **14**(1), 202–217 (2020)

[BF11] Boneh, D., Freeman, D.M.: Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 1–16. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_1

[BGV12] Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: ITCS 2012 (2012)

[BHH+19] Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019. LNCS, vol. 11892, pp. 61–90. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-36033-7_3

[BLP+13] Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: STOC 2013 (2013)

[BLRL+18] Bai, S., Lepoint, T., Roux-Langlois, A., Sakzad, A., Stehlé, D., Steinfeld, R.: Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance. J. Cryptol. **31**(2), 610–640 (2018)

[BP18] Bernstein, D.J., Persichetti, E.: Towards KEM unification. IACR Cryptol. ePrint Arch. **2018**, 526 (2018)

[BPR12] Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 719–737. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_42

[Gen01] Gentry, C.: Key recovery and message attacks on NTRU-composite. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 182–194. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_12

[Gu17] Gu, C.: Integer version of ring-LWE and its applications. IACR Cryptol. ePrint Arch. **2017**, 641 (2017)

[Gu19] Gu, C.: Integer version of ring-LWE and its applications. In: Meng, W., Furnell, S. (eds.) SocialSec 2019. CCIS, vol. 1095, pp. 110–122. Springer, Singapore (2019). https://doi.org/10.1007/978-981-15-0758-8_9

[Ham17] Hamburg, M.: Three bears: Candidate to NIS (2017)

[HHK17] Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017. LNCS, vol. 10677, pp. 341–371. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70500-2_12

[KSS+20] Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.-F.: Measure-rewind-measure: tighter quantum random oracle model proofs for one-way to hiding and CCA security. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020. LNCS, vol. 12107, pp. 703–728. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45727-3_24

[LM06] Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (2006). https://doi.org/10.1007/11787006_13

[LPR10] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1

[LS15] Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Crypt. **75**(3), 565–599 (2014). https://doi.org/10.1007/s10623-014-9938-4

[LSS14] Langlois, A., Stehlé, D., Steinfeld, R.: GGHLite: more efficient multilinear maps from ideal lattices. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 239–256. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_14

[NIS] NIST: Post-Quantum Cryptography Project. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/

[PRS17] Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-LWE for any ring and modulus. In: STOC 2017 (2017)

[Reg09] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 34 (2009)

[RSW18] Rosca, M., Stehlé, D., Wallet, A.: On the ring-LWE and polynomial-LWE problems. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 146–173. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78381-9_6

[SSTX09] Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_36

[SXY18] Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10822, pp. 520–551. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78372-7_17

[Sze17] Szepieniec, A.: Ramstake: Candidate to NIS (2017)