Efficient RLWE based Chosen-Ciphertext Secure Dual-Receiver Encryption and Sender-Binding KEM in the Standard Model

Laurin Benz[1,2] and Robert Brede[1,2]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany
[2] KASTEL Security Research Labs, Karlsruhe, Germany
{laurin.benz,robert.brede}@kit.edu

Abstract. Key encapsulation mechanism (KEM) is an often used primitive in communication, closely related to public key encryption (PKE). Dual-receiver encryption (DRE) is another primitive closely related to PKE that allows a sender to encrypt a message to two different receivers. Most applications of DRE need the soundness property which guarantees that both receivers decrypt any ciphertext to the same message. Additionally, IND-CPA security is often not enough and therefore schemes should satisfy a stronger notion like IND-CCA2. Meanwhile, an alternative to IND-CCA2 for KEMs is the IND-SB-CPA security notion which was proven to be strong enough to realize secure channels while in theory enabling the construction of more efficient schemes.
Most IND-CCA2 security proofs rely on the FO transformation, which is only secure in the ROM, and the standard model DREs and KEMs are far from efficient. We fill this gap by providing a sound DRE and a KEM satisfying IND-CCA2 and IND-SB-CPA security respectively. Both schemes are based on RLWE, proven secure in the standard model, and have key sizes of 150 KB and ciphertext sizes of 100 KB, improving upon previous results by a factor of 10x to 100x.

Keywords: Dual-receiver encryption (DRE) · Soundness · Sender-binding key encapsulation mechanism (SB-KEM) · Hybrid Encryption · Ring Learning With Errors (RLWE) · Post-Quantum · IND-CCA2 · Standard Model

1 Introduction

Broadcast encryption (BE) [14], a special form of public key encryption (PKE), allows a sender to encrypt a message to multiple receivers with a single ciphertext. Dual-receiver encryption (DRE) can be seen as a special case of BE for two receivers. While the definition is syntactically simple, Chow, Franklin, and Zhang [11] showed that most applications need the special property "soundness", which guarantees that one receiver can be certain that the other receiver decrypts the ciphertext to the same message. Additionally, the usual indistinguishability under chosen plaintext attack (IND-CPA) security notion is often not strong enough and

instead the more restrictive indistinguishability under adaptive chosen ciphertext attack (IND-CCA2) security, adapted to DRE, is needed. Benz *et al.* [5] conducted a survey on post-quantum IND-CCA2 secure DRE constructions in the standard model and noticed that all of them lack the soundness property, rendering them useless in applications that require this property [4, 8, 11, 12, 13, 27, 30].

Furthermore, most IND-CCA2 secure PKE schemes use the well-known Fujisaki-Okamoto (FO) transformation [16] to convert an IND-CPA secure scheme into an IND-CCA2 one. This transformation relies on the Random Oracle Model (ROM), a model where overidealized hash functions are available. While Canetti, Goldreich, and Halevi [10] proved over 20 years ago that there exist schemes which are secure in the ROM, but insecure whenever the random oracle is instantiated, their examples were specifically designed to fail. Recently however, Khovratovich, Rothblum, and Soukhanov [19] presented an attack on the similar Fiat-Shamir transformation [15], using the reliance on the ROM to break a natural proof-system. This motivates further research into secure constructions in the standard model. Recently for example, Hsieh, Waters, and Wu [18] used a special form of pseudorandom generator (PRG) to generically create BE in the standard model, but their scheme only satisfies the BE version of IND-CPA security.

As standard model IND-CCA2 security is hard to achieve and known to be unnecessarily strong for many applications, Beskorovajnov *et al.* [8] devised a new security notion for PKEs, called indistinguishability under sender-binding chosen plaintext attack (IND-SB-CPA). This notion, which they proved to be between IND-CPA and IND-CCA2, was introduced to enable the construction of smaller, more efficient encryption schemes that are still secure enough to realize secure channels, one of the main uses of IND-CCA2 security. It was also adapted to the key encapsulation mechanism (KEM) framework, resulting in the indistinguishability under sender-binding chosen plaintext attack (IND-SB-$\text{CPA}_{\text{SB-KEM}}$) security notion [6].

Even though there are many applications for efficient DRE schemes as well as sender-binding key encapsulation mechanisms (SB-KEM), so far the most efficient standard model IND-CCA2 DRE constructions have either key and ciphertext sizes of around 700 MB and 25 KB, or around 120 MB and 100 KB [5]. Also, while the IND-SB-$\text{CPA}_{\text{SB-KEM}}$ security notion was introduced to allow for more efficient schemes, the only standard model IND-SB-$\text{CPA}_{\text{SB-KEM}}$ KEM prior to this work [6] has worse sizes than the most efficient standard model IND-CCA2 KEMs which in turn have key and ciphertext sizes of around 3 MB and 1 MB, or around 110 MB and 5 KB [31, 32].

In this work, we derive a DRE scheme and a SB-KEM based on Ring Learning With Errors (RLWE) satisfying the aforementioned properties. For this, we use a ring version of the trapdoor construction by Micciancio and Peikert [25]. The resulting schemes have key and ciphertext sizes around 150 KB and 100 KB for 162 bit security, significantly improving upon previous results. In addition, we prove that RLWE samples are unique under certain conditions, which was shown for LWE by Zhang *et al.* [33] and could be of independent interest.

Outline. In Section 2 we introduce notations and primitives needed for our constructions. We also state and prove some new lemmas on the used rings. More specifically, Section 2.1 introduces algebraic notation, Sections 2.2 to 2.4 deal with lattices and RLWE including our new results, while Section 2.5 defines all needed cryptographic primitives and their security notions.

We then define our DRE scheme in Section 3. Additionally, we prove correctness, soundness and IND-CCA2 security. For this, we adapt the proofs of Benz *et al.* [5], Boyen, Izabachène, and Li [9], and Kiltz, Masny, and Pietrzak [20] to our setting.

The SB-KEM is the focus of Section 4. As the scheme is a simplification of our DRE construction, the proofs carry over from Section 3.

Finally, in Section 5 we give concrete parameters and compare our results to the literature. We also note that using Module Learning With Errors (MLWE) did not improve the parameters, even though the proofs could also be adapted to that setting.

2 Fundamentals

For a matrix S and $p \in [1, \infty)$ we write $\|S\|_p = \max_{\|x\|_p=1} \|Sx\|_p$. For $\alpha \in \mathbb{Z}_q$ we write $\lfloor \alpha \rceil_{q/2}$ for rounding to 0 if $\alpha \mod q \in [-q/4, q/4)$ and $q/2$ otherwise. A function $f : \mathbb{N} \to \mathbb{R}$ is *negligible* if for every $k \in \mathbb{N}$ there is an $n \in \mathbb{N}$ such that for all $x > n : f(x) \leq x^{-k}$. We use the standard big O notations. For a set $\mathbf{S}$ we denote by $x \xleftarrow{\$} \mathbf{S}$ the uniform sampling of an element x from $\mathbf{S}$. For a probability distribution χ, $x \leftarrow \chi$ denotes sampling according to that distribution. Similarly, if P is a probabilistic algorithm, we denote by $y \leftarrow P(x)$ the result of one execution of P with input x. Two distribution ensembles $\mathcal{X}_n, \mathcal{Y}_n (n \in \mathbb{N})$ over set $\mathbf{S}$ are called *statistically indistinguishable* if the statistical distance $\Delta(\mathcal{X}_n, \mathcal{Y}_n) = \sup_{A \subseteq S} |\mathbb{P}[x \in A \mid x \leftarrow \mathcal{X}_n] - \mathbb{P}[y \in A \mid y \leftarrow \mathcal{Y}_n]|$ is negligible in n. The component-wise multiplication of two vectors e, f is denoted by $e \odot f$.

2.1 Algebraic Number Theory

Here, we recall the major definitions of algebraic number theory required for this work. We work with cyclotomic number fields (cyclotomics). The $\tilde{n}$-th cyclotomic is $K = \mathbb{Q}[\zeta]$, where ζ is a primitive $\tilde{n}$-th root of unity. It is isomorph to $\mathbb{Q}[X]/\Phi_{\tilde{n}}$, where $\Phi_{\tilde{n}}$ is the minimal polynomial of ζ, which is also called the $\tilde{n}$-th cyclotomic polynomial. Its ring of integers is always denoted by $R = \mathbb{Z}[X]/\Phi_{\tilde{n}}$ while its degree is denoted by n. For an integer q, we write $R_q = R/qR$ and we always center our elements around 0, such that all coefficients are in the interval $[-q/2, q/2)$. Throughout this work, we will always consider the elements of this ring in their polynomial representation.

There are two different commonly used embeddings for these elements. The first embedding is the coefficient embedding φ, which embeds a polynomial into $\mathbb{Q}$ via the power basis. As $\varphi(R) = \mathbb{Z}^n$, this embedding is especially useful for storing ring elements and performing operations on them. The canonical

embedding instead embeds a polynomial into a subset $H \subseteq \mathbb{C}^n$ by evaluating it at each root of $\Phi_{\tilde{n}}$. More specifically, for integers s_1, s_2 with $n = s_1 + 2s_2$ let $H = \{x \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \mid x_{2j-1+s_1} = \overline{x_{2j+s_1}}, 1 \leq j \leq s_2\}$. The canonical embedding $\sigma \coloneqq (\sigma_1, ..., \sigma_n) : K \to H$ consists of the embeddings $\sigma_i : h \mapsto h(\zeta_i)$, which evaluate h at the i-th root ζ_i of $\Phi_{\tilde{n}}$, where we reorder the roots in such a way that we end up in H. To draw a random element of R embedded in H we define the space $J \coloneqq \sigma(R)$.

For vectors of ring elements, we sometimes use a different norm on each ring element than on the whole vector, and the norms we use also depend on the chosen embedding. Hence, for $p, q \in \{2, \infty\}$, $e \in \{\varphi, \sigma\}$ and $x \in R^m$, we define $\left\|[x]_{e,p}\right\|_q \coloneqq \|(v_1, ..., v_m)\|_q, v_i = \|e(x_i)\|_p$ and we write $\|x\|_{e,p} \coloneqq \left\|[x]_{e,p}\right\|_p$ for short. For an already canonical embedded element $x \in H$ we abuse notation and also write $\left\|[x]_{e,p}\right\|_q$ for $\left\|\left[\sigma^{-1}(x)\right]_{e,p}\right\|_q$.

Notice that the two embeddings are correlated by the matrix $B_\Lambda = (\zeta_i^{j-1})_{ij}$, where ζ_i is the i-th root of $\Phi_{\tilde{n}}$. Also, the space $(H, +, \odot)$ is isomorph to $(\mathbb{R}^n, +, \cdot)$ via the isomorphism

$$\psi = \begin{pmatrix} I_{s_1} & 0 \\ 0 & \sqrt{2} I_{s_2} \otimes \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \end{pmatrix}.$$

Note that the multiplication $\cdot$ in $\mathbb{R}^n$ is performed by a matrix multiplication to simulate $\odot$ in H. For $e, f \in H$ we denote by A_e the matrix depending on e that satisfies $\psi(e \odot f) = A_e \cdot \psi(f)$. A concrete definition can be found in Appendix A. For vectors and matrices over H or $\mathbb{R}^n$, we write $\psi(A)$ or $\psi^{-1}(A)$ for applying the function to each element.

Lyubashevsky, Peikert, and Regev [22] analyzed the fraction of invertible elements in the ring of integers of a cyclotomic after applying a modulo q. Their result is that the fraction is at least polynomial in n and q, as described in the following lemma.

Lemma 1. *([22], Claim 2.25) Consider the $\tilde{n}$-th cyclotomic number field of degree n for some $\tilde{n} \geq 2$. Then for any $q \geq 2$, the fraction of invertible elements in R_q is at least $1/poly(n, \log q)$.*

2.2 Lattices and Gaussian Random Variables

We now recall some basic definitions and lemmas related to lattices and Gaussian distributions.

A lattice $\Lambda \subseteq \mathbb{R}^n$ is a discrete subspace of $\mathbb{R}^n$. As throughout this work we only consider lattices of full-rank, we can alternatively define the lattice as $\Lambda = \{\sum z_i b_i \mid z_i \in \mathbb{Z}\}$ for a set $B = \{b_1, \ldots, b_n\} \subseteq \mathbb{R}^n$ of linear independent vectors. The set B is then called the basis of Λ. The dual lattice of $\Lambda \subseteq \mathbb{R}^n$ is defined as $\Lambda^\vee = \{x \in \mathbb{R}^n \mid \forall y \in \Lambda : \langle x, y \rangle \in \mathbb{Z}\}$. For a basis B, we denote with $\mathcal{P}_{1/2}(B)$ the origin centered parallelepiped $\mathcal{P}_{1/2}(B) = B \cdot [-1/2, 1/2)^n$. For a modulo q and a vector $a \in R_q^m$, we define $\Lambda_q^\perp(a) \coloneqq \{x \in R_q^m \mid a^T x = 0 \mod q\}$.

Regarding the Gaussian random variables, we adopt the notation of Genise *et al.* [17]. The Gaussian function is defined as $\rho : \mathbb{R}^n \to \mathbb{R}, \rho(x) = \exp(-\pi\langle x, x\rangle)$. By normalizing we obtain the Gaussian distribution $\mathcal{D}$. For a matrix $S \in \mathbb{R}^{n\times n}$, the Gaussian distribution $\mathcal{D}_S$ is defined as $\mathcal{D}_S \coloneqq \sqrt{2\pi}S \cdot \mathcal{D}$. For $s \in \mathbb{R}$, we write $\mathcal{D}_s$ as short for $\mathcal{D}_{sI}$ and denote this by the Gaussian of parameter s. For a lattice $\Lambda \subseteq \mathbb{R}^n$, the discrete Gaussian is defined as the Gaussian restricted to the lattice, meaning $\mathcal{D}_{\Lambda,S}(x) = \mathcal{D}_S(x)/\mathcal{D}_S(\Lambda)$ for $x \in \Lambda$ and 0 otherwise.

Micciancio and Regev [26] introduced the *smoothing parameter* for working with discrete Gaussians.

Definition 1 (Smoothing Parameter). For a lattice $\Lambda \subseteq \mathbb{R}^n$ and positive real $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\Lambda)$ is the smallest real s, such that $\rho(s \cdot \Lambda^\vee) \leq 1 + \varepsilon$.

We use the extension of the smoothing parameter to matrices as in the work by Genise *et al.* [17]. For any matrix S of full column rank we write $\eta_\varepsilon(\Lambda) \leq S$ if $\eta_\varepsilon(S^+\Lambda) \leq 1$, where S^+ is the pseudoinverse of S.

The tail of a discrete Gaussian can be bounded as follows.

Lemma 2. *Let $t > 1$ and $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Let also $\Sigma \in \mathbb{R}^{n\times n}_{\geq 0}$ be a diagonal matrix and $s = \|\sqrt{\Sigma}\|_2$. Then we have*

$$\mathbb{P}\left[\|x\|_2 > st\sqrt{n} \mid x \leftarrow \mathcal{D}_{\Lambda,\sqrt{\Sigma}}\right] < \left(e^{\frac{-t^2}{2}} t\sqrt{e}\right)^n,$$

which is negligible in n.

The proof of this is an adaption of a work by Banaszczyk [3, Lemma 1.5(i)], which is shown in Appendix A.

The next lemma shows that the linear combination of multiple discrete Gaussian distributed variables is again a discrete Gaussian.

Lemma 3. *Consider the $\tilde{n}$-th cyclotomic number field of degree n for some $\tilde{n} \geq 2$, $J \subseteq H$ its embedded ring of integers and $\Lambda = \psi(J) \subseteq \mathbb{R}^n$ the corresponding lattice. Let Σ_f be a positive definite diagonal matrix. For $s_T > 0$, an integer m and $1 \leq i \leq m$, let $t_i \leftarrow \psi^{-1}\left(\mathcal{D}_{\Lambda,s_T}\right), e_i \in J$ and $f \leftarrow \psi^{-1}\left(\mathcal{D}_{\Lambda,\sqrt{\Sigma_f}}\right)$. Let $\varepsilon \coloneqq \varepsilon(n) > 0$ be negligible in n. If $\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi}\cdot A_{e_i}^{-1}\sqrt{\left(\Sigma_f^{-1} + \left(s_T^2 A_{e_i} A_{e_i}^T\right)^{-1}\right)^{-1}}$ for every i, where $e_i \neq 0$ and $\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi}\cdot\sqrt{\Sigma_f}$, then the distribution of*

$$f + \sum_{i=1}^{m} e_i \odot t_i$$

is statistically close to $\psi^{-1}\left(\mathcal{D}_{\Lambda,\sqrt{\Sigma}}\right)$, where we define the width of the Gaussian as $\Sigma \coloneqq \Sigma_f + s_T^2 \sum_{i=1}^m A_{e_i} A_{e_i}^T = \Sigma_f + s_T^2 Mul(e)$ for $e \coloneqq (e_1, \ldots, e_m)$ and $Mul(e) \coloneqq \sum_{i=1}^m A_{e_i} A_{e_i}^T$.

The proof for this is a repeated application of a theorem by Genise *et al.* [17, Theorem 3] and can be found in Appendix A.

Another important lemma is the regularity lemma shown by Lyubashevsky, Peikert, and Regev [22], which provides bounds on the variance of a Gaussian distributed x, such that Ax is statistically indistinguishable from uniform, when parts of A are uniformly random. As our Gaussian distribution is scaled up by $\sqrt{2\pi}$ compared to their work, the bound on the parameter of Gaussian is adjusted.

Lemma 4 ([22], Corollary 7.5). *Consider the $\tilde{n}$-th cyclotomic number field of degree n for some $\tilde{n} \geq 2$. Let q as well as $z_1 \leq z_2 \leq poly(n)$ be positive integers. Assume $A = (I_{z_1}, \bar{A}) \in R_q^{z_1 \times z_2}$, where $I_{z_1} \in R_q^{z_1 \times z_1}$ is the identity matrix and $\bar{A} \in R_q^{z_1 \times (z_2 - z_1)}$ is uniformly random. Then with probability $1 - 2^{-\Omega(n)}$ over the choices of $\bar{A}$, the distribution of $Ax \in R_q^{z_1}$, where each coordinate of $x \in R_q^{z_2}$ is chosen from a discrete Gaussian distribution of parameter $r > \sqrt{2\pi^{-1}} n \cdot q^{z_1/z_2 + 2/(nz_2)}$ over R, satisfies that the probability of each of the q^{nz_1} possible outcomes is in the interval $(1 \pm 2^{-\Omega(n)})q^{-nz_1}$ (and in particular is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over $R_q^{z_1}$).*

2.3 Ring LWE and its Trapdoor

In this paper, we use the decision variant of the Normal Form Ring Learning With Errors (NRLWE) assumption, which is as follows.

Definition 2 (NRLWE). Let λ be the security parameter, $m = m(\lambda), q = q(\lambda) \in \mathbb{Z}$ and $\chi = \chi(\lambda)$ be an error distribution over R_q. The advantage of an adversary $\mathcal{A}$ against the $\mathrm{NRLWE}_{m,q,\chi}$ problem, denoted by $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NRLWE}_{m,q,\chi}}$ is

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NRLWE}_{m,q,\chi}} \coloneqq \left| \mathbb{P}\left[\mathcal{A}(a, as + e) = 1\right] - \mathbb{P}\left[\mathcal{A}(a, u) = 1\right] \right|,$$

where $a \leftarrow R_q^m, s \leftarrow \chi, e \leftarrow \chi^m, u \xleftarrow{\$} R_q^m$.

Notice that in contrast to the usual RLWE assumption, the secret is also drawn from the error distribution instead of being uniformly random. Lyubashevsky, Peikert, and Regev [22] showed that NRLWE is as hard as RLWE.

Micciancio and Peikert [25] introduced an efficient method to recover s from $gs + e$, where g is the gadget vector $g = (1, 2, \ldots, 2^{k-1}) \in R_q^k$ for $k = \lceil \log q \rceil$. To recover s from $c = as + e$, one uses a trapdoor for a, which is defined as follows.

Definition 3 (Trapdoor, adapted from [25]). Consider the $\tilde{n}$-th cyclotomic number field of degree n for some $\tilde{n} \geq 2$ and q a modulo. Let $m > k \geq 1$ be integers, $a \in R_q^m$ and $g \in R_q^k$. A g-trapdoor $T \in R^{k \times (m-k)}$ for a is a matrix for which $(T, I_k)a = gh$ for some invertible $h \in R_q$. We refer to h as the tag or label of the trapdoor.

To guarantee correct inversion, one needs a basis of $\Lambda_q^{\perp}(g)$. For a prime $q = \sum_{i=1}^{k} q_i 2^{i-1}$, it can be shown that B_g as follows is such a basis [25, Section 4.2].

$$B_g = \begin{pmatrix} 2 & & & & q_1 \\ -1 & 2 & & & q_2 \\ & -1 & & & q_3 \\ & & \ddots & \ddots & \vdots \\ & & & -1 \;\; 2 & q_{k-1} \\ & & & -1 & q_k \end{pmatrix} \in R_q^{k \times k}. \tag{1}$$

Here, each $q_i \in \{0, 1\}$ is interpreted as constant polynomial.

For any $a \in R_q^m$ with a g-trapdoor T, one can recover s, e from $c = as + e$ with the `invert` function described in Figure 1.

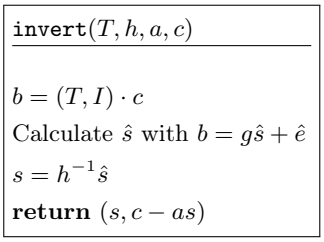

Fig. 1. Invert function.

The `invert` function returns the correct s, if the error $\hat{e} \coloneqq (T, I_k)e$ is suitable small as stated in the following lemma.

Lemma 5. *Consider the $\tilde{n}$-th cyclotomic number field of degree n for some $\tilde{n} \geq 2$ and q a modulo. Take $m > k$ to be integers, $a \in R_q^m$ and $g \in R_q^k$ the gadget vector above. Let also T be a g-trapdoor for a with tag $h \in R_q$, $s \in R_q$ be a secret and $c = as + e$ for some error $e \in R_q^m$. Finally take either B to be B_g as in Equation* (1) *or its Gram-Schmidt orthogonalization. If $(T, I_k)e \in \mathcal{P}_{1/2}(q \cdot B^{-T})$, then* `invert`$(T, h, a, c)$ *returns the correct s.*

Proof. The correctness of the `invert` function relies on the inversion of $g\hat{s} + \hat{e}$ in the second step. More specifically, we have $\hat{e} = (T, I_k)e$ as

$$b = (T, I_k)c = (T, I_k)as + (T, I_k)e = ghs + (T, I_k)e.$$

If $\hat{e} \in \mathcal{P}_{1/2}(q \cdot B^{-T})$, then the correct $\hat{s} = hs$ is calculated [21, 25]. As h is invertible, $s = h^{-1}\hat{s}$ is uniquely determined by $\hat{s}$. □

2.4 Uniqueness of RLWE

This chapter proves that under certain conditions, RLWE samples have a unique witness. Zhang *et al.* [33] showed this property for LWE. We show the uniqueness

only for power of two cyclotomics with a very special modulo as these yield nicer structures.

In this section, let $\tilde{n} = 2n > r > 1$ be powers of two and q be some prime with $q = 2r + 1 \mod 4r$. Let $\Phi_{\tilde{n}}$ be the $\tilde{n}$-th cyclotomic polynomial with order n, i.e. $\Phi_{\tilde{n}} = X^n + 1 \equiv f_1 \cdot \ldots \cdot f_r \pmod q$ where $f_i \in \mathbb{Z}_q[X]$ are irreducible in $\mathbb{Z}_q$.

A careful analysis of the decomposition of $\Phi_{\tilde{n}} \mod q$ and the CRT decomposition yields the following probability bound. The details can be found in Appendix B.

Lemma 6. *Let $\nu \in R_q \setminus \{0\}$ such that the CRT decomposition of ν is $\pi(\nu) = (\nu_1, \ldots, \nu_r)$ with $\nu_i = \nu \mod f_i \in \{0, 1\}$. Consider the subspace $U \coloneqq \nu R_q$. Then $\mathbb{P}\left[\|u\|_{\psi,\infty} < q/4 \mid u \xleftarrow{\$} U\right] \leq 2^{-n/r}$.*

With this we can show the uniqueness of RLWE samples.

Lemma 7. *Let $m \geq r \log q + \frac{r\omega(\log n)}{n}$ for some superlogarithmic function $\omega(\log n)$. Then for all but a negligible fraction of $a \in R_q^m$ and for any $b \in R_q^m$, there exists at most one pair $(s, e) \in R_q \times R_q^m$ such that $as + e = b$ and $\|e\|_{\psi,\infty} < q/8$.*

The proof is very similar to the proof from Zhang *et al.* [33, Lemma 6], except that the distribution of $a(s - s')$ is uniform in U^m with U as in Lemma 6.

2.5 Cryptographic Primitives

We now define some cryptographic primitives. If not otherwise noted our definitions in this section are based on a paper by Benz *et al.* [5].

Our first definition describes a public key encryption scheme which can be used to encrypt a message to two different public keys.

Definition 4 (DRE). A public-key dual-receiver encryption (DRE) scheme $\mathtt{DRE} = (\mathtt{DRE.gen}, \mathtt{DRE.enc}, \mathtt{DRE.dec})$ consists of the following probabilistic polynomial time (PPT) algorithms:

- $\mathtt{DRE.gen}(1^\lambda) \to (pk, sk)$: The randomized *key generation algorithm* outputs a public/secret key pair (pk, sk). We write (pk^R, sk^R) and (pk^S, sk^S) for the key pairs of two independent users.
- $\mathtt{DRE.enc}(pk^R, pk^S, m) \to c$: The randomized *encryption algorithm* takes as input two public keys pk^R and pk^S and a message m and outputs a cipher text c.
- $\mathtt{DRE.dec}(sk^i, pk^R, pk^S, c) \to m$: The deterministic *decryption algorithm* takes one of the secret keys $sk^i \in \{sk^R, sk^S\}$, two public keys pk^R, pk^S and a ciphertext c and outputs a message m. We write $m^i = \mathtt{DRE.dec}(sk^i, pk^R, pk^S, c)$.

We also require perfect correctness defined as $\mathtt{DRE.dec}(sk^i, pk^R, pk^S, c) = m$ for $(pk^R, sk^R), (pk^S, sk^S) \leftarrow \mathtt{DRE.gen}(1^\lambda)$ and $c \leftarrow \mathtt{DRE.enc}(pk^R, pk^S, m)$.

The strongest security definition for DRE schemes mimics the IND-CCA2 definition for PKE schemes but additionally allows the adversary to choose for which receiver the decryption oracle is supposed to decrypt a ciphertext.

Definition 5 (IND-CCA2$_{\mathbf{DRE}}$). A DRE scheme satisfies indistinguishability under adaptive chosen ciphertext attack (IND-CCA2$_{\mathrm{DRE}}$), if any PPT algorithm $\mathcal{A}$ wins the IND-CCA2$_{\mathrm{DRE}}$ game in Figure 2 with probability at most $\frac{1}{2}+\mathtt{negl}(\lambda)$, i. e. the advantage

$$\mathsf{Adv}^{\text{IND-CCA2}_{\mathrm{DRE}}}_{\mathtt{DRE},\mathcal{A}}(\lambda) \coloneqq \left| \mathbb{P}\left[\mathsf{Exp}^{\text{IND-CCA2}_{\mathrm{DRE}}}_{\mathtt{DRE},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right| \leq \mathtt{negl}(\lambda)\,.$$

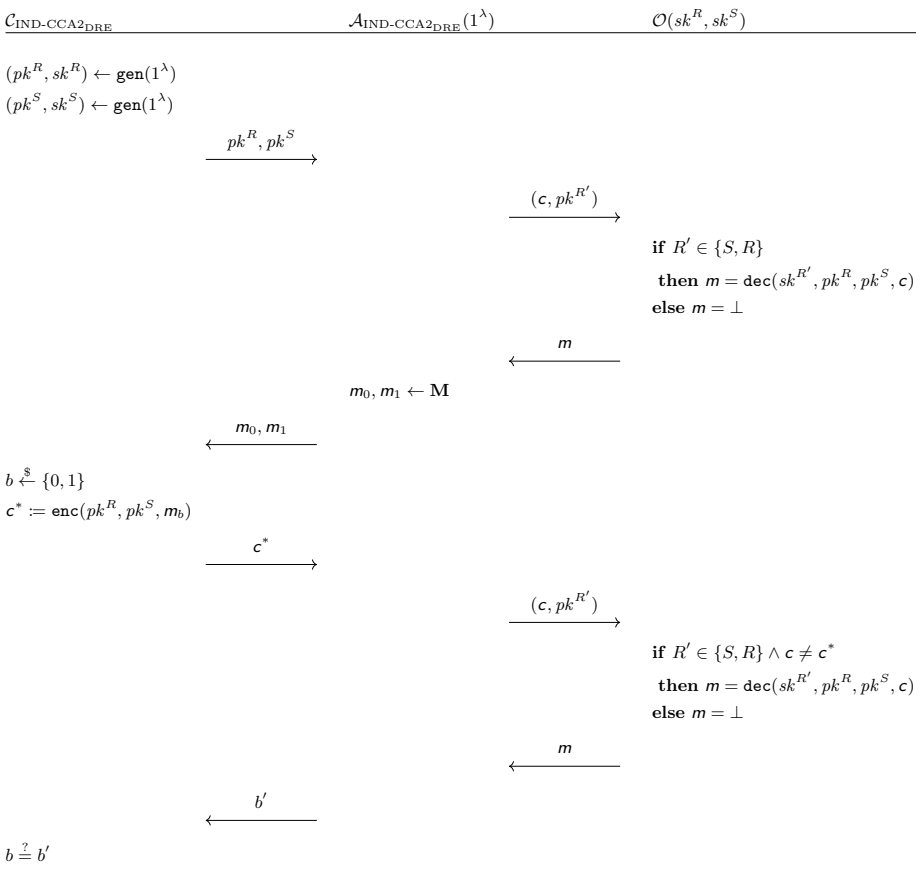

Fig. 2. Depiction of the IND-CCA2$_{\mathrm{DRE}}$ game.

While multiple DRE schemes are defined in the literature, few of them satisfy the important soundess property.

Definition 6 (Soundness for DRE). A DRE scheme $\mathtt{DRE}$ is said to be sound, if the advantage $\mathsf{Adv}^{\mathrm{sound}}_{\mathtt{DRE},\mathcal{A}}$ is negligible small, where

$$\mathsf{Adv}^{\mathrm{sound}}_{\mathtt{DRE},\mathcal{A}}(\lambda) \coloneqq \mathbb{P}\left[\mathtt{DRE.dec}(sk^R, pk^R, pk^S, c) \neq \mathtt{DRE.dec}(sk^S, pk^R, pk^S, c)\right]$$

with $(pk^R, sk^R), (pk^S, sk^S) \leftarrow \texttt{DRE.gen}(1^\lambda)$ and $c \leftarrow \mathcal{A}(sk^R, sk^S, pk^R, pk^S)$.

We also look at a special version of KEM. Introduced by Benz *et al.* [6] this adaptation binds ciphertexts to the sender which allows different security notions.

Definition 7 (SB-KEM, [6]). A sender-binding key encapsulation mechanism (SB-KEM) is given by a set of three PPT algorithms $(\texttt{gen}, \texttt{enc}, \texttt{dec})$:

- $\texttt{gen}(1^\lambda) \to (pk, sk)$: The randomized *key generation algorithm* generates a public/secret key pair.
- $\texttt{enc}(pk, \mathcal{S}) \to (K, c)$: The randomized *encryption algorithm* takes as input a public key and a sender identity and outputs a symmetric key K and a ciphertext c.
- $\texttt{dec}(sk, pk, \mathcal{S}, c) \to K$: The deterministic *decryption algorithm* takes as input a public/secret key pair, a sender identity and a ciphertext and returns the symmetric key K.

such that correctness holds, which means $K = \texttt{dec}(sk, pk, \mathcal{S}, c)$ for honestly generated $(pk, sk) \leftarrow \texttt{gen}(1^\lambda)$ and $(K, c) \leftarrow \texttt{enc}(pk, \mathcal{S})$.

The state of the art security definition for a SB-KEM scheme can be seen as a middle ground between IND-CPA and IND-CCA2. This allows for more efficient constructions while still giving most of the benefits of IND-CCA2 like realizing secure channels [6].

Definition 8 (IND-SB-CPA$_{\text{SB-KEM}}$, [6]). A SB-KEM $\Gamma = (\texttt{gen}, \texttt{enc}, \texttt{dec})$ with the set of Party IDs $\mathbf{P}$ satisfies IND-SB-CPA$_{\text{SB-KEM}}$ security, if for any PPT adversary $\mathcal{A}$ the advantage $\mathsf{Adv}^{\text{IND-SB-CPA}_{\text{SB-KEM}}}_{\mathcal{A},\Gamma}(1^\lambda) := \left|\mathbb{P}\left[b = b^*\right] - \frac{1}{2}\right|$ of winning the IND-SB-CPA game shown in Figure 3 is negligible in λ.

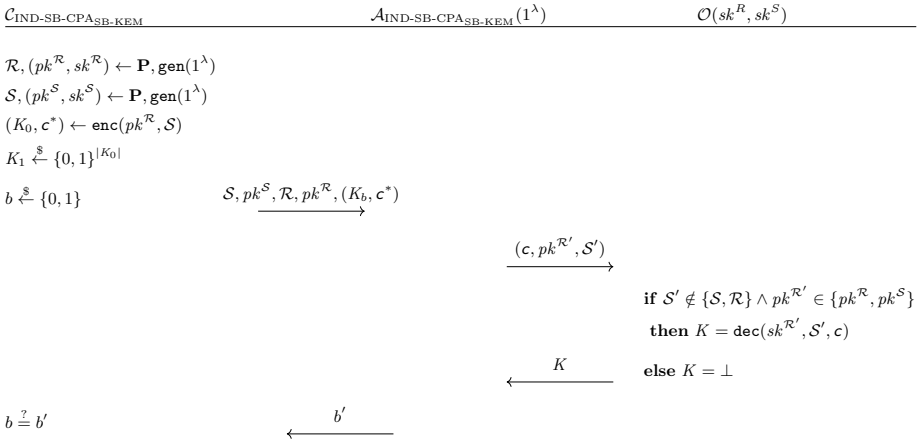

Fig. 3. Depiction of the IND-SB-CPA$_{\text{SB-KEM}}$ game.

Commitment schemes are used in our construction to prevent malicious manipulations of ciphertexts. They can be constructed from many different assumptions with many different properties. See for example the work by Alkadri, Demirel, and El Bansarkhani [2] for more information.

Definition 9 (Commitment scheme). A commitment scheme is a set of three PPT algorithms $\mathtt{COM} = (\mathtt{COM.gen}, \mathtt{COM.com}, \mathtt{COM.unveil})$:

- $\mathtt{COM.gen}(1^\lambda) \to ck$: The randomized *key generation algorithm* generates a commitment key ck.
- $\mathtt{COM.com}(ck, m) \to (c, d)$: The randomized *commitment algorithm* takes as input a commitment key ck and a message m to generate a commitment c together with decommitment information d.
- $\mathtt{COM.unveil}(ck, c, d) \to m$: The deterministic *unveil algorithm* takes a commitment key ck, a commitment c and decommitment information d and outputs a message m.

We require that for all $ck \leftarrow \mathtt{COM.gen}(1^\lambda)$ and $(c, d) \leftarrow \mathtt{COM.com}(ck, m)$ we have

$$m = \mathtt{COM.unveil}(ck, c, d)\,.$$

Our commitment scheme has to satisfy computationally hiding and statistically binding as defined in the following two definitions.

Definition 10 (Hiding). A commitment scheme $\mathtt{COM}$ is said to be computationally hiding, if for every PPT attacker $\mathcal{A}$ the advantage

$$\mathsf{Adv}^{\text{Hiding}}_{\mathtt{COM},\mathcal{A}} := \left| \mathbb{P}\left[\mathsf{Exp}^{\text{Hiding}}_{\mathtt{COM},\mathcal{A}}(1^\lambda)\right] - \frac{1}{2} \right|$$

in the hiding experiment in Figure 4 is negligible.

$\mathsf{Exp}^{\text{Hiding}}_{\mathtt{COM},\mathcal{A}}(1^\lambda)$

$ck \leftarrow \mathtt{COM.gen}(1^\lambda)$
$(m_0, m_1, state) \leftarrow \mathcal{A}(1^\lambda, ck, \text{find})$
$b \xleftarrow{\$} \{0, 1\}$
$(c, d) \leftarrow \mathtt{COM.com}(ck, m_b)$
$b' \leftarrow \mathcal{A}(1^\lambda, \text{guess}, state, c)$
return $b \stackrel{?}{=} b'$

Fig. 4. Hiding experiment.

Definition 11 (Binding). A commitment scheme $\mathtt{COM}$ is said to be statistically binding if there is a negligible function $\mathtt{negl}$ such that

$$\mathop{\mathbb{P}}_{\substack{ck \leftarrow \mathtt{COM.gen}(1^\lambda) \\ (c,d_0) \leftarrow \mathtt{COM.com}(ck, m_0)}} \left[\exists (m_1, d_1) \;\middle|\; \begin{array}{l} m_0 \neq m_1, \\ \mathtt{COM.unveil}(ck, c, d_1) = m_1 \end{array} \right] \leq \mathtt{negl}(1^\lambda) \,.$$

As our constructions are defined as hybrid encryption schemes we need symmetric encryption primitives as well. Our security definitions are very weak and yet enough to realize the strong security notions for our constructions.

Definition 12 (SKE). A secret-key encryption (SKE) scheme is a pair of PPT algorithms $\mathtt{SKE} = (\mathtt{SKE.enc}, \mathtt{SKE.dec})$ with key space $\mathbf{K}_{\mathtt{SKE}}$ and ciphertext space $\mathbf{C}_{\mathtt{SKE}}$ satisfying

- $\mathtt{SKE.enc}(dk, m) \to c$: The randomized *encryption algorithm* takes as input a key $dk \in \mathbf{K}_{\mathtt{SKE}}$ and a message m, and outputs a ciphertext c.
- $\mathtt{SKE.dec}(dk, c) \to m$: The deterministic *decryption algorithm* takes as input a key $dk \in \mathbf{K}_{\mathtt{SKE}}$ and a ciphertext c, and outputs a message m (which may be the special symbol $\perp$)

We require that for all $dk \in \mathbf{K}_{\mathtt{SKE}}$ it holds that

$$m = \mathtt{SKE.dec}(dk, \mathtt{SKE.enc}(dk, m)) \,.$$

As each encryption in the hybrid encryption draws a new symmetric key, we require only one-time indistinguishability.

Definition 13 (OT-IND). A SKE scheme $\mathtt{SKE}$ is said to be secure under one-time indistinguishability (OT-IND), if the advantage $\mathsf{Adv}^{\text{OT-IND}}_{\mathtt{SKE},\mathcal{A}}$ of any PPT adversary $\mathcal{A}$ is negligible, where

$$\mathsf{Adv}^{\text{OT-IND}}_{\mathtt{SKE},\mathcal{A}}(\lambda) := \left| \mathbb{P}\left[\mathcal{A}(1^\lambda, \text{guess}, state, \Phi_b) = b\right] - \frac{1}{2} \right| \leq \mathtt{negl}(1^\lambda)$$

with $dk \xleftarrow{\$} \mathbf{K}_{\mathtt{SKE}}, b \xleftarrow{\$} \{0,1\}, \Phi_0 \leftarrow \mathtt{SKE.enc}(dk, m), \Phi_1 \xleftarrow{\$} \mathbf{C}_{\mathtt{SKE}}$ and $(m, state) \leftarrow \mathcal{A}(1^\lambda, \text{mesg})$.

We also require message authentication codes to prevent tampering of the messages.

Definition 14 (MAC). A message authentication code (MAC) scheme $\mathtt{MAC}$ with key space $\mathbf{K}_{\mathtt{MAC}}$ consists of the two PPT algorithms $\mathtt{MAC} = (\mathtt{MAC.sign}, \mathtt{MAC.verify})$, where

- $\mathtt{MAC.sign}(mk, m) \to \tau$: The randomized *signing algorithm* takes as input a signing key $mk \in \mathbf{K}_{\mathtt{MAC}}$ and a message m, and outputs a tag τ.
- $\mathtt{MAC.verify}(mk, m, \tau) \to \{0,1\}$: The deterministic *verification algorithm* takes as input a signing key $mk \in \mathbf{K}_{\mathtt{MAC}}$, a message m and a tag τ, and outputs 1 if τ is a possible output of $\mathtt{MAC.sign}(mk, m)$.

Again, each encryption draws a new key and thus, one-time strongly unforgeability is enough.

Definition 15 (OT-SUF). A MAC scheme $\mathtt{MAC}$ is one-time strongly unforgeable (OT-SUF) if the advantage $\mathsf{Adv}^{\text{OT-SUF}}_{\mathtt{MAC},\mathcal{A}}$ of any PPT adversary $\mathcal{A}$ is negligible, where

$$\mathsf{Adv}^{\text{OT-SUF}}_{\mathtt{MAC},\mathcal{A}}(\lambda) \coloneqq \mathbb{P}\left[\begin{array}{l|l} \mathtt{MAC.verify}(mk,\tau') = 1 & \tau \leftarrow \mathtt{MAC.sign}(mk, m) \\ \tau' \neq \tau & \tau' \leftarrow \mathcal{A}(1^\lambda, \text{forge}, state, \tau) \end{array}\right]$$

with $mk \xleftarrow{\$} \mathbf{K}_{\mathtt{MAC}}$, $(m, state) \leftarrow \mathcal{A}(1^\lambda, \text{sign})$.

A hash function $\mathtt{H}$ is used to map an arbitrary input to a specific output format. In our case we only need a very basic property of our hash functions called collision resistance.

Definition 16 (Collision Resistance). A family of hash functions $\{\mathtt{H}_k\}_{k\in\mathbf{K}}$ is said to be collision resistant (CR) if for all PPT algorithms $\mathcal{A}$ the advantage $\mathsf{Adv}^{\text{CR}}_{\mathtt{H},\mathcal{A}}(\lambda)$ is negligibly small, where

$$\mathsf{Adv}^{\text{CR}}_{\mathtt{H},\mathcal{A}}(\lambda) \coloneqq \mathbb{P}\left[k \xleftarrow{\$} \mathbf{K}, (x, x') \leftarrow \mathcal{A}(1^\lambda, \mathtt{H}_k) : x \neq x' \text{ and } \mathtt{H}(x) = \mathtt{H}(x')\right].$$

We need to look at keyed hash functions, as for every fixed hash function there exists an adversary with a collision hard coded by the pigeonhole principle. Still, in a slight abuse of notation we will speak of a "collision resistant hash function", by which we mean a function sampled uniformly from a collision resistant hash function family.

We also use a key derivation function $\mathtt{KDF} : \{0,1\}^n \to \mathbf{K}$ to generate keys for the $\mathtt{SKE}$- and $\mathtt{MAC}$-schemes from a short seed.

Definition 17 (IND KDF [9]). A key derivation function (KDF) $\mathtt{KDF} : \{0,1\}^n \to \mathbf{K}$ satisfies indistinguishability (IND) security if for all PPT algorithms $\mathcal{A}$ the advantage $\mathsf{Adv}^{\text{IND}}_{\mathtt{KDF},\mathcal{A}}(\lambda)$ is negligibly small, where

$$\mathsf{Adv}^{\text{IND}}_{\mathtt{KDF},\mathcal{A}}(\lambda) \coloneqq \left|\mathbb{P}\left[\mathcal{A}(1^\lambda, \mathtt{KDF}(k)) = 1\right] - \mathbb{P}\left[\mathcal{A}(1^\lambda, r) = 1\right]\right|$$

for $k \xleftarrow{\$} \{0,1\}^n$ and $r \xleftarrow{\$} \mathbf{K}$.

The last primitive we need are full-rank difference encodings which enables us to hide game changes in our hybrid proof later on.

Definition 18 (Full-rank difference encoding [7]). Let $\mathbf{S}$ be a set, R the ring of integers of a number field K and q a modulo. A function $\mathtt{FRD} : \mathbf{S} \to R_q$ is a full rank difference encoding (FRD), if it satisfies the following three properties:

(1) For all $x \in \mathbf{S}$, $\mathtt{FRD}(x)$ is invertible
(2) For all $x, y \in \mathbf{S}$ with $x \neq y$, the element $\mathtt{FRD}(x) - \mathtt{FRD}(y)$ is invertible
(3) $\mathtt{FRD}$ is computable in polynomial time

3 DRE Construction

We now turn towards the new DRE construction based on NRLWE.

We describe two variants of the scheme: the *computational variant* and the *statistical variant*. The difference is in the public key, which is either computationally or statistically indistinguishable from uniform. This yields different bounds on the advantage of adversaries on the scheme and different limitations for the parameters.

Let R be the ring of integers with order $n \in \mathbb{N}$ as in Section 2, $q \in \mathbb{N}$ a modulo, $J_q = \sigma(R)/q\sigma(R) \subseteq H/qH$ and J_q^* the invertible elements in J_q. Denote with Λ the lattice of the embedded ring $\Lambda \coloneqq \psi(\sigma(R)) \subseteq \mathbb{R}^n$ and with $B_\Lambda = \{\psi(\sigma(1)), \psi(\sigma(X)), \dots, \psi(\sigma(X^{n-1}))\} \subseteq \mathbb{R}^n$ the basis of Λ.

Take parameters $l \coloneqq \lceil \log q \rceil$ and $m \in \mathbb{N}, m \geq 2$. We use the gadget vector $g \in J_q^l$ with its `invert` function and the Gram-Schmidt orthogonalized basis $\tilde{B_g} \in R_q^{l \times l}$ of $\Lambda_q^\perp(g)$ as defined in Section 2.3. Additional building tools are a commitment scheme `COM`, a SKE `SKE`, a MAC `MAC`, a KDF `KDF`, a hash function $\mathtt{H} : \{0,1\}^* \to \{0,1\}^\nu$ and a FRD $\mathtt{FRD} : \{0,1\}^\nu \to J_q^*$ for some $\nu \in \mathbb{N}$.

For the statistical variant take a $\beta_T > \sqrt{2\pi^{-1}} n \cdot q^{1/m+2/(mn)}$, while for the computational variant choose $\beta_T \in \mathbb{R}$ such that $\mathrm{NRLWE}_{1,q,\chi_2}$ with $\chi_2 = \psi^{-1}(\mathcal{D}_{\Lambda,t\beta_T})$ is hard. Let $t \in \mathbb{R}^+$ be such that for any diagonal matrix $\Sigma \in \mathbb{R}_{\geq 0}^{n \times n}$ we have

$$\delta := \mathbb{P}\left[\|x\|_2 > \|\sqrt{\Sigma}\|_2 \cdot \frac{1}{t} \cdot \sqrt{n} \mid x \leftarrow \mathcal{D}_{\Lambda,\sqrt{\Sigma}}\right] \leq \epsilon(n) \tag{2}$$

for some negligible function ϵ, which exists by Lemma 2. Finally, take $\alpha \in \mathbb{R}$ with

$$\frac{1}{\alpha} \geq 2\beta_T \left\| \tilde{B_g}^T \right\|_{\varphi,\infty} \cdot \|B_\Lambda^{-1}\|_2 \cdot \sqrt{nm}\left(\sqrt{nm} + \sqrt{n+1}\right) \text{ and} \tag{3}$$

$$\frac{1}{\alpha} \geq 4\left\|B_\Lambda^{-1}\right\|_2 \cdot \sqrt{n} \tag{4}$$

such that $q \geq (\sqrt{2\pi} \cdot \alpha t \beta_T \sqrt{m})^{-1} \cdot \sqrt{n} \cdot \omega(\sqrt{\log n})$ for some superlogarithmic function $\omega(\sqrt{\log n})$ and $\mathrm{NRLWE}_{2m,q,\chi_1}$ with $\chi_2 = \psi^{-1}(\mathcal{D}_{\Lambda,tq\alpha})$ is hard.

For a canonically embedded ring element $e = (e_1, \dots, e_n) \in J$ we write $Mul(e) \in \mathbb{R}^{n \times n}$ for the diagonal matrix with $|e_i|^2$ at the i-th diagonal entry. For a vector v of ring elements we write $Mul(v) \coloneqq \sum_i Mul(v_i) \in \mathbb{R}^{n \times n}$. Also, calculations with elements in J are performed in J_q.

An overview of the used parameters can be found in Table 1.

Symbol	Constraints	Meaning
K	$K = \mathbb{Q}[\zeta]$	The used cyclotomic number field
n	$n \in \mathbb{N}$	The dimension of K
R	$R = \mathbb{Z}[X]/f(X)$	The ring of integers of K
q	$q \in \mathbb{N}$	The used modulo
R_q	$R_q = \mathbb{Z}_q[X]/f(x)$	The ring of the integers of the cyclotomic number field K modulo q
σ	$\sigma : K \to H$	The canonical embedding
φ	$\varphi : K \to \mathbb{Q}^n$	The coefficient embedding
ψ	$\psi : H \to \mathbb{R}^n$	The isomorphism from $H \subseteq \mathbb{C}^n$ to $\mathbb{R}^n$
J_q	$J_q = \sigma(R)/q\sigma(R)$	The canonically embedded ring of integers modulo q
J_q^*	$J_q^* \subseteq J_q$	The invertible elements of J_q
Λ	$\Lambda = \psi(\sigma(R))$	The ring of integers embedded into $\mathbb{R}^n$ interpreted as a lattice
B_Λ	$B_\Lambda \subseteq \mathbb{R}^n$	Basis of Λ
α	$\alpha \in \mathbb{R}$ $\frac{1}{\alpha} \geq 2\beta_T \left\|\tilde{B_g}^T\right\|_{\varphi,\infty} \|B_\Lambda^{-1}\|_2 \cdot \sqrt{nm}\left(\sqrt{nm} + \sqrt{n+1}\right)$ $\frac{1}{\alpha} \geq 4\left\|B_\Lambda^{-1}\right\|_2 \sqrt{n}$	Parameter for the width of the discrete Gaussian of $\bar{s}$ and e_1
β_T	$\beta_T \in \mathbb{R}$	Parameter for the width of the discrete Gaussian for the trapdoor
l	$l = \lceil \log q \rceil$	The dimension of the gadget vector and one of the dimensions of the trapdoor
m	$m \geq 2$	The primary dimension of the keys
g	$g = (1, 2, \ldots, 2^{l-1}) \in J_q^l$	The gadget vector by Micciancio and Peikert [25]
$\tilde{B_g}$	$\tilde{B_g} \in R_q^{l \times l}$	Gram-Schmidt orthogonalization of the basis of $\Lambda_q^\perp(g)$
δ	$\delta = \underset{x \leftarrow \mathcal{D}_{\Lambda,\sqrt{\Sigma}}}{\mathbb{P}}\left[\|x\|_2 > \frac{1}{t}\sqrt{n}\|\sqrt{\Sigma}\|_2\right]$	Probability for a Gaussian drawn vector to be to large. Should be negligible
t	$t \in \mathbb{R}$	Parameter, such that δ is negligible or small enough
A_e	$A_e \in \mathbb{R}^{n \times n}$	For $e, t \in H$, A_e is the matrix that satisfies $A_e\psi(t) = \psi(e \odot t)$
$Mul(e)$	$Mul(e) \in \mathbb{R}^{n \times n}$	For $e \in J$, $Mul(e)$ is the diagonal matrix with $\lvert e_i \rvert$ on its $i-th$ diagonal entry

Table 1. Overview of the used notation

We also employ a commitment scheme that was absent in the previous work of Benz *et al.* [5]. This addition is needed because RLWE samples are not unique for commonly used parameters. It can be omitted if the parameters are chosen in such a way that Lemma 7 applies to c_1 of our scheme. Then the used key is uniquely determined by c_1 with overwhelming probability, making the use of `COM` obsolete. While the resulting parameter sets can be found in Appendix C, we now focus on the scheme using commitments.

With all this, we can now define the DRE $\mathtt{DRE} = (\mathsf{KGen}, \mathtt{Enc}, \mathtt{Dec})$ in Figure 5.

$\mathsf{KGen}(1^\lambda)$

1 : $a_0 \xleftarrow{\$} J_q^*, a' \xleftarrow{\$} J_q^{m-1}, T \leftarrow \psi^{-1}(\mathcal{D}_{\Lambda,t\beta_T}^{l\times m})$
2 : $ck \leftarrow \mathtt{COM.gen}(1^\lambda), a \coloneqq (a_0, a')$
3 : **return** $(pk, sk) \coloneqq ((a, Ta, ck), T)$

$\mathtt{Enc}(pk^R, pk^S, m)$

1 : parse $pk^R = (a^R, a_1^R, ck^R)$
2 : parse $pk^S = (a^S, a_1^S, ck^S)$
3 : $k \xleftarrow{\$} \{0,1\}^n$
4 : $(mk, dk) \coloneqq \mathtt{KDF}(k)$
5 : $(c_0^R, d^R) \leftarrow \mathtt{COM.com}(ck^R, k)$
6 : $(c_0^S, d^S) \leftarrow \mathtt{COM.com}(ck^S, k)$
7 : $c_0 \coloneqq (c_0^R, c_0^S), d \coloneqq (d^R, d^S)$
8 : $\bar{s} \leftarrow \psi^{-1}(\mathcal{D}_{\Lambda,tq\alpha})$
9 : $s \coloneqq \psi^{-1}\left(B_\Lambda\left(\frac{q}{2}\cdot d\right)\right) + \bar{s} \in J_q$
10 : $e_1^R, e_1^S \leftarrow \psi^{-1}(\mathcal{D}_{\Lambda,tq\alpha}^m)$
11 : $c_1 \coloneqq (a^R s + e_1^R, a^S s + e_1^S)$
12 : $\Sigma^R \coloneqq t^2\beta_T^2 Mul(e_1^R) + t^2\beta_T^2 m(q\alpha)^2 I_n$
13 : $\Sigma^S \coloneqq t^2\beta_T^2 Mul(e_1^S) + t^2\beta_T^2 m(q\alpha)^2 I_n$
14 : $e_2^R \leftarrow \psi^{-1}(\mathcal{D}_{\Lambda,\Sigma^R}^l), e_2^S \leftarrow \psi^{-1}(\mathcal{D}_{\Lambda,\Sigma^S}^l)$
15 : $c_2 \coloneqq ((a_1^R + g\cdot \mathtt{FRD}(\mathtt{H}(c_0, c_1)))s + e_2^R, (a_1^S + g\cdot \mathtt{FRD}(\mathtt{H}(c_0, c_1)))s + e_2^S)$
16 : $\Delta \leftarrow \mathtt{SKE.enc}(dk, m)$
17 : $\tau \leftarrow \mathtt{MAC.sign}(mk, (c_0, c_1, c_2, \Delta))$
18 : **return** $(c_0, c_1, c_2, \Delta, \tau)$

$\mathtt{Dec}(sk^R, pk^R, pk^S, c)$

1 : parse $sk^R = T$
2 : parse $pk^R = (a^R, a_1^R, ck^R)$
3 : parse $pk^S = (a^S, a_1^S, ck^S)$
4 : parse $c = (c_0^R, c_0^S, c_1^R, c_1^S, c_2^R, c_2^S, \Delta, \tau)$
5 : $(s, (e_1^R, e_2^R)) \coloneqq \mathtt{invert}(T, \mathtt{FRD}(\mathtt{H}(c_0, c_1)), (a^R, (a_1^R + g\cdot \mathtt{FRD}(\mathtt{H}(c_0, c_1)))), (c_1^R, c_2^R))$
6 : **if** $\left\| \left[e_1^R\right]_{\sigma,2} \right\|_\infty > q\alpha\sqrt{n}$: **return** $\perp$
7 : **if** $\left\| \left[e_2^R\right]_{\sigma,2} \right\|_\infty > q\alpha\beta_T\sqrt{n(n+1)m}$: **return** $\perp$
8 : $e_1^S \coloneqq c_1^S - a^S s$
9 : $e_2^S \coloneqq c_2^S - (a_1^S + g\cdot \mathtt{FRD}(\mathtt{H}(c_0, c_1)))s$
10 : **if** $\left\| \left[e_1^S\right]_{\sigma,2} \right\|_\infty > q\alpha\sqrt{n}$: **return** $\perp$
11 : **if** $\left\| \left[e_2^S\right]_{\sigma,2} \right\|_\infty > q\alpha\beta_T\sqrt{n(n+1)m}$: **return** $\perp$
12 : $d \coloneqq (d^R, d^S) \coloneqq \frac{2}{q}\cdot \lfloor B_\Lambda^{-1}\psi(s)\rceil_{q/2}$
13 : **if** $\left\|\psi(s) - \frac{q}{2}B_\Lambda\cdot d\right\|_2 > q\alpha\sqrt{n}$: **return** $\perp$
14 : $k \coloneqq \mathtt{COM.unveil}(ck^R, c_0^R, d^R)$
15 : **if** $k \neq \mathtt{COM.unveil}(ck^S, c_0^S, d^S)$: **return** $\perp$
16 : $(mk, dk) \coloneqq \mathtt{KDF}(k)$
17 : **if** $\mathtt{MAC.verify}(mk, (c_0, c_1, c_2, \Delta), \tau) \neq 1$: **return** $\perp$
18 : $m \coloneqq \mathtt{SKE.dec}(dk, \Delta)$
19 : **return** m

Fig. 5. NRLWE based DRE

To prove correctness and security we need the following lemma which bounds the smoothing parameter in terms of the Gaussian parameters.

Lemma 8. *For the parameters of the DRE* `DRE`*,* $\Sigma_f := \Sigma^i \in \mathbb{R}^{n\times n}$*,* $e = (e_1, \dots e_m) := e_1^i \in J_q^m$ *with* $i \in \{R, S\}$ *and* $\epsilon = \epsilon(n) > 0$ *negligible, it holds that*

$$\eta_\epsilon(\Lambda) \leq \sqrt{2\pi}\sqrt{\Sigma_f},$$
$$\eta_\epsilon(\Lambda) \leq \sqrt{2\pi}t\beta_T\sqrt{m}q\alpha \text{ and}$$
$$\eta_\epsilon(\Lambda) \leq \sqrt{2\pi}A_{e_\nu}^{-1}\sqrt{\left(\Sigma_f^{-1} + (t^2\beta_T^2 A_{e_\nu}A_{e_\nu}^T)^{-1}\right)^{-1}}$$

for $1 \leq \nu \leq m$ *where* $e_\nu \neq 0$.

The proof can be found in Appendix A.

Theorem 1. *The DRE* `DRE` *from Figure 5 is correct with overwhelming probability over the errors.*

Proof. The proof of correctness requires two things. First, `invert` needs to return the correct s. Second, the errors need to be small enough, such that the checks do not fail and k can be recovered from s and c_0. The rest follows from the correctness of `SKE` and `MAC`. We consider the decryption for R, the decryption for S is analogous.

As stated in Lemma 5, the `invert` function returns the correct s if

$$\sigma^{-1}\left(Te_1^R + e_2^R\right) \in q \cdot \mathcal{P}_{1/2}(\tilde{B_g}^{-T}) \tag{5}$$

holds, where $\tilde{B}_g \in R_q^{l\times l}$ is the Gram-Schmidt orthogonalization of the basis of $\Lambda_q^\perp(g)$. This is equivalent to

$$\left\|\tilde{B_g}^T \sigma^{-1}\left(Te_1^R + e_2^R\right)\right\|_{\varphi,\infty} \leq \frac{q}{2}.$$

By Lemmas 3 and 8 each entry of $Te_1^R + e_2^R \in J_q^l$ is distributed as $\psi^{-1}(\mathcal{D}_{\Lambda,\sqrt{\Sigma}})$, where $\Sigma = t^2\beta_T^2 Mul(e_1^R) + \Sigma^R$. Using the definitions of Σ^R and $Mul(e_1^R)$ and

$$(r_1)^2 := \beta_T^2 \cdot \max_j Mul(e_1^R)_{j,j} \in \mathbb{R}^+$$
$$(r_2)^2 := \beta_T^2 \cdot \max_j Mul(e_1^R)_{j,j} + \beta_T^2 m(q\alpha)^2 \in \mathbb{R}^+$$
$$r^2 := (r_1)^2 + (r_2)^2,$$

it holds that

$$\Sigma \leq t^2 r^2 I_n,$$

where $\leq$ is on every entry. As each entry of $e_1^R \in J_q^m$ is drawn by a discrete Gaussian, Equation (2) yields

$$\left|(e_1^R)_{i,j}\right| \leq \left\|(e_1^R)_i\right\|_{\sigma,2} \leq \sqrt{n}q\alpha$$

and thus

$$(r_1)^2 \leq \beta_T^2 mn(q\alpha)^2 \tag{6}$$
$$(r_2)^2 \leq \beta_T^2 mn(q\alpha)^2 + \beta_T^2 m(q\alpha)^2 = \beta_T^2(n+1)m(q\alpha)^2 \tag{7}$$

with overwhelming probability. By Equation (2) again, each element of $Te_1^R + e_2^R$ has 2-norm at most $r\sqrt{n}$ and therefore

$$\left\|\left[Te_1^R + e_2^R\right]_{\sigma,2}\right\|_\infty \leq r\sqrt{n} \leq \beta_T q\alpha\sqrt{n(2n+1)m}$$

with overwhelming probability. This yields

$$\begin{aligned}\left\|\tilde{B_g}^T\sigma^{-1}(Te_1^R + e_2^R)\right\|_{\varphi,\infty} &\leq \left\|\tilde{B_g}^T\right\|_{\varphi,\infty} \cdot \left\|\left[Te_1^R + e_2^R\right]_{\varphi,2}\right\|_\infty \\ &\leq \left\|\tilde{B_g}^T\right\|_{\varphi,\infty} \cdot \left\|B_\Lambda^{-1}\right\|_2 \cdot \left\|\left[Te_1^R + e_2^R\right]_{\sigma,2}\right\|_\infty \\ &\leq \left\|\tilde{B_g}^T\right\|_{\varphi,\infty} \cdot \left\|B_\Lambda^{-1}\right\|_2 \cdot \beta_T q\alpha\sqrt{n(2n+1)m} \overset{(*)}{\leq} \frac{q}{2}.\end{aligned}$$

The last inequality (*) holds because

$$\begin{aligned}\frac{1}{\alpha} &\overset{(3)}{\geq} 2\beta_T \cdot \left\|\tilde{B_g}^T\right\|_{\varphi,\infty} \cdot \left\|B_\Lambda^{-1}\right\|_2 \cdot \sqrt{nm}\left(\sqrt{nm} + \sqrt{n+1}\right) \\ &\geq 2\beta_T \cdot \left\|\tilde{B_g}^T\right\|_{\varphi,\infty} \cdot \left\|B_\Lambda^{-1}\right\|_2 \cdot \sqrt{n(2n+1)m}.\end{aligned}$$

Thus, the errors are small enough with overwhelming probability so that Equation (5) holds and `invert` returns the correct s.

The norm checks for e_1^R and e_1^S in the decryption (line 6 and 10) hold by Equation (2) with overwhelming probability. The norm checks for e_2^R and e_2^S (line 7 and 11) follow from Equations (2) and (7).

For the norm on $\bar{s} \in J_q$, by Equation (2), we have $\|\bar{s}\|_2 \leq q\alpha\sqrt{n}$ with overwhelming probability. This implies two facts. First, the correct seed k can be recovered in lines 12 and 14 with overwhelming probability by the correctness of `COM` and because

$$\left\|B_\Lambda^{-1}\bar{s}\right\|_\infty \leq \left\|B_\Lambda^{-1}\bar{s}\right\|_2 \leq \left\|B_\Lambda^{-1}\right\|_2 \cdot \|\bar{s}\|_2 \leq \left\|B_\Lambda^{-1}\right\|_2 \cdot q\alpha\sqrt{n} \overset{(4)}{\leq} \frac{q}{4}.$$

Second, the last norm check in line 13 succeeds with overwhelming probability.□

Having shown the correctness of the scheme we turn towards proving soundness.

Theorem 2. *The DRE* $\mathtt{DRE}$ *from Figure 5 is sound as in Definition 6.*

Proof. We need to show that no PPT adversary can produce a cipher c that decrypts to two different messages even given both secret keys. As this means that at least one of the two receivers will decrypt c to some message $\mathsf{m} \neq \perp$, we assume without loss of generality that $\mathtt{Dec}(sk^R, pk^R, pk^S, \mathsf{c}) \neq \perp$. Thus, we know that the error checks for R succeed and therefore it holds that $\mathsf{c}_1^S = a^S s + e_1^S$ for an $e_1^S \in J_q^m$ with $\left\| [e_1^S]_{\sigma,2} \right\|_\infty \leq q\alpha\sqrt{n}$. Similarly, we know that $\mathsf{c}_2^S = (a_1^S + g \cdot \mathtt{FRD}(\mathtt{H}(\mathsf{c}_0, \mathsf{c}_1)))s + e_2^S$ for an $e_2^S \in J_q^l$ with $\left\| [e_2^S]_{\sigma,2} \right\|_\infty \leq q\alpha\beta_T\sqrt{n(n+1)m}$.

As each entry of T is drawn by a discrete Gaussian, Equation (2) yields $\left\| [T]_{\sigma,2} \right\|_\infty \leq m\|T_{i,j}\|_{\sigma,2} \leq m\sqrt{n}\beta_T$ with overwhelming probability and thus

$$\begin{aligned}\left\| [Te_1^S]_{\sigma,2} \right\|_\infty &\leq \left\| [T]_{\sigma,2} \right\|_\infty \cdot \left\| [e_1^S]_{\sigma,2} \right\|_\infty \\ &\leq \frac{q\sqrt{nm}}{2 \cdot \left\| \tilde{B_g}^T \right\|_{\varphi,\infty} \cdot \left\| B_\Lambda^{-1} \right\|_2 \cdot (\sqrt{nm} + \sqrt{n+1})}.\end{aligned}$$

Combining the bounds on e_2^S and α yields

$$\left\| [e_2^S]_{\sigma,2} \right\|_\infty \leq \frac{q\sqrt{n+1}}{2 \cdot \left\| \tilde{B_g}^T \right\|_{\varphi,\infty} \cdot \left\| B_\Lambda^{-1} \right\|_2 \cdot (\sqrt{nm} + \sqrt{n+1})}.$$

Therefore, S recovers the correct s from `invert` by Lemma 5 as

$$\left\| \tilde{B_g}^T (Te_1^S + e_2^S) \right\|_{\varphi,\infty} \leq \left\| \tilde{B_g}^T \right\|_{\varphi,\infty} \cdot \left\| B_\Lambda^{-1} \right\|_2 \cdot \left\| [Te_1^S + e_2^S]_{\sigma,2} \right\|_\infty \leq \frac{q}{2}.$$

As all other steps of the decryption depend deterministically on s and the cipher, S recovers the same message m. □

For the security proof we need that the public key is indistinguishable from uniform randomness. For the statistical variant this is statistically true, whereas for the computational variant we need the following Lemma 9.

Lemma 9. *Let* $q, m, l, \beta_T, t, a_0, a', a, T, \Lambda$ *be as in the* $\mathtt{DRE}$ *from Figure 5 and* $u \xleftarrow{\$} J_q^m$*. Then* (a, Ta) *is computationally indistinguishable from* (a, u) *if the* $NRLWE_{1,q,\chi}$ *assumption holds for* $\chi = \psi^{-1}(\mathcal{D}_{\Lambda,t\beta_T})$*. Concretely, for any adversary* $\mathcal{A}$ *on the indistinguishability between* (a, Ta) *and* (a, u)*, there is an adversary* $\mathcal{A}_{NRLWE}$ *on* $NRLWE_{1,q,\chi}$ *with*

$$\mathsf{Adv}_{\mathcal{A}}^{IND}(\lambda) \leq l \cdot \mathsf{Adv}_{\mathcal{A}_{NRLWE}}^{NRLWE_{1,q,\chi}}(\lambda).$$

Proof. First, consider $m = 2$ so that $a' \in J_q$. We use a standard hybrid proof to show that given $(a, b) \in J_q^m \times J_q^l$ no adversary can decide whether $b = u$ or $b = Ta$. In game H_i the first i rows of b are uniformly random while the

other rows are $(Ta)_j$. Thus, in the game $G_0 := H_0$ we have $b = Ta$ as in the construction and in $G_1 := H_l$, $b = u$ is completely random. If there is an adversary $\mathcal{A}_i$, which distinguishes game H_{i-1} from H_i, there is an adversary $\mathcal{A}_{\text{NRLWE}}$ on $\text{NRLWE}_{1,q,\chi}$ with $\chi = \psi^{-1}(\mathcal{D}_{\Lambda,t\beta_T})$. Given one canonically embedded NRLWE sample $(a_{\text{NRLWE}}, b_{\text{NRLWE}}) \in J_q \times J_q$, $\mathcal{A}_{\text{NRLWE}}$ embeds this sample in the i-th row and samples everything else as in game H_i. To do this, it draws $a_0 \xleftarrow{\$} J_q^*$ and sets $a = (a_0, a_0 a_{\text{NRLWE}})$[3] and for b it chooses the vector

$$(u_1, \ldots, u_{i-1}, a_0 b_{\text{NRLWE}}, t_{i+1,1}a_0 + t_{i+1,2}a_0 a_{\text{NRLWE}}, \ldots, t_{l,1}a_0 + t_{l,2}a_0 a_{\text{NRLWE}})^T$$
$$= (u_1, \ldots, u_{i-1}, a_0 b_{\text{NRLWE}}, T(a_0, a')_{[i+1;l]})^T, a' = a_0 a_{\text{NRLWE}},$$

where $T(a_0, a')_{[i+1;l]}$ are the rows $i+1, \ldots, l$ of the resulting vector. Then, $\mathcal{A}_i$ is run with input (a, b). If $b_{\text{NRLWE}} = a_{\text{NRLWE}} s + e$ for some secret $s \in J_q$ and error $e \in J_q$, the i-th row is $a's + a_0 e \sim t_{i,1}a_0 + t_{i,2}a'$ and thus, this simulates game H_{i-1}. If b_{NRLWE} is random instead, it simulates game H_i. Therefore, for any adversary $\mathcal{A}_i$ we have

$$\left| \mathbb{P}\left[\mathcal{A}_i^{H_i}(\lambda) = 1\right] - \mathbb{P}\left[\mathcal{A}_i^{H_{i-1}}(\lambda) = 1\right] \right| \leq \mathsf{Adv}^{\text{NRLWE}_{1,q,\chi}}_{\mathcal{A}_{\text{NRLWE}}}(\lambda).$$

With that, we can bound the advantage of every adversary $\mathcal{A}$ against distinguishing G_0 from G_1 as

$$\begin{aligned}
\mathsf{Adv}^{\text{IND}}_{\mathcal{A},G_0,G_1}(\lambda) &= \left| \mathbb{P}\left[\mathcal{A}^{H_l}(\lambda) = 1\right] - \mathbb{P}\left[\mathcal{A}^{H_0}(\lambda) = 1\right] \right| \\
&\leq \sum_{i=1}^{l} \left| \mathbb{P}\left[\mathcal{A}^{H_i}(\lambda) = 1\right] - \mathbb{P}\left[\mathcal{A}^{H_{i-1}}(\lambda) = 1\right] \right| \\
&\leq l \cdot \mathsf{Adv}^{\text{NRLWE}_{m,q,\chi}}_{\mathcal{A}_{\text{NRLWE}}}(\lambda).
\end{aligned}$$

As for $m > 2$ the j-th row is $(T(a_0, a'))_j = t_{j,1}a_0 + t_{j,2}a_2 + t_{j,3}a_3 + \cdots + t_{j,m}a_m$ for some $a_2, \cdots, a_m$, and $t_{j,1}a_0 + t_{j,2}a_2$ looks uniform for each j and thus, $T(a_0, a')$ looks uniformly random as claimed. □

Now we turn towards proving the security of our construction by using a series of game hops. We start with the $\text{IND-CCA2}_{\text{DRE}}$ game and slowly change parts such that we end up with a scheme where the challenge ciphertext is independent of the chosen challenge messages. Therefore, no adversary can win the resulting game with probability better than $\frac{1}{2}$. Using our previous results we are able to show that no game hop can be detected by an adversary as long as our security assumptions hold. The proof uses some ideas of Benz *et al.* [5, Theorem 6], Boyen, Izabachène, and Li [9, Theorem 1] and Kiltz, Masny, and Pietrzak [20, Theorem 2], but we have to take some extra precautions.

Theorem 3. *The DRE* `DRE` *from Figure 5 is* IND-CCA2_{DRE}*-secure if the problem* $NRLWE_{2m,q,\chi_1}$ *is hard, where* $\chi_1 = \psi^{-1}(\mathcal{D}_{\Lambda,tq\alpha})$ *and* `COM`, `SKE`, `MAC`, `KDF` *and* `H` *are secure with regards to Definitions 10, 11, 13 and 15 to 17. The computational variant also requires that* $NRLWE_{1,q,\chi_2}$ *for* $\chi_2 = \psi^{-1}(\mathcal{D}_{\Lambda,t\beta_T})$ *is hard.*

[3] Which is distributed as in the `DRE` because a_0 is invertible and a_{NRLWE} is uniform.

Proof. We give an overview of our games: Game 1 to 3 change the decryption oracle in such a way that we can change the public key in Game 4 without being detected. This change in turn allows us to replace c_1^* and c_2^* by randomness in Game 5 and 6, as well as remove k^* from the commitment in c_0^* in Game 7. Finally, we can now replace the symmetric parts by randomness in Game 8 and 9.

Denote by $\mathbb{P}[S_i]$ the probability that the experiment returns 1 in Game i.

Game 0: This game follows the IND-CCA2$_{\text{DRE}}$ game of Figure 2. The adversary $\mathcal{A}$ gets two independent public keys (pk^R, pk^S) for which it can make decryption queries. We call this phase 1. At one point $\mathcal{A}$ outputs two messages $m_0, m_1 \in \mathbf{M}$ and gets $c^* \coloneqq \texttt{Enc}(pk^R, pk^S, m_b)$ for $b \xleftarrow{\$} \{0,1\}$. It can now make additional decryption queries in what we call phase 2 as long as the public key is either pk^R or pk^S and $c \neq c^*$. Finally $\mathcal{A}$ outputs b' and wins if $b = b'$.
We thus have

$$\mathbb{P}[S_0] = \mathsf{Adv}^{\text{IND-CCA2}_{\text{DRE}}}_{\texttt{DRE},\mathcal{A}}(\lambda) + \frac{1}{2}.$$

Game 1: In this game, (c_0^*, c_1^*) are calculated just before the public keys are send to $\mathcal{A}$. As both parts are unavailable to $\mathcal{A}$ until c^* is released, we have

$$\mathbb{P}[S_1] = \mathbb{P}[S_0].$$

Game 2: Now we reject any requests with $\texttt{H}(c_0, c_1) = \texttt{H}(c_0^*, c_1^*)$ in phase 1 and $(c_0, c_1) \neq (c_0^*, c_1^*)$ with $\texttt{H}(c_0, c_1) = \texttt{H}(c_0^*, c_1^*)$ in phase 2. As in phase 1, $\mathcal{A}$ does not know anything about $\texttt{H}(c_0^*, c_1^*)$ it can only make such a query by chance. In phase 2 we can use any adversary returning a query that is now rejected to build an adversary $\mathcal{B}_1$ breaking the collision resistance of the hash function. Therefore, just as in prior works [9, Lemma 4], we have for Q_1 and $X_{\texttt{H}}$ being the amount of queries in phase 1 and the number of hash values respectively

$$|\mathbb{P}[S_2] - \mathbb{P}[S_1]| \leq \frac{Q_1}{X_{\texttt{H}}} + \mathsf{Adv}^{\text{CR}}_{\texttt{H},\mathcal{B}_1}(\lambda).$$

Game 3: In this game the decryption oracle additionally rejects requests with (c_0^*, c_1^*) in phase 2. We can bound the probability by which $\mathcal{A}$ makes such a request by two sub-events[4]

- NoBind: a different $k \neq k^*$ is associated with (c_0^*, c_1^*). For this to return something else than $\perp$, it requires $\texttt{COM.unveil}(ck, (c_0^R)^*, d_1) = k \neq k^* = \texttt{COM.unveil}(ck, (c_0^R)^*, d_2)$, but this violates the statistical binding property of the commitment.
- Forge: the same $k = k^*$ is associated with (c_0^*, c_1^*). For a valid query, we have $\texttt{MAC.verify}(mk^*, (c_0^*, c_1^*, c_2, \Delta), \tau) = 1$, where $(mk^*, dk^*) = \texttt{KDF}(k^*)$.

[4] Notice that queries in phase 2 still need to satisfy $c \neq c^*$.

Thus, we can bound the probability by

$$|\mathbb{P}[S_3] - \mathbb{P}[S_2]| \leq \mathbb{P}[\text{Forge}] + \mathtt{negl}(\lambda).$$

We show that we can bound the difference between Forge probabilities in the games. For this we define an algorithm $\mathcal{B}_{\mathrm{f}}^i$ that simulates Game i with $\mathcal{A}$ and outputs 1 if $\mathcal{A}$ sends a cipher to the decryption oracle with $(c_2, \Delta) \neq (c_2^*, \Delta^*)$ and $\mathtt{MAC.verify}(mk^*, (c_0^*, c_1^*, c_2, \Delta), \tau) = 1$, and a random bit if no such cipher was sent to the decryption oracle. Then we have

$$\begin{aligned}\mathbb{P}\left[\mathcal{B}_{\mathrm{f}}^i = 1\right] &= \mathbb{P}\left[\mathcal{B}_{\mathrm{f}}^i = 1 \mid \text{Forge}_i\right] \cdot \mathbb{P}[\text{Forge}_i] \\ &\quad + \mathbb{P}\left[\mathcal{B}_{\mathrm{f}}^i = 1 \mid \neg\text{Forge}_i\right] \cdot \mathbb{P}[\neg\text{Forge}_i] \\ &= \mathbb{P}[\text{Forge}_i] + \frac{1}{2}(1 - \mathbb{P}[\text{Forge}_i]) \\ &= \frac{1}{2} + \frac{1}{2} \cdot \mathbb{P}[\text{Forge}_i]\end{aligned}$$

This yields for $i, j \in \mathbb{N}$:

$$\begin{aligned}\left|\mathbb{P}\left[\text{Forge}_j\right] - \mathbb{P}[\text{Forge}_i]\right| &= 2 \cdot \left|\mathbb{P}\left[\mathcal{B}_{\mathrm{f}}^j = 1\right] - \mathbb{P}\left[\mathcal{B}_{\mathrm{f}}^i = 1\right]\right| \\ &\leq 2 \cdot |\mathbb{P}[S_j] - \mathbb{P}[S_i]|.\end{aligned}$$

Game 4: Notice that after the last game change, $\mathcal{A}$ is not allowed to make any decryption queries with $(c_0, c_1) = (c_0^*, c_1^*)$ in either phase. We can use this to change the public key in this game. More specifically, the goal is to change the (a, a_1) part of both parties to $(a, Ta - g \cdot \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*)))$ instead of (a, Ta). Here, we have to differentiate between the variants of the scheme's parameter. First, we show how to do this change in the computational variant because it is more instructive.

As Ta is only computational indistinguishable from randomness in this variant, we cannot do the change directly. Instead, we proceed with a series of smaller games, using our sound decryption capabilities to change the public keys of both parties one after another.

Game 4.1 We use sk^R for all decryption queries. Any adversary that can distinguish between Game 3 and 4.1 has to create a ciphertext that decrypts differently depending on whether one uses sk^R or sk^S, thus breaking soundness. As Theorem 2 shows that this can only happen with negligible probability we have

$$|\mathbb{P}[S_{4.1}] - \mathbb{P}[S_3]| \leq \mathtt{negl}(\lambda).$$

Game 4.2 We replace a_1^S by a random $u \in J_q^m$. As we don't use sk^S in our decryption oracle anymore we can use Lemma 9 to see that

$$|\mathbb{P}[S_{4.2}] - \mathbb{P}[S_{4.1}]| \leq l \cdot \mathsf{Adv}_{\mathcal{A}_{\mathrm{NRLWE}}}^{\mathrm{NRLWE}_{1,q,\chi_2}}(\lambda).$$

Game 4.3 We replace $a_1^S = u$ by $a_1^S = u - g \cdot \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*))$. As u acts as a one time pad we have

$$\mathbb{P}[S_{4.3}] = \mathbb{P}[S_{4.2}].$$

Game 4.4 We further replace $a_1^S = u - g \cdot \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*))$ by $a_1^S = T^S a^S - g \cdot \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*))$. Once again, Lemma 9 can be used to show that

$$|\mathbb{P}[S_{4.4}] - \mathbb{P}[S_{4.3}]| \leq l \cdot \mathsf{Adv}^{\mathrm{NRLWE}_{1,q,\chi_2}}_{\mathcal{A}_{\mathrm{NRLWE}}}(\lambda)$$

Game 4.5 We now use sk^S for all decryption queries. To see that the decryption oracle can still handle all the same queries, notice that for a valid $c = (c_0, c_1, c_2, \Delta, \tau)$ we have

$$\begin{aligned} c_2^S &= (a_1^S + g \cdot \mathtt{FRD}(\mathtt{H}(c_0, c_1)))s + e_2^S \\ &= (T^S a^S + g(\mathtt{FRD}(\mathtt{H}(c_0, c_1)) - \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*))))s + e_2^S. \end{aligned}$$

As $\mathtt{FRD}(\mathtt{H}(c_0, c_1)) - \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*))$ is invertible for all $\mathtt{H}(c_0, c_1) \neq \mathtt{H}(c_0^*, c_1^*)$, and such queries were already rejected before, we can use the trapdoor to decrypt all valid queries. Also, as in Game 4.1, the soundness property makes sure that the difference between using sk^R or sk^S is negligible, and so

$$|\mathbb{P}[S_{4.5}] - \mathbb{P}[S_{4.4}]| \leq \mathtt{negl}(\lambda).$$

Game 4.6 We now apply the changes of Games 4.2-4.4 to sk^R. As before, this yields

$$|\mathbb{P}[S_{4.6}] - \mathbb{P}[S_{4.5}]| \leq 2l \cdot \mathsf{Adv}^{\mathrm{NRLWE}_{1,q,\chi_2}}_{\mathcal{A}_{\mathrm{NRLWE}}}(\lambda) + \mathtt{negl}(\lambda)$$

This finishes the public key change in the computational variant. In the statistical variant each row of Ta is statistically indistinguishable from uniform by Lemma 4 with $z_1 = 1$ and $z_2 = m$. Therefore, we can skip Game 4.2-4.4 and Game 4.6 but otherwise use the same arguments.
To summarize, after Game 4 we have:

$$(pk, sk) = ((a, Ta - g \cdot \mathtt{FRD}(\mathtt{H}(c_0^*, c_1^*))), T),$$

and we reject all queries with $\mathtt{H}(c_0, c_1) = \mathtt{H}(c_0^*, c_1^*)$.

Game 5: This game changes c_1^*, c_2^* for both parties. Instead of drawing them honestly, we draw $\bar{c}_1^* \xleftarrow{\$} J_q^m$ for each party and set $c_1^* = \bar{c}_1^* + a \cdot \psi^{-1}(B_\Lambda(q/2 \cdot d))$. For c_2^* we draw $\bar{e} \leftarrow \psi^{-1}(\mathcal{D}^l_{\Lambda, t\beta_T q\alpha\sqrt{m}})$ and set $c_2^* = Tc_1^* + \bar{e}$, also for each party.
Assume that there is an adversary that can distinguish both games. We use it to build an adversary $\mathcal{B}_2$ against the $\mathrm{NRLWE}_{2m,q,\chi_1}$ assumption[5] that receives

[5] We need $2m$ to split the vectors for both parties.

the canonically embedded samples $(a_{\text{NRLWE}}, b_{\text{NRLWE}}) = ((a^R_{\text{NRLWE}}, a^S_{\text{NRLWE}}), (b^R_{\text{NRLWE}}, b^S_{\text{NRLWE}})) \in J_q^{2m} \times J_q^{2m}$. By Lemma 1, we can assume that both a^i_{NRLWE} have an invertible element and without loss of generality we can assume that both a^i_{NRLWE} have the invertible element at the first position[6]. The adversary $\mathcal{B}_2$ simulates Game 5 with $a = a_{\text{NRLWE}}$, while still generating honest secret keys. It also sets $(\bar{\mathsf{c}}_1^R)^* = b^R_{\text{NRLWE}}$ and $(\bar{\mathsf{c}}_1^S)^* = b^S_{\text{NRLWE}}$ instead of drawing it randomly.
If b_{NRLWE} is random, then this perfectly simulates Game 5. If $b_{\text{NRLWE}} = a_{\text{NRLWE}}x + y$ for some $x \leftarrow \chi_1, y \leftarrow \chi_1^{2m}$ instead, then it simulates Game 4, as

$$\begin{aligned} \mathsf{c}_1^* &= b_{\text{NRLWE}} + a_{\text{NRLWE}} \cdot \psi^{-1}\left(B_\Lambda\left(\frac{q}{2} \cdot d\right)\right) \\ &= a_{\text{NRLWE}}\left(x + \psi^{-1}\left(B_\Lambda\left(\frac{q}{2} \cdot d\right)\right)\right) + y \sim as + e \end{aligned} \tag{8}$$

and

$$\begin{aligned} \mathsf{c}_2^* &= T\mathsf{c}_1^* + \bar{e} \overset{(8)}{\sim} T(as + e) + \bar{e} = Tas + Te + \bar{e} \\ &= (a_1 + g \cdot \mathtt{FRD}(\mathtt{H}(\mathsf{c}_0^*, \mathsf{c}_1^*)))s + Te + \bar{e} \overset{(*)}{\sim} (a_1 + g \cdot \mathtt{FRD}(\mathtt{H}(\mathsf{c}_0^*, \mathsf{c}_1^*)))s + \tilde{e}. \end{aligned}$$

For $(*)$ to hold, we need that $Te + \bar{e} = \tilde{e}$ is distributed as e_2^i. By Lemma 3, $Te + \bar{e}$ is distributed as $\psi^{-1}(\mathcal{D}^l_{\Lambda,\sqrt{\Sigma}})$ with $\Sigma = t^2\beta_T^2 Mul(e_1^i) + t^2\beta_T^2 m(q\alpha)^2$, which is the distribution of e_2^i. The bounds on the smoothing parameter hold by Lemma 8. Therefore we have

$$|\mathbb{P}[S_5] - \mathbb{P}[S_4]| \leq \mathsf{Adv}^{\text{NRLWE}_{2m,q,\chi_1}}_{\mathcal{B}_2}.$$

Game 6: We now choose c_1^* completely random. As $\bar{\mathsf{c}}_1^*$ acted as a one-time pad, the adversary cannot distinguish this and hence

$$\mathbb{P}[S_6] = \mathbb{P}[S_5].$$

Game 7: The next change is to make the commitment independent of k^*. We achieve this by changing $\mathsf{c}_0^* = (\mathtt{COM.com}(ck^i, k^*, r^i))_{i\in\{R,S\}}$ to $\mathsf{c}_0^* = (\mathtt{COM.com}(ck^i, k', r^i))_{i\in\{R,S\}}$ with random $k' \xleftarrow{\$} \{0,1\}^n$ over two games. As all parts of the challenge cipher are independent of d, a straightforward reduction shows for an adversary $\mathcal{B}_3$ on the hiding game

$$|\mathbb{P}[S_7] - \mathbb{P}[S_6]| \leq 2 \cdot \mathsf{Adv}^{\text{Hiding}}_{\mathtt{COM},\mathcal{B}_3}.$$

Game 8: In this game, we change mk^*, dk^* to random. As k^* is not used anymore, this reduces to the indistinguishability from the KDF as in the works of Boyen, Izabachène, and Li [9, Lemma 6]. Additionally, as the MAC

[6] Otherwise reorder a_{NRLWE} and b_{NRLWE} such that an invertible element is at the first position.

key is now random, the Forge probability can be directly reduced to the forgery game of the MAC and thus

$$|\mathbb{P}[S_8] - \mathbb{P}[S_7]| \leq \mathsf{Adv}^{\text{IND}}_{\mathtt{KDF},\mathcal{B}_4}(\lambda)$$
$$\mathbb{P}[\text{Forge}_8] \leq \mathsf{Adv}^{\text{OT-SUF}}_{\mathtt{MAC},\mathcal{B}_5}(\lambda).$$

This also bounds $\mathbb{P}[\text{Forge}_3]$ and hence $|\mathbb{P}[S_3] - \mathbb{P}[S_2]|$ by a negligible function using the arguments in Game 3.

Game 9: Finally, we can change Δ^* to random. As dk^* is random, any adversary $\mathcal{B}_6$ that distinguishes this breaks the SKE indistinguishability, and thus

$$|\mathbb{P}[S_9] - \mathbb{P}[S_8]| \leq \mathsf{Adv}^{\text{OT-IND}}_{\mathtt{SKE},\mathcal{B}_6}(\lambda).$$

We now have a game with a ciphertext independent of the chosen value b. Using our assumptions we thus see that

$$\mathsf{Adv}^{\text{IND-CCA2}_{\text{DRE}}}_{\text{DRE},\mathcal{A}}(\lambda) \leq \mathtt{negl}(\lambda). \qquad \square$$

4 SB-KEM Construction

We now construct a SB-KEM from the same ingredients. So choose $R, n, q, m, l, \beta_T, t, \Lambda, B_\Lambda, g, \tilde{B}_g, J_q, J_q^*$ as for the DRE scheme from Section 3. The only difference is the bound α, which changes to

$$\frac{1}{\alpha} \geq 2\beta_T \cdot \left\| \tilde{B_g}^T \right\|_{\varphi,\infty} \cdot \left\| B_\Lambda^{-1} \right\|_2 \cdot \sqrt{n(2n+1)m}$$

as no soundness is required for the SB-KEM. For the computational variant, a double trapdoor similar to the work of Kiltz, Masny, and Pietrzak [20] is required, doubling the cipher size. While the resulting sizes can be found in Section 5, we only describe the statistical variant in this section.

Additional building blocks are again a key derivation function KDF and a FRD $\mathtt{FRD} : \mathbf{P} \to J_q^*$, where $\mathbf{P}$ is the set of parties.

Figure 6 shows the definition of the SB-KEM $\mathtt{KEM} = (\mathsf{KGen}, \mathtt{Enc}, \mathtt{Dec})$.

Theorem 4. *The SB-KEM KEM from Figure 6 is correct with overwhelming probability over the errors $e_1, e_2, \bar{s}$.*

The proof is the same as for Theorem 1.

Theorem 5. *The SB-KEM KEM from Figure 6 is IND-SB-CPA$_{SB\text{-}KEM}$ given that NRLWE$_{m,q,\chi}$ is hard, where $\chi = \psi^{-1}(\mathcal{D}_{\Lambda,tq\alpha})$ and the KDF satisfies Definition 17.*

The proof is very similar to Theorem 3 except half of the games can be omitted. Games 1-3 can be omitted as the security game already does not accept these queries. Also Game 7-9 can be done in one game, where we replace the key k with randomness, reducing this game hop straight to the KDF indistinguishability game.

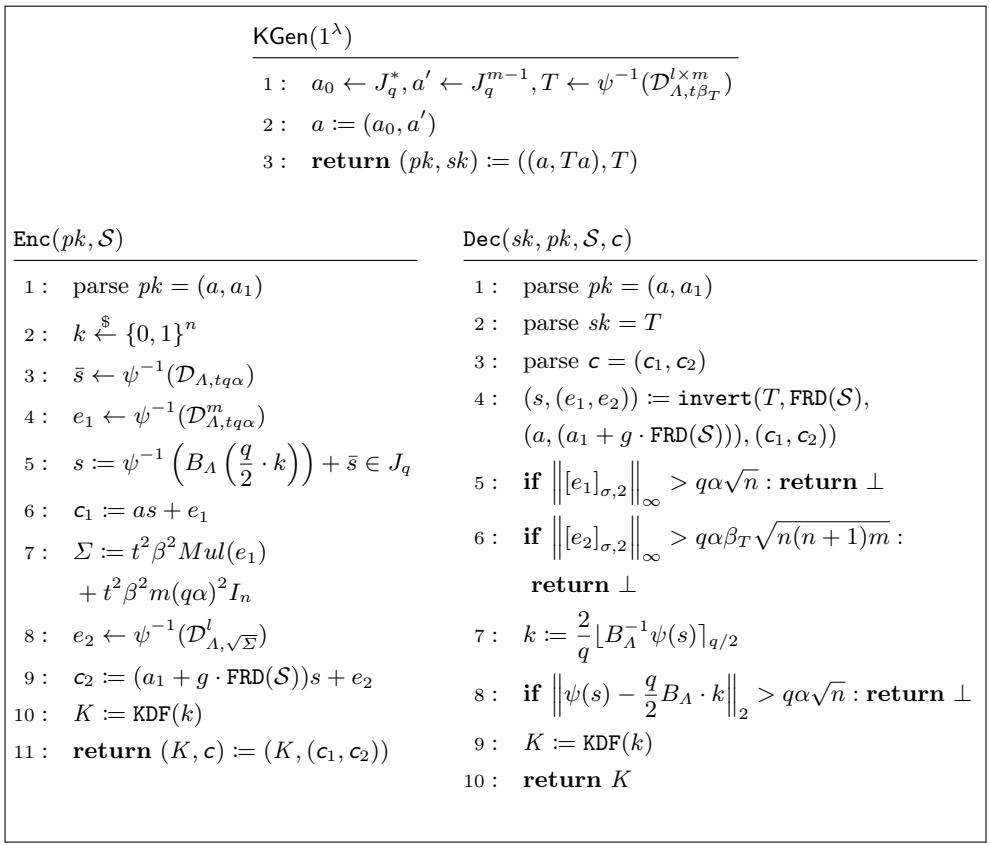

Fig. 6. RLWE based SB-KEM

5 Parameter Sets

The computations are performed in the polynomial representation instead of the canonical embedding to avoid complex numbers. Hence, the discrete Guassians have to be translated to the coefficent embedding. For $2n$-cyclotomics, where n is a power of two, the Gaussians simply translate to the coefficent embedding with a scaling of $\frac{1}{\sqrt{n}}$ as shown by Lyubashevsky, Peikert, and Regev [22]. For the modulo q we choose a prime with $q = 2r + 1 \mod 4r$, for $r = 16$, as Bert *et al.* [7] showed a FRD for these parameters.

The construction requires that the bound of a vector sampled from a discrete Gaussian is not too large with overwhelming probability as described in Equation (2). For concrete parameters we choose to have $\delta \leq 2^{-\lambda}$, where λ is the security parameter. Using the bound from Lemma 2, we obtain the values for t depending on n and λ summarized in Table 2. The values for t are determined such that they best fit the security level λ which the parameter sets achieve.

n	λ	t
512	90	0.731
1024	157	0.745
1024	165	0.74
2048	192	0.79
2048	302	0.749

Table 2. The values for t depending on the dimension n and λ to achieve $\delta \leq 2^{-\lambda}$

The norm $\left\|\tilde{B_g}^T\right\|_{\varphi,\infty}$ was determined numerically and yielded $\left\|\tilde{B_g}^T\right\|_{\varphi,\infty} = 4$ for any q and n. For B_Λ^{-1} it can be shown that $\left\|B_\Lambda^{-1}\right\|_2 = \frac{1}{n}\|B_\Lambda\|_2 = \frac{1}{\sqrt{n}}$, based on the fact that B_Λ contains n orthogonal vectors of length $\sqrt{n}$ [22, 25].

To estimate the hardness of NRLWE, we use the lattice estimator [1], a tool frequently used to estimate the hardness of LWE instances. Concretely, we use commit "5ba00f5" and the cost model "MINZOV" [24].

The parameter sets for the DRE and the KEM are shown in Table 3 and Table 4, respectively. The parameters $\gamma_T := \frac{1}{\sqrt{n}} t\beta_T$ and $\gamma_e := \frac{1}{\sqrt{n}} tq\alpha$ are the parameters of the Gaussian distribution in the coefficient embedding for T and the errors, respectively. More specifically, each coefficient of the polynomial is drawn independently from a Gaussian distribution with that width. The "C/S" column specifices whether the parameter set is in the computational (C) or statistical (S) variant. The column "λ" specifices the bit security. For t we use the values from Table 2, which ensure $\delta \leq 2^{-\lambda}$. For example, for $n = 1024$ all parameter sets with $\lambda \leq 157$ use $t = 0.745$, while the others use $t = 0.74$.

n	q ($\lceil \log_2 q \rceil$)	m	γ_T	γ_e	C/S	λ	size(pk)	size(sk)	size(c)
512	0xF3d21 (20)	2	1.29	1.29	C	84	28.2 KB	51.2 KB	56.4 KB
1024	0xF69A1 (20)	2	0.79	0.79	C	155	56.3 KB	102 KB	112.6 KB
1024	0x31F7E1 (22)	2	1.42	1.42	C	157	67.6 KB	124 KB	135.2 KB
2048	0x31F7E1 (22)	2	0.85	0.85	C	302	135.2 KB	247.8 KB	270.3 KB
1024	0x7884418FD21 (43)	2	2048	2513	C	138	247 KB	473 KB	494 KB
1024	0x4dd796487d61 (47)	6	3987	5306	S	132	318 KB	1.7 MB	638 KB
2048	0x1F24D205A1 (37)	7	1073	10.1	S	192	416 KB	2.45 MB	833 KB

Table 3. Parameter Sets for the DRE

We now turn towards comparing our constructions to the existing literature. The only existing IND-SB-CPA$_{\text{SB-KEM}}$ secure SB-KEM by Benz *et al.* [6] has no concrete parameters but we estimate their size to be much worse than the most efficient standard model post-quantum KEMs, which is why we compare our construction to those instead. To the best of our knowledge, the currently most efficient post-quantum KEMs in the standard model are the Learning Parity with Noise (LPN)-based construction by Xu and Li [31] and the RLWE-based construction by Yang, Ma, and Zhang [32]. As representative for KEMs in the

n	q ($\lceil \log_2 q \rceil$)	m	γ_T	γ_e	C/S	λ	size(pk)	size(sk)	size(c)
512	0xF3d21 (20)	2	1.69	1.7	C	87	28.2 KB	51.2 KB	56.4 KB
1024	0xF69A1 (20)	2	1.027	1.027	C	162	56.3 KB	102 KB	112.6 KB
1024	0x31F7E1 (22)	2	1.85	1.85	C	163	67.6 KB	124 KB	135.2 KB
1024	0x3c7d313b5a5 (42)	2	2048	2148	C	144	237 KB	452 KB	473 KB
1024	0x3ac62ca642e1 (46)	6	3804	10240	S	143	306 KB	1.62 MB	306 KB
2048	0x1F24D205A1 (37)	6	1976	15.3	S	192	407 KB	2.1 MB	407 KB

Table 4. Parameter Sets for the SB-KEM

ROM, Kyber [29] is used as it has been standardized recently. Table 5 shows the parameters of the different KEMs. While our scheme is worse than Kyber, it is significantly better than existing non-ROM KEMs by improving the public and secret key compared to the LPN-based or the ciphertext size compared to the RLWE-based scheme.

Scheme	λ	pk	sk	c
Kyber512 [29]	128	0.8 KB	1.632 KB	0.768 KB
Kyber768 [29]	192	1.184 KB	2.4 KB	1.088 KB
LPN-based [31]	128	50.78 MB	62.50 MB	4.54 KB
RLWE-based [32]	80	1.923 MB	0.96 MB	1.280 MB
Ours	87	28.2 KB	51.5 KB	56.4 KB
Ours	162	56.3 KB	102 KB	112.6 KB

Table 5. Comparison of the key sizes for our construction with existing post-quantum KEMs.

With regards to our DRE scheme, there are, to the best of our knowledge, only two sound post-quantum IND-CCA2$_{\text{DRE}}$ DRE schemes, both by Benz *et al.* [5]. One is LPN based, while the other is LWE based. We compare ourselves to their proposed parameters though we note that they chose a very small Gaussian width for the LWE errors which makes the scheme less secure than claimed. The results can be found in Table 6.

Scheme	λ	pk	sk	c
LWE-based [5]	"256"	61.45 MB	58.49 MB	91.45 KB
LPN-based [5]	256	351.13 MB	351.13 MB	26.5 KB
Ours	157	56.3 KB	102 KB	112.6 KB
Ours	302	135.2 KB	247.8 KB	270.3 KB

Table 6. Comparison of the key sizes for our construction with existing post-quantum IND-CCA2$_{\text{DRE}}$ DREs.

6 Conclusion

In this work, we constructed efficient RLWE based DRE and SB-KEM schemes. Both are IND-CCA2 secure in the standard model. The resulting sizes are a significant improvement on the best currently known constructions in the literature.

We also want to mention that in the process of developing this paper we implemented a proof of concept of the resulting SB-KEM which can be found on Gitlab[7]. This shows the accessibility of the scheme, making it usable in applications.

Finally, we note that our sizes can probably be improved even further by using compression tactics, which could push the schemes into the regime of ROM based PKEs. This is left as a further research topic.

Acknowledgements. We thank the PKC 2026 anonymous reviewers for their valuable feedback. We also thank Michael Klooß for his valuable input and Wasilij Beskorovajnov for his part in kickstarting our research. This work was funded by the Topic Engineering Secure Systems of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs, Karlsruhe.

References

1. Albrecht, M.R., Player, R., Scott, S.: On the Concrete Hardness of Learning with Errors. Journal of Mathematical Cryptology **9**(3), 169–203 (2015). https://doi.org/10.1515/jmc-2015-0016
2. Alkadri, N.A., Demirel, D., El Bansarkhani, R.: Post-quantum commitment schemes. HNO **9**, 32 (2015)
3. Banaszczyk, W.: New Bounds in some Transference Theorems in the Geometry of Numbers. Mathematische Annalen **296**, 625–635 (1993)
4. Bellare, M., Rogaway, P.: Optimal Asymmetric Encryption. In: De Santis, A. (ed.) Advances in Cryptology – EUROCRYPT'94. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053428
5. Benz, L., Beskorovajnov, W., Eilebrecht, S., Gröll, R., Müller, M., Müller-Quade, J.: Chosen-Ciphertext Secure Dual-Receiver Encryption in the Standard Model Based on Post-quantum Assumptions. In: Tang, Q., Teague, V. (eds.) PKC 2024: 27th International Conference on Theory and Practice of Public Key Cryptography, Part IV. LNCS, vol. 14604, pp. 257–288. Springer, Heidelberg (2024). https://doi.org/10.1007/978-3-031-57728-4_9
6. Benz, L., Beskorovajnov, W., Eilebrecht, S., Müller-Quade, J., Ottenhues, A., Schwerdt, R.: Sender-binding Key Encapsulation. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023: 26th International Conference on Theory and Practice of Public Key Cryptography, Part I. LNCS, vol. 13940, pp. 744–773. Springer, Heidelberg (2023). https://doi.org/10.1007/978-3-031-31368-4_26

[7] https://gitlab.kit.edu/robert.brede/rlwe-sb-kem

7. Bert, P., Eberhart, G., Prabel, L., Roux-Langlois, A., Sabt, M.: Implementation of Lattice Trapdoors on Modules and Applications. In: Cheon, J.H., Tillich, J.-P. (eds.) Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, pp. 195–214. Springer, Cham, Switzerland, Daejeon, South Korea (2021). https://doi.org/10.1007/978-3-030-81293-5_11
8. Beskorovajnov, W., Gröll, R., Müller-Quade, J., Ottenhues, A., Schwerdt, R.: A new security notion for PKC in the standard model: weaker, simpler, and still realizing secure channels. In: IACR International Conference on Public-Key Cryptography, pp. 316–344 (2022)
9. Boyen, X., Izabachène, M., Li, Q.: Secure Hybrid Encryption in the Standard Model from Hard Learning Problems. In: Cheon, J.H., Tillich, J.-P. (eds.) Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, pp. 399–418. Springer, Cham, Switzerland, Daejeon, South Korea (2021). https://doi.org/10.1007/978-3-030-81293-5_21
10. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. Journal of the ACM (JACM) **51**(4), 557–594 (2004)
11. Chow, S.S.M., Franklin, M.K., Zhang, H.: Practical Dual-Receiver Encryption - Soundness, Complete Non-malleability, and Applications. In: Benaloh, J. (ed.) Topics in Cryptology – CT-RSA 2014. LNCS, vol. 8366, pp. 85–105. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-319-04852-9_5
12. Damgård, I., Hofheinz, D., Kiltz, E., Thorbek, R.: Public-Key Encryption with Non-interactive Opening. In: Malkin, T. (ed.) Topics in Cryptology – CT-RSA 2008. LNCS, vol. 4964, pp. 239–255. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79263-5_15
13. Dodis, Y., Katz, J., Smith, A., Walfish, S.: Composability and On-Line Deniability of Authentication. In: Reingold, O. (ed.) TCC 2009: 6th Theory of Cryptography Conference. LNCS, vol. 5444, pp. 146–162. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00457-5_10
14. Fiat, A., Naor, M.: Broadcast Encryption. In: Stinson, D.R. (ed.) Advances in Cryptology – CRYPTO'93. LNCS, vol. 773, pp. 480–491. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_40
15. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology – CRYPTO'86. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
16. Fujisaki, E., Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes. In: Wiener, M.J. (ed.) Advances in Cryptology – CRYPTO'99. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_34
17. Genise, N., Micciancio, D., Peikert, C., Walter, M.: Improved Discrete Gaussian and Subgaussian Analysis for Lattice Cryptography. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part I. LNCS, vol. 12110, pp. 623–651. Springer, Heidelberg (2020). https://doi.org/10.1007/978-3-030-45374-9_21
18. Hsieh, Y.-C., Waters, B., Wu, D.J.: A Generic Approach to Adaptively-Secure Broadcast Encryption in the Plain Model. In: Fehr, S., Fouque, P.-A. (eds.) Advances in Cryptology – EUROCRYPT 2025, Part III. LNCS, vol. 15603, pp. 336–365. Springer, Heidelberg (2025). https://doi.org/10.1007/978-3-031-91131-6_12
19. Khovratovich, D., Rothblum, R.D., Soukhanov, L.: How to Prove False Statements: Practical Attacks on Fiat-Shamir. In: Kalai, Y.T., Kamara, S.F. (eds.) Advances

in Cryptology – CRYPTO 2025, Part VI. LNCS, vol. 16005, pp. 3–26. Springer, Heidelberg (2025). https://doi.org/10.1007/978-3-032-01887-8_1
20. Kiltz, E., Masny, D., Pietrzak, K.: Simple Chosen-Ciphertext Security from Low-Noise LPN. In: Krawczyk, H. (ed.) PKC 2014: 17th International Conference on Theory and Practice of Public Key Cryptography. LNCS, vol. 8383, pp. 1–18. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_1
21. Lai, R.W., Cheung, H.K., Chow, S.S.: Trapdoors for Ideal Lattices with Applications. In: Information Security and Cryptology, pp. 239–256. Springer International Publishing, Cham (2014)
22. Lyubashevsky, V., Peikert, C., Regev, O.: A Toolkit for Ring-LWE Cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology – EUROCRYPT 2013. LNCS, vol. 7881, pp. 35–54. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_3
23. Lyubashevsky, V., Seiler, G.: Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-Based Zero-Knowledge Proofs. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 204–224. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-319-78381-9_8
24. MATZOV, Report on the Security of LWE: Improved Dual Lattice Attack, https://zenodo.org/records/6412487 (2022). Accessed 08-24-2024.
25. Micciancio, D., Peikert, C.: Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
26. Micciancio, D., Regev, O.: Worst-Case to Average-Case Reductions Based on Gaussian Measures. SIAM Journal on Computing **37**(1), 267–302 (2007). https://doi.org/10.1137/S0097539705447360
27. Noh, G., Hong, D., Kwon, J.O., Jeong, I.R.: A strong binding encryption scheme from lattices for secret broadcast. IEEE communications letters **16**(6), 781–784 (2012)
28. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th Annual ACM Symposium on Theory of Computing, pp. 84–93. ACM Press, Baltimore, MA, USA (2005). https://doi.org/10.1145/1060590.1060603
29. of Standards, N.I., Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication (2024). https://doi.org/10.6028/NIST.FIPS.203
30. Unger, N., Goldberg, I.: Improved Strongly Deniable Authenticated Key Exchanges for Secure Messaging. Proceedings on Privacy Enhancing Technologies **2018**(1), 21–66 (2018). https://doi.org/10.1515/popets-2018-0003
31. Xu, S., Li, X.: Chosen-Ciphertext Secure Key Encapsulation Mechanism in the Standard Model. IEEE Access **9**, 13683–13690 (2021). https://doi.org/10.1109/ACCESS.2021.3051047
32. Yang, X., Ma, W., Zhang, C.: Efficient Chosen Ciphertext Secure Key Encapsulation Mechanism in Standard Model over Ideal Lattices. International Journal of Computer Mathematics **94**(5), 866–883 (2017). https://doi.org/10.1080/00207160.2016.1149578
33. Zhang, J., Yu, Y., Fan, S., Zhang, Z.: Improved lattice-based CCA2-secure PKE in the standard model. Science China Information Sciences **63**(8), 182101 (2020)

A Gaussian Bounds

This section proves the statements related to Gaussian bounds, which are Lemmas 2, 3 and 8. For this, we need the partial order upon positive semidefinite matrices Σ_1, Σ_2 denoted as $\Sigma_1 \preceq \Sigma_2$, if $\Sigma_2 - \Sigma_1$ is positive semidefinite. For matrices S, T, we write $S \leq T$, if $SS^T \preceq TT^T$. Now we define the matrix A_e, which corresponds to the multiplication with an element $e \in H$.

Definition 19. Let $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ be defined as in Section 2. For an element $e = (r_1, \ldots, r_{s_1}, c_1, \bar{c}_1, \ldots, c_{s_2}, \bar{c}_{s_2}) \in H$, the matrix $A_e \in \mathbb{R}^{n \times n}$ with $n = s_1 + 2s_2$ is defined as

$$A_e = \begin{pmatrix} D(r_1, \ldots, r_{s_1}) & & & \\ & Rot(c_1) & & \\ & & \ddots & \\ & & & Rot(c_{s_2}) \end{pmatrix}, Rot(c = a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

where $D(r_1, \ldots, r_{s_1}) \in \mathbb{R}^{s_1 \times s_1}$ is the diagonal matrix with $r_1, \ldots, r_{s_1}$ on its diagonal.

Multiplication with A_e corresponds to multiplication in H as stated by the following lemma.

Lemma 10. *Let $\psi : H \to \mathbb{R}^n$ be the isomorphism from H to $\mathbb{R}^n$, $e, t \in H$ and A_e as in Definition 19. Then it holds that $\psi(e \odot t) = A_e \psi(t)$.*

Proof. For complex numbers $c_1 = a_1 + b_1 i, c_2 = a_2 + b_2 i \in \mathbb{C}$, $Rot(c_1)(a_2\ b_2)^T = (a_1 a_2 - b_1 b_2\ a_1 b_2 + b_1 a_2)^T = \psi(c_1 \cdot c_2)$. From the diagonal structure of A_e it follows that $\psi(e \odot t) = A_e \psi(t)$. □

If e is a canonical embedded field element of a number field, then A_e is invertible as stated in the following lemma.

Lemma 11. *Let K be a cyclotomic number field, $x \in K, x \neq 0$ and $e = \sigma(x)$. Then the function $f : \mathbb{R}^n \to \mathbb{R}^n, f(y) = A_e y$ is injective.*

Proof. As K is a field and σ is an injective ring homomorphism [22], any element $x \in K, x \neq 0$ is invertible and thus embedded to an invertible $e \neq 0$ and hence $f(y) = A_e y = \psi(e \odot \psi^{-1}(y))$ is injective. □

For the proof of Lemma 3, we need two results of Genise *et al.* [17], related to discrete Gaussian distributions. The first follows from the definition of the smoothing parameter.

Lemma 12 ([17, Lemma 2]). *For any lattice $\Lambda \subseteq \mathbb{R}^n, \varepsilon \geq 0$ and matrices S, T of full rank, we have $\eta_\varepsilon(\Lambda) \leq S$ if and only if $\eta_\varepsilon(T\Lambda) \leq TS$.*

The second is a theorem, which states that the sum of two discrete Gaussians is again a discrete Gaussian and is as follows.

Theorem 6 ([17, Theorem 3]). *Let $\varepsilon \in (0,1)$, define $\varepsilon' = 4\varepsilon/(1-\varepsilon)^2$. Let $A_1, A_2 \subseteq \mathbb{R}^n$ be cosets of full-rank lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{R}^n$ (respectively), let Σ_1, Σ_2 be positive definite matrices where $\eta_\varepsilon(\Lambda_2) \leq \sqrt{2\pi} \cdot \sqrt{\Sigma_2}$ and let*

$$\mathcal{X} = \left[(x_1, x_2) | x_1 \leftarrow \mathcal{D}_{A_1, \sqrt{\Sigma_1}}, x_2 \leftarrow x_1 + \mathcal{D}_{A_2 - x_1, \sqrt{\Sigma_2}}\right].$$

If $\eta_\varepsilon(\Lambda_1) \leq \sqrt{2\pi} \cdot \sqrt{\Sigma_3}$ where $\Sigma_3^{-1} = \Sigma_1^{-1} + \Sigma_2^{-1}$, then the marginal distribution $\mathcal{X}_2$ of x_2 in $\mathcal{X}$ satisfies

$$\mathcal{X}_2 \overset{\varepsilon'}{\approx} \mathcal{D}_{A_2, \sqrt{\Sigma_1 + \Sigma_2}}.$$

With that we can show Lemma 3 from Section 2.

Lemma 3. *Consider the $\tilde{n}$-th cyclotomic number field of degree n for some $\tilde{n} \geq 2$, $J \subseteq H$ its embedded ring of integers and $\Lambda = \psi(J) \subseteq \mathbb{R}^n$ the corresponding lattice. Let Σ_f be a positive definite diagonal matrix. For $s_T > 0$, an integer m and $1 \leq i \leq m$, let $t_i \leftarrow \psi^{-1}\left(\mathcal{D}_{\Lambda, s_T}\right), e_i \in J$ and $f \leftarrow \psi^{-1}\left(\mathcal{D}_{\Lambda, \sqrt{\Sigma_f}}\right)$. Let $\varepsilon := \varepsilon(n) > 0$ be negligible in n. If $\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi} \cdot A_{e_i}^{-1} \sqrt{\left(\Sigma_f^{-1} + \left(s_T^2 A_{e_i} A_{e_i}^T\right)^{-1}\right)^{-1}}$ for every i, where $e_i \neq 0$ and $\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi} \cdot \sqrt{\Sigma_f}$, then the distribution of*

$$f + \sum_{i=1}^{m} e_i \odot t_i$$

is statistically close to $\psi^{-1}\left(\mathcal{D}_{\Lambda, \sqrt{\Sigma}}\right)$, where we define the width of the Gaussian as $\Sigma := \Sigma_f + s_T^2 \sum_{i=1}^m A_{e_i} A_{e_i}^T = \Sigma_f + s_T^2 Mul(e)$ for $e := (e_1, \ldots, e_m)$ and $Mul(e) := \sum_{i=1}^m A_{e_i} A_{e_i}^T$.

Proof. Each summand with $e_i = 0$ can obviously be ignored and therefore we assume $e_i \neq 0$ for each i. Combining Lemmas 10 to 12 yields that $\psi(e_i \odot t_i)$ is distributed as $\mathcal{D}_{A_{e_i}\Lambda,\, s_T A_{e_i}}$.

The rest is shown by an induction over m. For the m-th addition, we show that $\psi(f + \sum_{i=1}^m e_i \odot t_i)$ is statistically close to $\mathcal{D}_{\Lambda, \sqrt{\Sigma_m}}$, where $\Sigma_m = \Sigma_f + s_T^2 \sum_{i=1}^m A_{e_i} A_{e_i}^T$. For $m = 0$ this is simply $\psi(f) \sim \mathcal{D}_{\Lambda, \sqrt{\Sigma_f}}$.

For $m+1$, we use Theorem 6 with the following instantiation:

$$\begin{aligned} A_1 &= A_{e_m}\Lambda,\ \Sigma_1 = s_T^2 A_{e_m} A_{e_m}^T, \\ A_2 &= \Lambda,\ \Sigma_2 = \Sigma_m. \end{aligned}$$

The theorem has two requirements:

$$\begin{aligned} \eta_\varepsilon(\Lambda) &\leq \sqrt{2\pi} \cdot \sqrt{\Sigma_m}, \\ \eta_\varepsilon(A_{e_m}\Lambda) &\leq \sqrt{2\pi} \cdot \sqrt{\Sigma_3} \end{aligned}$$

where $\Sigma_3^{-1} = \Sigma_1^{-1} + \Sigma_2^{-1}$. The first equation holds as

$$\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi} \cdot \sqrt{\Sigma_f} \leq \sqrt{2\pi} \cdot \sqrt{\Sigma_f + s_T^2 \sum_{i=1}^{m} A_{e_m} A_{e_m}^T} = \sqrt{2\pi} \cdot \sqrt{\Sigma_m}.$$

As $e_m \neq 0$, $A_{e_m}^{-1}$ exists and is injective. Therefore, by Lemma 12 the second inequality is equal to

$$\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi} \cdot A_{e_m}^{-1} \sqrt{\Sigma_3}.$$

As Σ_f and $A_{e_m} A_{e_m}^T$ are diagonal matrices, it holds that

$$\begin{aligned} \Sigma_3 &= \left(\left(\Sigma_f + s_T^2 \sum_{i=0}^{k-1} A_{e_m} A_{e_m}^T \right)^{-1} + \left(s_T^2 A_{e_m} A_{e_m}^T \right)^{-1} \right)^{-1} \\ &\succeq \left(\Sigma_f^{-1} + \left(s_T^2 A_{e_m} A_{e_m}^T \right)^{-1} \right)^{-1} \end{aligned}$$

and therefore

$$\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi} \cdot A_{e_m}^{-1} \sqrt{\left(\Sigma_f^{-1} + \left(s_T^2 \Sigma_{e_m} \right)^{-1} \right)^{-1}} \leq \sqrt{2\pi} \cdot A_{e_m}^{-1} \sqrt{\Sigma_3}.$$

Therefore, $\psi(\sum_{i=1}^{m} e_i \odot t_i + f)$ is statistically close to $\mathcal{D}_{\Lambda,\sqrt{\Sigma}}$. □

To prove Lemma 2 we need the bound established by Banaszczyk [3].

Lemma 13. *([3], Lemma 1.5(i)) Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $B_n \subseteq \mathbb{R}^n$ be the open sphere of unity. For each $c \geq (2\pi)^{-1/2}$ one has*

$$\rho(\Lambda \setminus c\sqrt{n} B_n) < \left(e^{-\pi c^2} c\sqrt{2\pi e} \right)^n \rho(\Lambda).$$

With this we can prove Lemma 2.

Lemma 2. *Let $t > 1$ and $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Let also $\Sigma \in \mathbb{R}_{\geq 0}^{n \times n}$ be a diagonal matrix and $s = \|\sqrt{\Sigma}\|_2$. Then we have*

$$\mathbb{P}\left[\|x\|_2 > st\sqrt{n} \mid x \leftarrow \mathcal{D}_{\Lambda,\sqrt{\Sigma}} \right] < \left(e^{\frac{-t^2}{2}} t\sqrt{e} \right)^n,$$

which is negligible in n.

Proof. As $\mathcal{D}_{\Lambda,\sqrt{\Sigma}}$ corresponds to drawing n independent Gaussians, zeros on the diagonal of Σ correspond to one index always being zero. This zero does not increase the norm and thus we can assume that $\Sigma \in \mathbb{R}_{>0}^{n \times n}$. As the Gaussian distribution only depends on Σ, not on the choice of $\sqrt{\Sigma}$, choose $S := \sqrt{\Sigma}$ invertible. Such a matrix exists because of the structure of Σ. Let $y \leftarrow \mathcal{D}_{\Lambda,I_n}$

and $B_n \subseteq \mathbb{R}^n$ the open sphere of unity. Let $\Lambda' \coloneqq (\sqrt{2\pi}S)^{-1}\Lambda$ and $c \coloneqq (\sqrt{2\pi})^{-1}t$. Using the definition of $\mathcal{D}_{\Lambda,\sqrt{\Sigma}}$, we have

$$\begin{aligned}\mathbb{P}\left[\|x\|_2 \geq st\sqrt{n} \mid x \leftarrow \mathcal{D}_{\Lambda,S}\right] &= \mathbb{P}\left[\|\sqrt{2\pi}Sy\|_2 \geq st\sqrt{n} \mid y \leftarrow \mathcal{D}_{\Lambda',I_n}\right] \\ &\leq \mathbb{P}\left[\|\sqrt{2\pi}S\|_2 \cdot \|y\|_2 \geq st\sqrt{n} \mid y \leftarrow \mathcal{D}_{\Lambda',I_n}\right] \\ &= \mathbb{P}\left[\|y\|_2 \geq c\sqrt{n} \mid y \leftarrow \mathcal{D}_{\Lambda',I_n}\right].\end{aligned}$$

By Lemma 13 it holds that

$$\mathbb{P}\left[\|y\|_2 \geq c\sqrt{n} \mid y \leftarrow \mathcal{D}_{\Lambda',I_n}\right] = \frac{\rho(\Lambda \setminus c\sqrt{n}B_n)}{\rho(\Lambda)} < \left(e^{-\pi c^2} c\sqrt{2\pi e}\right)^n.$$

For t, c as defined, we have

$$\left(e^{-\pi c^2} c\sqrt{2\pi e}\right) < 1$$

and therefore, the probability is negligible in n. □

For a lattice in $\mathbb{R}^n$, the smoothing parameter can be bounded as follows.

Lemma 14 (Regev [28, Lemma 2.12]). *For any lattice $\Lambda \subseteq \mathbb{R}^n$ and $\varepsilon > 0$,*

$$\eta_\varepsilon(\Lambda) \leq \lambda_n(\Lambda) \cdot \sqrt{\frac{\ln(2n(1+1/\varepsilon))}{\pi}}.$$

In particular, for any superlogarithmic function $\omega(\log n)$ and any negligible function $\varepsilon(n)$, it holds that $\eta_\varepsilon(\Lambda) \leq \lambda_n(\Lambda)\sqrt{\omega(\log n)}$.

To prove Lemma 8, we first need a bound on the n-th smallest vector for the embedded lattice of a cyclotomic number field.

Lemma 15. *Let K be a cyclotomic number field with ring of integers R. For the canonical embedded lattice $\Lambda = \psi(\sigma(R)) \subseteq \mathbb{R}^n$ we have $\lambda_n(\Lambda) \leq \sqrt{n}$.*

Proof. The Basis matrix B_Λ contains n linear independent vectors of that size [22, 25]. □

With that we can prove Lemma 8.

Lemma 8. *For the parameters of the DRE* `DRE`*, $\Sigma_f \coloneqq \Sigma^i \in \mathbb{R}^{n\times n}$, $e = (e_1, \dots e_m) \coloneqq e_1^i \in J_q^m$ with $i \in \{R, S\}$ and $\epsilon = \epsilon(n) > 0$ negligible, it holds that*

$$\begin{aligned}&\eta_\epsilon(\Lambda) \leq \sqrt{2\pi}\sqrt{\Sigma_f}, \\ &\eta_\epsilon(\Lambda) \leq \sqrt{2\pi}t\beta_T\sqrt{m}q\alpha \text{ and} \\ &\eta_\epsilon(\Lambda) \leq \sqrt{2\pi}A_{e_\nu}^{-1}\sqrt{\left(\Sigma_f^{-1} + (t^2\beta_T^2 A_{e_\nu}A_{e_\nu}^T)^{-1}\right)^{-1}}\end{aligned}$$

for $1 \leq \nu \leq m$ where $e_\nu \neq 0$.

Proof. First we prove that $\eta_\varepsilon(\Lambda) \leq \sqrt{2\pi} \cdot t\beta_T\sqrt{m}q\alpha$. Using the definition of q combined with Lemmas 14 and 15 and the fact that `DRE` uses a cyclotomic number field yields

$$\eta_\varepsilon(\psi(\Lambda)) \leq \lambda_n(\psi(\Lambda)) \cdot \omega(\sqrt{\log n}) \leq \sqrt{n} \cdot \omega(\sqrt{\log n}) \leq \sqrt{2\pi} \cdot t\beta_T\sqrt{m}q\alpha.$$

By definition of Σ_f we have

$$\Sigma_f = t^2\beta_T^2 Mul(e) + t^2\beta_T^2 m(q\alpha)^2 I \succeq t^2\beta_T^2 m(q\alpha)^2 I$$

and therefore

$$\eta_\varepsilon(\psi(\Lambda)) \leq \sqrt{2\pi} \cdot t\beta_T\sqrt{m}q\alpha I_n \leq \sqrt{2\pi} \cdot \sqrt{\Sigma_f}.$$

For the last inequality let $S \coloneqq A_{e_\nu}^{-1}\sqrt{\left(\Sigma_f^{-1} + (t^2\beta_T^2 A_{e_\nu}A_{e_\nu}^T)^{-1}\right)^{-1}}$. Let also $1 \leq \nu \leq m$ be arbitrary but fixed and $e_\nu = (r_1, ..., r_{s_1}, c_1, \overline{c_1}, ..., c_{s_2}, \overline{c_{s_2}})^T$, where $r_j \in \mathbb{R}$ and $c_j = a_j + b_j i \in \mathbb{C}$. By the structure of A_{e_ν}, it is

$$A_{e_\nu}^{-1} = \begin{pmatrix} D(r_1^{-1}, \dots, r_{s_1}^{-1}) & & & \\ & \frac{1}{a_1^2+b_1^2}Rot_1^T & & \\ & & \ddots & \\ & & & \frac{1}{a_{s_2}^2+b_{s_2}^2}Rot_{s_2}^T \end{pmatrix}.$$

Let $y_j^2 = (\sum_{\nu=1}^m A_{e_\nu}A_{e_\nu}^T)_{jj} + m(q\alpha)^2$. For $1 \leq j \leq s_1$ let

$$s_j^r \coloneqq r_j^{-1}\sqrt{\left(\frac{1}{t^2\beta_T^2 y_j^2} + \frac{1}{t^2\beta_T^2 r_j^2}\right)^{-1}}.$$

For $1 \leq j \leq s_2$, define the block matrix S_j^c as

$$S_j^c \coloneqq \frac{1}{a_j^2+b_j^2} \cdot \sqrt{\left(\frac{1}{t^2\beta_T^2 y_j^2} + \frac{1}{t^2\beta_T^2(a_j^2+b_j^2)}\right)^{-1}} \cdot Rot_j^T \in \mathbb{R}^{2\times 2}.$$

Using those definitions, S can be written as

$$S = \begin{pmatrix} D(s_1^r, \dots, s_{s_1}^R) & & & \\ & S_1^c & & \\ & & \ddots & \\ & & & S_{s_2}^c \end{pmatrix}.$$

With that, SS^T comes down to $(s_j^r)^2$ and $S_j^c(S_j^c)^T$, which is

$$\begin{aligned}(s_j^r)^2 &= r_j^{-2} \cdot \left(\frac{1}{t^2\beta_T^2 y_j^2} + \frac{1}{t^2\beta_T^2 r_j^2}\right)^{-1} = \left(\frac{r_j^2}{t^2\beta_T^2 y_j^2} + \frac{1}{t^2\beta_T^2}\right)^{-1} \\ &= \frac{t^2\beta_T^2 y_j^2}{r_j^2 + y_j^2} \overset{(*)}{\geq} \frac{t^2\beta_T^2}{2}\end{aligned}$$

and

$$S_j^c(S_j^c)^T = \frac{1}{a_j^2+b_j^2}\cdot\left(\frac{1}{t^2\beta_T^2 r_j^2}+\frac{1}{t^2\beta_T^2(a_j^2+b_j^2)}\right)^{-1}\cdot I_2$$
$$= \left(\frac{a_j^2+b_j^2}{t^2\beta_T^2 r_j^2}+\frac{1}{t^2\beta_T^2}\right)^{-1}\cdot I_2 \overset{(**)}{\succeq} \frac{t^2\beta_T^2}{2}\cdot I_2.$$

The inequalities (*) and (**) hold because $r_j^2 \le y_j^2$ and $a_j^2+b_j^2 \le y_j^2$, respectively. With that, it holds that

$$SS^T \succeq \frac{t^2\beta_T^2}{2} I_n.$$

Using Lemmas 14 and 15 with $t\sqrt{n}$ as $\omega(\sqrt{\log n})$ function yields

$$\begin{aligned}
\eta_\varepsilon(\psi(\Lambda)) &\le \sqrt{n}\cdot t\sqrt{n} I_n \\
&\le t\sqrt{2}n\cdot q^{1/m+2/(mn)} I_n \\
&\le \frac{t\beta_T}{\sqrt{2}} I_n \\
&\le A_{e_\nu}^{-1}\sqrt{\left(\Sigma_f^{-1}+(t^2\beta_T^2\Sigma_{e_\nu})^{-1}\right)^{-1}} \\
&\le \sqrt{2\pi}\cdot A_{e_\nu}^{-1}\sqrt{\left(\Sigma_f^{-1}+(t^2\beta_T^2\Sigma_{e_\nu})^{-1}\right)^{-1}}.
\end{aligned}$$

□

B Uniqueness of RLWE witness

This section proves the statements related to the unique RLWE witness, i.e. Lemmas 6 and 7. First, we have a closer look at how $\Phi_{2n}(X)$ decomposes under the modulo.

Lemma 16. *There exists $a_i^j \in \mathbb{Z}_q$ for $j \in [\log(r)]$ and $i \in [r]$ such that*

$$\begin{aligned}
\Phi_{2n}(X) &\equiv X^n+1 \\
&\equiv (X^{n/2}+a_1^1)(X^{n/2}-a_1^1) \\
&\equiv (X^{n/4}+a_2^1)(X^{n/4}-a_2^1)(X^{n/4}+a_2^2)(X^{n/4}-a_2^2) \\
&\equiv \dots \\
&\equiv \prod_{j\in[\log(r)],i\in[r]} (X^{n/r}+a_j^i)(X^{n/r}-a_j^i) \pmod q.
\end{aligned}$$

Moreover, $(a_{j+1}^i)^2 = (-1)^i a_j^{\lceil i/2\rceil}$.

Proof. As $q \equiv 1 \pmod{2r}$, there is an element z with order $2r$ in $\mathbb{Z}_q$ [23]. Combining this with the fact that r is a power of two, we get $\sqrt{-1} = z^{r/2} \in \mathbb{Z}_q$. Therefore, $a_1^1 = z^{r/2}$ satisfies the first equation. For the other equations, it suffices to show that for $j < \log r$, each a_j^i has a root in $\mathbb{Z}_q$ as

$$\begin{aligned}\left(X^{n/2^j} + a_j^i\right) &= \left(X^{n/2^{j+1}} + \sqrt{-1}\sqrt{a_j^i}\right)\left(X^{n/2^{j+1}} - \sqrt{-1}\sqrt{a_j^i}\right) \\ &= \left(X^{n/2^{j+1}} + z^{r/2}\sqrt{a_j^i}\right)\left(X^{n/2^{j+1}} - z^{r/2}\sqrt{a_j^i}\right) \text{ and} \\ \left(X^{n/2^j} - a_j^i\right) &= \left(X^{n/2^{j+1}} + \sqrt{a_j^i}\right)\left(X^{n/2^{j+1}} - \sqrt{a_j^i}\right).\end{aligned}$$

With an induction over j, it can be shown that each a_j^i is a product of powers of z with a power of two as exponent. Starting with $a_1^1 = z^{r/2}$, $-a_1^1 = z^r z^{r/2}$, taking the root of these elements, each exponent is halved. As r is a power of two, the halved exponents are again powers of two, until z^1 is reached. This happens exactly when $j = \log r$. The factors of $\sqrt{-1} = z^{r/2}$ do not change this fact. □

In addition, the last polynomials are all irreducible in $\mathbb{Z}_q$ [23]. Using this special decomposition, we can show that the reverse CRT has a very special structure.

Lemma 17. *Let $x \in R_q$ such that $\pi(x) = (0, \ldots, 0, x_r)$. Let also $a_k \coloneqq a_k^{2^k}$ be some of the factors from Lemma 16. Then, applying the reverse CRT yields*

$$\begin{aligned}x = x_r &\cdot (2a_{\log r})^{-1}(X^{n/r} + a_{\log r}) \\ &\cdot (2a_{\log r - 1})^{-1}(X^{2n/r} + a_{\log r - 1}) \\ &\cdots \\ &\cdot (2a_1)^{-1}(X^{n/2} + a_1).\end{aligned}$$

This is just applying the reverse CRT decomposition a few times with the polynomials from Lemma 16. Also note that if you use another x_i instead of x_r this works similar except for that the a_i are different.

Having a closer look at the coefficients of the reverse CRT of elements of the form $(0, \ldots, 0, x_i, 0, \ldots, 0)$ we can deduce the following corollary.

Corollary 1. *Let $x_i \in R_q/f_i$. The j-th coefficient of $\pi^{-1}((0, \ldots, 0, x_i, 0, \ldots, 0))$ depends only on the k-th coefficient of x_i, where $k = j \mod n/r$.*

Note that the mapping between the k-th coefficient in x_i and the j-th coefficient in $\pi^{-1}(0, \ldots, 0, x_i, 0, \ldots, 0)$ is bijective between $\mathbb{Z}_q$ and $\mathbb{Z}_q$.

Having this, we can bound the number of small elements in the different subspaces.

Lemma 6. *Let $\nu \in R_q \setminus \{0\}$ such that the CRT decomposition of ν is $\pi(\nu) = (\nu_1, \ldots, \nu_r)$ with $\nu_i = \nu \mod f_i \in \{0, 1\}$. Consider the subspace $U \coloneqq \nu R_q$. Then $\mathbb{P}\left[\|u\|_{\psi,\infty} < q/4 \mid u \xleftarrow{\$} U\right] \leq 2^{-n/r}$.*

Proof. First note that to draw a uniform random $u \xleftarrow{\$} U$ we can equivalently draw $u_i \xleftarrow{\$} U_i \coloneqq U/f_i$ and use π^{-1}.

Consider any j with $\nu_j = 1$. Assume we have drawn all u_i for $i \neq j$ and consider what happens if we draw u_j. We can decompose $\pi(u)$ into

$$\begin{aligned}&(u_1, \ldots, u_{j-1}, 0, u_{j+1}, \ldots u_r) + (0, \ldots, 0, u_j, 0, \ldots, 0)\\ &= \pi(c) + (0, \ldots, 0, u_j, 0, \ldots, 0),\end{aligned}$$

for some $c \in U$.

Let Cof be the function that maps a polynomial $y \in R_q$ to the vector containing the first n/r coefficients of y. By Corollary 1 each coefficient of $u_j \in U_j$ affects exactly one coefficient in $Cof(\pi^{-1}((0, \ldots, 0, u_j, 0, \ldots, 0)))$, and therefore we have

$$u_j \mapsto Cof(\pi^{-1}((0, \ldots, 0, u_j, 0, \ldots, 0)))$$

is bijective from U_j to $\mathbb{Z}_q^{n/r}$. Adding any $c \in U$ does not change this fact. Thus, the amount of small elements in $U_j + c$ and $\mathbb{Z}_q^{n/r}$ are the same.

As $\mathbb{Z}_q$ has $q/2$ elements with norm less than $q/4$ we get

$$\mathbb{P}\left[\|u\|_{\varphi,\infty} < q/4 \mid u \xleftarrow{\$} U\right] = \mathbb{P}\left[\|x + c\|_{\varphi,\infty} < q/4 \mid x \xleftarrow{\$} U_i, c \in U\right] \leq 2^{-n/r}$$

which finishes the proof. □

Lemma 7. *Let $m \geq r \log q + \frac{r\omega(\log n)}{n}$ for some superlogarithmic function $\omega(\log n)$. Then for all but a negligible fraction of $a \in R_q^m$ and for any $b \in R_q^m$, there exists at most one pair $(s, e) \in R_q \times R_q^m$ such that $as + e = b$ and $\|e\|_{\psi,\infty} < q/8$.*

Proof. For any $a \in R_q^m$ assume that there are $(s, e) \neq (s', e')$ such that $a \cdot s + e = a \cdot s' + e'$ with $\|e\|_{\varphi,\infty}, \|e'\|_{\varphi,\infty} < q/8$. Then, we have $\|a \cdot z\|_{\varphi,\infty} < q/4$ for $z = s - s' \neq 0$.

So let $z \in R_q$ be arbitrary but fixed. We can write $z = \nu \cdot d$ with $d \in R_q$ invertible and $\nu = \pi^{-1}((\delta_1, \ldots, \delta_r)) \in R_q$ where $\delta_i = 1$ if $\pi(z)_i \neq 0$, else 0. Then $a \cdot z = a \cdot \nu \cdot d = \nu \cdot a \cdot d$. As d is invertible, $a \cdot d$ is uniform over R_q^m. Therefore, by Lemma 6,

$$\begin{aligned}\mathbb{P}\left[\|a \cdot z\|_{\varphi,\infty} < q/4 \mid a \xleftarrow{\$} R_q^m\right] &= \mathbb{P}\left[\|\nu \cdot a \cdot d\|_{\varphi,\infty} < q/4 \mid a \xleftarrow{\$} R_q^m\right]\\ &= \mathbb{P}\left[\|u\|_{\varphi,\infty} < q/4 \mid u \xleftarrow{\$} U^m \coloneqq (\nu R_q)^m\right]\\ &= \left(\mathbb{P}\left[\|u_i\|_{\varphi,\infty} < q/4 \mid u_i \xleftarrow{\$} U\right]\right)^m \leq 2^{-nm/r}.\end{aligned}$$

So by the union bound we have

$$\mathbb{P}\left[\exists z \in R_q : \|a \cdot z\|_{\varphi,\infty} < q/4 \mid a \leftarrow R_q^m\right] \leq q^n \cdot 2^{-nm/r} \leq \text{negl},$$

which by the first observation proves the lemma. □

C Parameter Sets with Unique RLWE Samples

This Section describes the parameter sets for the DRE in which the RLWE samples are unique and thus, no commitment scheme is needed. As stated in Lemma 7, for unique RLWE samples we require $m \geq r \log q + \frac{r\omega(\log n)}{n}$ for $r > 1$ a power of two. We choose $r = 2$ and $m = \lceil r \log q + \frac{r(\log n)^2}{n} \rceil$. Note that this is the same r for which $q = 2r + 1 \mod 4r$. This yields the parameter sets shown in Table 7. Again, $\gamma_T = \frac{1}{\sqrt{n}} t\beta_T$ and $\gamma_e = \frac{1}{\sqrt{n}} tq\alpha$ describe the width of the Gaussian distribution for each coefficent of the trapdoor and errors, respectively.

n	q ($\lceil \log_2 q \rceil$)	m	γ_T	γ_e	C/S	SecLvl	size(pk)	size(sk)	size(c)
1024	0x3b18215 (26)	52	1.6	1.6	C	132	259 KB	4.5 MB	519 KB
2048	0x1F24D205A1 (37)	74	109	14.6	S	232	1.05 MB	25.9 MB	2.1 MB

Table 7. Parameter sets for the DRE with unique RLWE samples.